

An algebraic approach to Latin squares of prime power order by local permutation polynomials

Raúl M. Falcón^{1*}, Jaime Gutiérrez² and Jorge Jiménez Urroz³

^{1*}Departamento de Matemática Aplicada I, Universidad de Sevilla,
Avenida Reina Mercedes, 4 A, Seville, 41012, Spain.

²Departamento de Matemática Aplicada y Ciencias de la Computación,
Universidad de Cantabria, Avenida Los Castros 44, Santander, 39005,
Spain.

³Departamento de Matemática e Informática Aplicadas a la Ingeniería
Civil y Naval, Universidad Politécnica de Madrid, Calle Profesor
Aranguren S/N, Madrid, 28040, Spain.

*Corresponding author(s). E-mail(s): rafalgan@us.es;

Contributing authors: jaime.gutierrez@unican.es; jorge.urroz@upm.edu;

Abstract

Every Latin square of prime power order q is uniquely described by a local permutation polynomial (LPP) in the polynomial ring $\mathbb{F}_q[x, y]$. Despite this equivalence, one may find in the literature only some preliminary results on the relationship among Latin squares and LPPs. This paper delves into this topic by showing how the coefficients of any LPP are identified with the zeros of an algebraic set over $\mathbb{F}_q$. This allows for an algebraic description of all Latin squares of order q by means of a unique polynomial in $\mathbb{F}_q[x, y]$, whose coefficients satisfy the constraints defined by the algebraic set under consideration. In order to make much easier the construction of this polynomial, we also deal with the natural translation to LPPs of both notions of reduced and isotopic Latin squares. Our algebraic approach is readily adapted to identify both types of Latin squares. All of the above is constructively illustrated for $q \in \{4, 5\}$. We finish our study with the natural translation to LPPs of both notions of complete mappings and orthomorphisms of quasigroups, showing their relationship with transversals and isotopisms of Latin squares.

Keywords: Local permutation polynomial; permutation polynomial; Latin square; quasigroup; isotopism; complete mapping; orthomorphism.

MSC Classification: 11T06; 05B05; 20N05

1 Introduction

Let $\mathbb{F}_q$ be the finite field of order a prime power q . It is well known [1] that any mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$ is defined by a unique polynomial in the polynomial ring $\mathbb{F}_q[x]$ of degree lower than q . This is called a *permutation polynomial* (PP) if it acts as a permutation on $\mathbb{F}_q$. This kind of polynomials has relevant applications in cryptography, coding theory, and combinatorial design (see [2] for a survey on PPs.) Furthermore, a polynomial f in the polynomial ring $\mathbb{F}_q[x, y]$ is called a *local permutation polynomial* (LPP) if both polynomials $f(x, a)$ and $f(a, x)$ are PPs in $\mathbb{F}_q[x]$ for all $a \in \mathbb{F}_q$. From now on, we denote by $\mathcal{P}_q$ and $\mathcal{LP}_q$ the respective sets of PPs in $\mathbb{F}_q[x]$ and LPPs in $\mathbb{F}_q[x, y]$. Throughout this paper, we identify all functions $\mathbb{F}_q^2 \rightarrow \mathbb{F}_q$ with the interpolating polynomial, with degree less than q in each variable.

Each polynomial in $\mathcal{LP}_q$ describes uniquely both a quasigroup and a Latin square of order q . Recall here that, if $\mathbb{F}_q$ is endowed with a binary operation f such that both equations $f(s, a) = b$ and $f(a, s) = b$ have exactly one solution $s \in \mathbb{F}_q$ for any $a, b \in \mathbb{F}_q$, then the pair $(\mathbb{F}_q, f)$ is said to be a *quasigroup* of order q . Its multiplication table is a *Latin square* of the same order, which we denote by L_f . (That is, $L_f[a, b] := f(a, b)$ for all $a, b \in \mathbb{F}_q$.) This is a $q \times q$ array such that each element in $\mathbb{F}_q$ appears exactly once per row and exactly once per column. In cryptography, quasigroups and Latin squares have been used to design error-correcting codes, cryptographic primitives, pseudorandom sequences with high period growth or image encryption algorithms, among other applications (see [3]). From now on, we denote by $\mathcal{L}_q$ the set of Latin squares over $\mathbb{F}_q$. Mullen [4] (see also [5, 6]) realized that every Latin square $L \in \mathcal{L}_q$ is uniquely identified with a polynomial $f_L \in \mathcal{LP}_q$, with $\deg(f_L) < 2q - 1$, so $f_L(a, b) := L[a, b]$ for all $a, b \in \mathbb{F}_q$. That is, (L, f_L) is a quasigroup.

This equivalence among Latin squares, quasigroups and LPPs gives rise to a natural translation of related concepts and results. This paper delves into this topic by focusing on how the study of LPPs can provide some relevant information on the problems of counting, enumerating, and distributing Latin squares into isotopism classes. These problems have been completely solved only for Latin squares of order $n \leq 11$ (see [7–9]). In the literature, one may find only some preliminary results on this topic [5, 6, 10–15]. In particular, Mullen [5] described the set of coefficients of every polynomial in $\mathcal{LP}_p$, with p an odd prime, as an algebraic set over $\mathbb{F}_p$. This algebraic set is in one-to-one correspondence with the set $\mathcal{L}_p$. In this regard, he proved that every polynomial in $\mathcal{LP}_2$ and $\mathcal{LP}_3$ is linear. More precisely,

$$\mathcal{LP}_2 = \bigcup_{s_{00} \in \mathbb{F}_2} \{x + y + s_{00}\} \quad (1)$$

and

$$\mathcal{LP}_3 = \bigcup_{a, b, c \in \mathbb{F}_3} \{s_{10}x + s_{01}y + s_{00} : s_{10}^2 s_{01}^2 = 1\}. \quad (2)$$

As a consequence,

$$\mathcal{L}_2 \cong \mathbb{F}_2 \quad \text{and} \quad \mathcal{L}_3 \cong \{(a, b, c) \in \mathbb{F}_3^3 : a^2 b^2 = 1\}.$$

This paper deals with the following more general question.

Problem 1.1 *Let q be a prime power. Describe explicitly the sets of coefficients of any polynomial in $\mathcal{P}_q$ (respectively, $\mathcal{LP}_q$), as an algebraic set over $\mathbb{F}_q$. Use this algebraic set to count the number of polynomials in $\mathcal{LP}_q$.*

In this paper, we show how the existence of these algebraic sets allows the description of all Latin squares of order q by a unique polynomial in $\mathbb{F}_q[x, y]$. This unified representation makes it much easier to deal with the problems of counting, enumerating, and classifying Latin squares. To the best of our knowledge, this paper is a pioneer in dealing with Problem 1.1 for LPPs. Concerning the set $\mathcal{P}_q$, in the literature one may find some partial results characterizing and counting some PPs with either few terms (see, for example, [16–20], and the references therein) or small degree. In this last regard, we have $ax + b \in \mathcal{P}_q$ for all $a, b \in \mathbb{F}_q$. In addition, Mollin and Small [21] proved the following two statements for PPs with degrees two and three.

- (D2) $ax^2 + bx + c \in \mathcal{P}_q$, with $a \neq 0$, if and only if $b = 0$ and $\text{char}(\mathbb{F}_q) = 2$.
- (D3) If $\text{char}(\mathbb{F}_q) \neq 3$, then $ax^3 + bx^2 + cx + d \in \mathcal{P}_q$, with $a \neq 0$, if and only if $b^2 = 3ac$ and $q \equiv 2 \pmod{3}$.

Let $\mathcal{P}_{q,d}$ be the subset of polynomials of degree d in $\mathcal{P}_q$. The problem of determining the number $N_q(d) := |\mathcal{P}_{q,d}|$ was introduced in [22]. In particular, $N_q(1) = q(q-1)$, and, if $q > 2$, then $N_q(d) = 0$ whenever d divides $q-1$. Hence, $q-2$ (respectively, $2q-4$) is an upper bound for the degree of a polynomial in $\mathcal{P}_q$ (respectively, $\mathcal{LP}_q$), with $q > 2$. The upper bound for LPPs decreases to $q-2$ if the polynomial describes an m -circulant Latin square (see [11]). A formula for $N_p(p-2)$, with p prime, was provided in [23] in terms of the permanent of a Vandermonde matrix whose entries are the p^{th} roots of unity. (A generalization for prime powers was provided in [24].) The number of polynomials in $\mathcal{P}_q$ of degree less than $q-2$ has been asymptotically bounded in [23–25]. This last number is explicitly only known for $q \leq 11$ (see [25]). There is no study on the distribution of polynomials in $\mathcal{LP}_q$ with respect to their total degrees.

The paper is organized as follows.

- In Section 2, we indicate some preliminary concepts and results on algebraic geometry and Latin squares that are used throughout the paper.
- In Section 3, we give the explicit description required in Problem 1.1 and we describe an algebraic geometry procedure to efficiently determine the constraints satisfied by the coefficients of any polynomial in $\mathcal{P}_q$ or $\mathcal{LP}_q$. We use this procedure to characterize all polynomials in $\mathcal{P}_4$, $\mathcal{P}_5$ and $\mathcal{LP}_4$. We conveniently modify our procedure to deal with polynomials of a given degree, symmetric LPPs and the so-called reduced LPPs, which we introduce as a natural translation of reduced Latin squares. In particular, we determine the values of $N_q(d)$ for all $q \leq 13$, and also the number of symmetric and reduced polynomials in $\mathcal{LP}_q$, with $q \in \{4, 5\}$, of any given degree.
- In Section 4, we introduce the natural translation to LPPs of the notion of isotopism of Latin squares, which allows the distribution of LPPs into isotopism classes. In particular, the class containing the linear polynomial $x + y$ gives rise to what we call isolinear LPPs. We show that any polynomial that is not isolinear constitutes a solution of an open problem raised by Lee and Ko in [10]. We also describe an isotopism that maps any polynomial in $\mathcal{L}_q$ to a reduced LPP. We illustrate for $q = 4$ how this map facilitates the distribution of LPPs into isotopism classes.

- Finally, Section 5 deals with the natural translation to LPPs of the notions of complete mappings and orthomorphisms of Latin squares of quasigroups, showing their relationship with transversals and isotopisms of Latin squares. Winterhof [26] had already considered the generalization of these concepts using PPs.

2 Preliminaries

In this section, we indicate some preliminary notions and results on algebraic geometry and transversals and isotopisms of Latin squares that we use throughout the paper. We refer the reader to [27, 28] for two more details on these topics. In addition, we refer the reader to [29, 30] for a pair of comprehensive surveys on transversals of Latin squares.

2.1 Algebraic geometry

Let $\mathbb{F}_q[X]$ be a multivariate polynomial ring over the finite field $\mathbb{F}_q$, with q a prime power, on a set of variables $X = \{x_1, \dots, x_n\}$. An *ideal* of $\mathbb{F}_q[X]$ is any subset $I \subseteq \mathbb{F}_q[X]$ such that $0 \in I$; $f + g \in I$ for all $f, g \in I$; and $fg \in I$ for all $(f, g) \in I \times \mathbb{F}_q[X]$. Its *algebraic set* is the set of zeros

$$\mathcal{Z}(I) := \{(s_1, \dots, s_n) \in \mathbb{F}_q^n : f(s_1, \dots, s_n) = 0, \text{ for all } f \in I\}.$$

The ideal I is *zero-dimensional* if and only if $\dim_{\mathbb{F}_q}(\mathbb{F}_q[X]/I) < \infty$. This is *radical* if every polynomial $f \in \mathbb{F}_q[X]$ such that $f^m \in I$ for some positive integer m belongs to I . If the ideal I is zero-dimensional and radical, then $\mathcal{Z}(I)$ contains precisely $\dim_{\mathbb{F}_q}(\mathbb{F}_q[X]/I)$ distinct elements (see [31, Theorem 3.7.19]). Its computation follows from the reduced Gröbner basis of the ideal, which also makes easier the computation of $\mathcal{Z}(I)$. We remind the concept of Gröbner basis in the following paragraph.

The ideal of $\mathbb{F}_q[X]$ that is *generated by* the polynomials $f_1, \dots, f_n \in \mathbb{F}_q[X]$ is

$$\langle f_1, \dots, f_n \rangle := \left\{ \sum_{i=1}^n f_i \cdot g_i : g_i \in \mathbb{F}_q[X], \text{ for all } i \right\}.$$

The largest monomial of a polynomial $f \in I$, with respect to a given monomial term ordering $\preceq$ is its *leading monomial*. The ideal generated by all the leading monomials in I is the *initial ideal* $I_{\preceq}$. A generating set of I whose leading monomials generate $I_{\preceq}$ is a *Gröbner basis* of I . It is *reduced* if all its polynomials are monic, and no monomial in a generator is generated by the leading monomials of the other generators. This reduced Gröbner basis is unique. Its computation is extremely sensitive to the number of variables, and the length and degree of the generators [32].

The computation of reduced Gröbner bases and dimensions of quotient rings in this paper has always been done by using our own library *lpp.lib* in the open computer algebra system for polynomial computations SINGULAR [33]. This library is available as supplementary material to the paper.

2.2 Transversals and isotopisms of Latin squares

Every Latin square $L \in \mathcal{L}_q$, with entries in $\mathbb{F}_q$, is uniquely determined by its set of entries

$$\text{Ent}(L) := \{(a, b, L[a, b]) : a, b \in \mathbb{F}_q\}.$$

A *transversal* of L is any subset $S \subset \text{Ent}(L)$ formed by q entries such that no two entries belong to the same row or the same column and no two entries contain the same symbol. Transversals of Latin squares are uniquely related to complete mappings and orthomorphisms of quasigroups, whose notions we recall here by means of the so-called Hadamard quasigroup product (see [34, 35]). The *Hadamard quasigroup product* of two permutations g_1 and g_2 in the symmetric group $\mathcal{S}_q$ on $\mathbb{F}_q$ with respect to a quasigroup $(\mathbb{F}_q, f)$ is a map $\odot_f(g_1, g_2) : \mathbb{F}_q \rightarrow \mathbb{F}_q$ that is defined so that

$$\odot_f(g_1, g_2)(a) := f(g_1(a), g_2(a)) \quad (3)$$

for all $a \in \mathbb{F}_q$. If Id is the trivial permutation on $\mathbb{F}_q$, then a *complete mapping* of the quasigroup $(\mathbb{F}_q, f)$ is any permutation $g \in \mathcal{S}_q$ such that $\odot_f(\text{Id}, g) \in \mathcal{S}_q$. The latter is called an *orthomorphism* of the quasigroup. Lemma 4.2 in [35] (see also Theorem 6.2 in [30]) ensures the following result.

Lemma 2.1 *Let $(\mathbb{F}_q, f)$ be a quasigroup. A subset $S \subset \text{Ent}(L_f)$ is a transversal of the Latin square $L_f \in \mathcal{L}_q$ if and only if there is a complete mapping g of the quasigroup such that*

$$S = \{(a, g(a), \odot_f(\text{Id}, g)(a)) : a \in \mathbb{F}_q\}.$$

Niederreiter and Robinson [36] proved that every polynomial in $\mathcal{P}_q$ describing a complete mapping of the additive group $(\mathbb{F}_q, +)$, with $q > 3$ an odd prime, has degree $\leq q - 3$. Then, they determined all these polynomials having degree < 6 , as well as those of degree six for finite fields of order prime to six.

Now, we recall how the symmetric group $\mathcal{S}_q$ acts on the set $\mathcal{L}_q$. An *isotopism* in $\mathcal{L}_q$ is every triple $\Theta := (\theta_1, \theta_2, \theta_3) \in \mathcal{S}_q \times \mathcal{S}_q \times \mathcal{S}_q$. The *isotope* $L^\Theta \in \mathcal{L}_q$ of a Latin square $L \in \mathcal{L}_q$ is defined so that

$$\text{Ent}(L^\Theta) := \{(\theta_1(a), \theta_2(b), \theta_3(c)) : (a, b, c) \in \text{Ent}(L)\}. \quad (4)$$

That is, θ_1 permutes the rows of L , θ_2 permutes its columns, and θ_3 permutes the symbols appearing in its cells. It is also said that L and L^Θ are *isotopic*. The isotopism Θ is *principal* if θ_3 is the trivial permutation on $\mathbb{F}_q$. If this is the case, then L and L^Θ are said to be *principal isotopic*. Furthermore, if $\theta_1 = \theta_2 = \theta_3$, then we get an *isomorphism* from L to L^Θ , which are then said to be *isomorphic*. Being (principal) isotopic or isomorphic are equivalence relations among Latin squares. Finally, if $L^\Theta = L$, then Θ is called an *autotopism* of L (an *automorphism* if $\theta_1 = \theta_2 = \theta_3$). The set of autotopisms of L has a group structure with the composition of permutations. All these notions are readily translated to quasigroups (see [37]) and hence to LPPs. Section 4 focuses on this last aspect.

3 Algebraic sets describing PPs and LPPs

This section deals with Problem 1.1. More precisely, we show how both sets $\mathcal{P}_q$ and $\mathcal{LP}_q$, with $q > 3$ a prime power, are identified with the algebraic sets of a pair of ideals over $\mathbb{F}_q$. (The case $q \in \{2, 3\}$ was already considered by Mullen [5].) The keystone here is the ideal associated with $\mathcal{P}_q$. It is due to the fact that every polynomial $f \in \mathcal{LP}_q$ is uniquely determined by the set of q^2 polynomials $\{f(x, c), f(c, x) : c \in \mathbb{F}_q\} \subseteq \mathcal{P}_q$. Thus, the ideal associated with $\mathcal{LP}_q$ has to be related to that associated with $\mathcal{P}_q$.

Let us consider the sets of variables

$$X_q := \{x_i : i \in \{0, \dots, q-2\}\} \quad \text{and} \quad \overline{X}_q := \{x_{ij} : i, j \in \{0, \dots, q-2\}\}.$$

In what follows, we show how the set $\mathcal{P}_q$ (respectively, $\mathcal{LP}_q$) is identified with the algebraic set of an ideal in $\mathbb{F}_q[X_q]$ (respectively, $\mathbb{F}_q[\overline{X}_q]$). To this end, we conveniently use the algebraic approach described by Bayer [38] (see also [39]) for solving the graph coloring problem, which has later been used in the literature [40–44] for enumerating and classifying Latin squares and some related structures. More precisely, we define the function

$$F(x) := x^{q-1} - 1.$$

Note here that every zero of the equation $F(x) = 0$ belongs to $\mathbb{F}_q \setminus \{0\}$, and hence the equation $F(x - y) = 0$ implies $x \neq y$. Then, for each $a, b, c \in \mathbb{F}_q$, with $a \neq b$, we define the following polynomials.

$$\begin{aligned} F_{a,b} &:= F\left(\sum_{i=0}^{q-2} (a^i - b^i)x_i\right) \in \mathbb{F}_q[X_q] \\ G_{a,b,c}^{\text{row}} &:= F\left(\sum_{i,j=0}^{q-2} (a^i - b^i)c^j x_{ji}\right) \in \mathbb{F}_q[\overline{X}_q] \\ G_{a,b,c}^{\text{col}} &:= F\left(\sum_{i,j=0}^{q-2} (a^i - b^i)c^j x_{ij}\right) \in \mathbb{F}_q[\overline{X}_q] \end{aligned}$$

Note that the polynomial $G_{a,b,c}^{\text{row}}$ (respectively, $G_{a,b,c}^{\text{col}}$) coincides with $F_{a,b}$ once each variable x_i is replaced by the polynomial $\sum_{j=0}^{q-2} c^j x_{ji}$ (respectively, $\sum_{j=0}^{q-2} c^j x_{ij}$). This fact will play a relevant role in Remark 3.1 to make our algebraic approach more efficient.

Lemma 3.1 *The next statements hold.*

- a) *The set $\mathcal{P}_q$ is identified with the algebraic set of the following zero-dimensional radical ideal in $\mathbb{F}_q[X_q]$.*

$$\mathcal{I}_q := \langle F_{a,b} : a, b \in \mathbb{F}_q, a \neq b \rangle + \langle x_i^q - x_i : i \in \{0, \dots, q-2\} \rangle$$

As a consequence, $|\mathcal{P}_q| = |\mathcal{Z}(\mathcal{I}_q)| = \dim_{\mathbb{F}_q}(\mathbb{F}_q[X_q]/\mathcal{I}_q)$.

b) The set $\mathcal{LP}_q$ is identified with the algebraic set of the following zero-dimensional radical ideal in $\mathbb{F}_q[\overline{X}_q]$.

$$\mathcal{J}_q := \langle G_{a,b,c}^{\text{row}}, G_{a,b,c}^{\text{col}} : a, b, c \in \mathbb{F}_q, a \neq b \rangle + \langle x_{ij}^q - x_{ij} : i, j \in \{0, \dots, q-2\} \rangle$$

As a consequence, $|\mathcal{LP}_q| = |\mathcal{Z}(\mathcal{J}_q)| = \dim_{\mathbb{F}_q}(\mathbb{F}_q[\overline{X}_q]/\mathcal{J}_q)$.

Proof Each zero $S := (s_0, \dots, s_{q-2}) \in \mathcal{Z}(\mathcal{I}_q)$ is uniquely identified with the polynomial

$$f_S := \sum_{i=0}^{q-2} s_i x^i \in \mathbb{F}_q[x].$$

We claim $f_S \in \mathcal{P}_q$ because, for each pair of elements $a, b \in \mathbb{F}_q$, with $a \neq b$, the polynomial $F_{a,b}$ implies that $f_S(a) \neq f_S(b)$. Since no polynomial in $\mathcal{P}_q$ has degree a divisor of $q-1$ (see [1]), the first statement holds.

Similarly, each zero $\overline{S} \in \mathcal{Z}(\mathcal{J}_q)$ is uniquely identified with the polynomial

$$f_{\overline{S}} := \sum_{i,j=0}^{q-2} s_{ij} x^i y^j \in \mathbb{F}_q[x, y],$$

where each s_{ij} is the component of $\overline{S}$ related to the variable x_{ij} . The second statement holds readily from (a) once we observe that $G_{a,b,c}^{\text{row}} = 0$ (respectively, $G_{a,b,c}^{\text{col}} = 0$) implies that $f_{\overline{S}}(c, x) \in \mathcal{P}_q$ (respectively, $f_{\overline{S}}(x, c) \in \mathcal{P}_q$) for all $c \in \mathbb{F}_q$.

The respective consequences hold from the fact that both ideals are zero-dimensional and radical. They are zero-dimensional because of the presence of all the generators $x_i^q - x$ in $\mathcal{I}_q$, and $x_{ij}^q - x_{ij}$ in $\mathcal{J}_q$, which make their respective zeros to take values in $\mathbb{F}_q$. They are radical from Seidenberg's Lemma (see [31, Proposition 3.7.15]). $\square$

From now on, we denote by $\mathcal{LP}_{q,d}$ the subset of polynomials of total degree d in $\mathcal{LP}_q$. The following result shows how the ideals described in Lemma 3.1 can be conveniently modified to identify both subsets $\mathcal{P}_{q,d}$ and $\mathcal{LP}_{q,d}$ with the algebraic sets of a pair of ideals over $\mathbb{F}_q$. Its proof is similar to that of the aforementioned lemma.

Lemma 3.2 *The next statements hold.*

a) The set $\mathcal{P}_{q,d}$, with $d \leq q-2$, is identified with the algebraic set of the following zero-dimensional radical ideal in $\mathbb{F}_q[X_q]$.

$$\mathcal{I}_{q,d} := \mathcal{I}_q + \langle x_i : i > d \rangle + \langle x_d^{q-1} - 1 \rangle$$

In particular, $N_q(d) = |\mathcal{Z}(\mathcal{I}_{q,d})| = \dim_{\mathbb{F}_q}(\mathbb{F}_q[X_q]/\mathcal{I}_{q,d})$.

b) The set $\mathcal{LP}_{q,d}$ is identified with the algebraic set of the following zero-dimensional radical ideal in $\mathbb{F}_q[\overline{X}_q]$.

$$\mathcal{J}_{q,d} := \mathcal{J}_q + \langle x_{ij} : i+j > d \rangle + \left\langle \prod_{i+j=d} (x_{ij}^{q-1} - 1) \right\rangle$$

As a consequence, $|\mathcal{LP}_{q,d}| = |\mathcal{Z}(\mathcal{J}_{q,d})| = \dim_{\mathbb{F}_q}(\mathbb{F}_q[\overline{X}_q]/\mathcal{J}_{q,d})$.

Remark 3.1 The reduced Gröbner basis of $\mathcal{I}_q$ in Lemma 3.1 establishes some constraints that must be satisfied by the coefficients of every polynomial in $\mathcal{P}_q$. We can use these constraints to compute much more efficiently the reduced Gröbner basis of the ideal $\mathcal{J}_q$ of the aforementioned lemma. To this end, note that, for each $c \in \mathbb{F}_q$, the polynomials

$$f_{\overline{S}}(x, c) = \sum_{i=0}^{q-2} \left(\sum_{j=0}^{q-2} s_{ij} c^j \right) x^i \quad \text{and} \quad f_{\overline{S}}(c, y) = \sum_{i=0}^{q-2} \left(\sum_{j=0}^{q-2} s_{ji} c^j \right) y^i$$

are PPs. In practice, for each $c \in \mathbb{F}_q$, we remove from $\mathcal{J}_q$ both sets of generators

$$\{G_{a,b,c}^{\text{row}} : a, b \in \mathbb{F}_q, a \neq b\} \quad \text{and} \quad \{G_{a,b,c}^{\text{col}} : a, b \in \mathbb{F}_q, a \neq b\}.$$

Instead of the first set (respectively, the second one), we include the reduced Gröbner basis of the ideal $\mathcal{I}_q$ by replacing each variable x_i in that basis by the expression

$$\sum_{j=0}^{q-2} x_{ij} c^j \quad (\text{respectively,} \quad \sum_{j=0}^{q-2} x_{ji} c^j).$$

(Recall here that each element s_{ij} in $f_{\overline{S}}$ is associated to the variable x_{ij} .) In particular, for $c = 0$, we replace each variable x_i by the variable x_{i0} (respectively, x_{0i}). This gives rise to a new zero-dimensional radical ideal in $\mathbb{F}_q[\overline{X}_q]$ whose algebraic set coincides with that of $\mathcal{J}_q$. Calculating the reduced Gröbner basis of this new ideal is much more efficient than calculating that of $\mathcal{J}_q$, because it avoids repeating computations.

We illustrate this approach by characterizing all polynomials in $\mathcal{P}_4$ and $\mathcal{P}_5$. This characterization is consistent with statements (D2) and (D3) in the introductory section. Then we decompose $\mathcal{LP}_4$ into two disjoint subsets that, as we prove in Section 4, separately describe the two isotopism classes of Latin squares of order four.

Proposition 3.1 *It is verified that*

$$\mathcal{P}_4 = \mathcal{P}_{4,1} \sqcup \mathcal{P}_{4,2} = \bigcup_{s_0, s_1, s_2 \in \mathbb{F}_4} \{s_2 x^2 + s_1 x + s_0 : s_1^3 + s_2^3 = 1\},$$

where

$$\mathcal{P}_{4,1} = \bigcup_{s_0, s_1 \in \mathbb{F}_4} \{s_1 x + s_0 : s_1^3 = 1\} \quad \text{and} \quad \mathcal{P}_{4,2} = \bigcup_{s_0, s_2 \in \mathbb{F}_4} \{s_2 x^2 + s_0 : s_2^3 = 1\}.$$

Proof The reduced Gröbner basis of the ideal $I_4 \subset \mathbb{F}_4[X_4]$ described in Lemma 3.1, with respect to the degree inverse lexicographical order, is the set

$$\{x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_2^3 + 1, \quad x_1 x_2, \quad x_2^4 + x_2\}. \quad (5)$$

This is also the reduced Gröbner basis of the ideal $\langle x_1^3 + x_2^3 - 1, \quad x_1 x_2 \rangle$, which therefore coincides with I_4 . Since the algebraic set of this last ideal coincides with that of the ideal generated only by the polynomial $x_1^3 + x_2^3 - 1$, Lemma 3.1 implies that

$$\mathcal{P}_4 \cong \mathcal{Z}(I_4) = \{(s_0, s_1, s_2) \in \mathbb{F}_4^3 : s_1^3 + s_2^3 = 1\}.$$

The characterization of the polynomials in both subsets $\mathcal{P}_{4,1}$ and $\mathcal{P}_{4,2}$ follows readily. $\square$

Proposition 3.2 *It is verified that*

$$\mathcal{P}_5 = \mathcal{P}_{5,1} \sqcup \mathcal{P}_{5,3} = \bigcup_{s_0, s_1, s_2, s_3 \in \mathbb{F}_5} \{s_3 x^3 + s_2 x^2 + s_1 x + s_0 : (s_1 + s_3)^4 = 1, s_2^2 = 3s_1 s_3\},$$

with

$$\mathcal{P}_{5,1} = \bigcup_{s_0, s_1 \in \mathbb{F}_5} \{s_1 x + s_0 : s_1^4 = 1\}$$

and

$$\mathcal{P}_{5,3} = \bigcup_{s_0, s_1, s_2, s_3 \in \mathbb{F}_5} \{s_3 x^3 + s_2 x^2 + s_1 x + s_0 : s_3^4 = 1, s_2^2 = 3s_1 s_3\}.$$

Proof The reduced Gröbner basis of the ideal $I_5 \subset \mathbb{F}_5[X_5]$ described in Lemma 3.1, with respect to the degree inverse lexicographical order, is the set

$$\left\{ (x_1 + x_3)^4 - 1, \quad x_2^2 + 2x_1 x_3, \quad x_2(x_1^2 + x_3^2), \quad x_3(x_1^3 + x_1 x_3^2), \quad x_3^5 - x_3, \quad x_2(x_3^4 - 1) \right\}.$$

This is also the reduced Gröbner basis of the ideal $\langle (x_1 + x_3)^4 - 1, \quad x_2^2 + 2x_1 x_3, \quad x_2(x_1^2 + x_3^2) \rangle$, which therefore coincides with I_5 . The result follows readily from Lemma 3.1 once we observe that the algebraic set of this last ideal coincides with that of the ideal $\langle (x_1 + x_3)^4 - 1, \quad x_2^2 + 2x_1 x_3 \rangle$. $\square$

Theorem 3.1 *The set $\mathcal{LP}_4$ is decomposed into the following two disjoint subsets.*

- The subset $\mathcal{LP}_{4,1} \sqcup \mathcal{LP}_{4,2}$, which is formed by 144 LPPs with separate variables of the form

$$s_{20}x^2 + s_{02}y^2 + s_{10}x + s_{01}y + s_{00} \in \mathbb{F}_4[x, y] \quad (6)$$

where

$$s_{01}^3 + s_{02}^3 = s_{10}^3 + s_{20}^3 = 1.$$

- The subset $\mathcal{LP}_{4,4}$, which is formed by 432 polynomials of the form

$$\begin{aligned} & (s_{22}xy + s_{21}x + s_{12}y + s_{12}s_{21}s_{22}^2)xy + s_{20}x^2 + s_{02}y^2 + \\ & + (s_{20}s_{22} + s_{21}^2)s_{12}s_{22}x + (s_{02}s_{22} + s_{12}^2)s_{21}s_{22}y + s_{00} \in \mathbb{F}_4[x, y] \end{aligned} \quad (7)$$

where

$$\begin{cases} s_{22}^3 = s_{21}^3 = s_{12}^3 = 1, \\ s_{20}(s_{20}s_{22} + s_{21}^2) = 0, \\ s_{02}(s_{02}s_{22} + s_{12}^2) = 0. \end{cases} \quad (8)$$

Proof In order to determine the set $\mathcal{LP}_4$, we conveniently replace the generators of the ideal $\bar{I}_4$ in Lemma 3.1 by the polynomials in (5) as we have indicated in Remark 3.1. The reduced Gröbner basis of the resulting ideal implies that every polynomial $\sum_{i,j=0}^2 s_{ij}x^i y^j \in \mathcal{LP}_4$ satisfies the next nine constraints.

$$\left\{ \begin{array}{l} s_{10}^3 + s_{20}^3 = 1, \\ s_{01}^3 + s_{02}^3 = 1, \\ s_{21}^3 + s_{22}^3 = 0, \\ s_{12}^3 + s_{22}^3 = 0, \\ s_{12}s_{10} + s_{11}^2s_{10}^3 = 0, \\ s_{11} + s_{12}s_{21}s_{22}^2 = 0, \\ s_{21} + s_{02}^2s_{12}s_{11} + s_{01}^2s_{11}^2 = 0, \\ s_{22} + s_{01}^2s_{12}s_{11} + s_{02}^2s_{12}^2 = 0, \\ s_{10}s_{22} + s_{12}s_{20} + s_{12}s_{21}^2s_{22}^2 = 0. \end{array} \right.$$

Depending on whether $s_{22} = 0$ or not, these constraints decompose $\mathcal{LP}_4$ into the two subsets $\mathcal{LP}_{4,2}$ and $\mathcal{LP}_{4,4}$ described in the statement. $\square$

In practice, if one is only interested in the number $N_q(d)$ (that is, in the cardinality of $\mathcal{P}_{q,d}$), and not in the enumeration of the polynomials in $\mathcal{P}_{q,d}$, then we can modify the ideals of Lemma 3.2 by including x_0 as generator of both ideals and replacing the generator $x_d^{q-1} - 1$ by $x_d - 1$. That is, we focus on monic polynomials without constant term. The cardinalities of the new quotient rings coincide with the required ones but are divided by $q(q-1)$. This is due to the fact that, if $f \in \mathcal{P}_q$, then $af + b \in \mathcal{P}_q$ for all $a, b \in \mathbb{F}_q$, with $a \neq 0$. Based on this algebraic geometry procedure, we show in Table 1 the number of polynomials in $\mathcal{P}_{q,d}$, with $q \leq 13$. (Note that the number of polynomials in $\mathcal{P}_8$ having degree less than six is 5,376, which differs from the value 5,368 indicated in [25]. The remaining values for the number of polynomials having degree less than $q-2$, for $q \leq 11$, coincide with those indicated in that paper.)

Table 1 Explicit values for $N_q(d)$.

q	d	$N_q(d)$	q	d	$N_q(d)$
4	1	12	11	1	110
	2	12		3	1,210
5	1	20		6	29,040
	3	100		7	272,250
7	1	42		8	3,332,340
	4	588		9	36,281,850
	5	4,410	13	1	156
8	1	56		5	38,532
	2	56		7	233,220
	3	448		8	2,798,640
	4	1,232		9	33,948,720
	5	3,584	10		442,144,560
	6	34,944	11		5,747,856,972
9	1	72			
	3	360			
	5	1,944			
	6	39,744			
	7	320,760			

The algebraic method described in Lemma 3.1, Lemma 3.2 and Remark 3.1 can be conveniently adapted to identify particular families of Latin squares, which in turn give rise to equivalent families of LPPs. As an illustrative example, we describe here the ideals associated with symmetric LPPs and reduced LPPs. First, let $\mathcal{SLP}_q$ and $\mathcal{SLP}_{q,d}$ denote, respectively, the subsets of symmetric polynomials in $\mathcal{LP}_q$ and $\mathcal{LP}_{q,d}$. Recall here that a polynomial $f \in \mathbb{F}_q[x, y]$ is called *symmetric* if $f(x, y) = f(y, x)$. Then, the next result holds readily from Lemmas 3.1 and 3.2.

Proposition 3.3 *The algebraic set of the zero-dimensional radical ideal*

$$\mathcal{J}_q + \langle x_{ij} - x_{ji} : 0 \leq i < j \leq q-2 \rangle \subset \mathbb{F}_q[\overline{X}_q].$$

If $\mathcal{J}_q$ is replaced by $\mathcal{J}_{q,d}$, then the resulting zero-dimensional radical ideal is identified with $\mathcal{SLP}_{q,d}$.

Furthermore, the notion of reduced Latin squares readily translates to LPPs as follows. Recall here that a Latin square $L \in \mathcal{L}_q$ is called *reduced* if $L[a, 0] = L[0, a] = a$ for all $a \in \mathbb{F}_q$.

Definition 3.1 *A polynomial $f \in \mathcal{LP}_q$ is called reduced if $f(x, 0) = x$ and $f(0, y) = y$. This is equivalent to say that*

$$f = g \cdot xy + x + y, \quad (9)$$

for some $g \in \mathbb{F}_q[x, y]$. We denote by $\mathcal{RLP}_q$ the subset of reduced polynomials in $\mathcal{LP}_q$.

This definition is justified by fact that a polynomial $f \in \mathcal{RLP}_q$ if and only if the Latin square L_f is reduced. Then, the next result holds readily from the equivalent relation among Latin squares

Lemma 3.3 *The number of local permutation polynomials over $\mathbb{F}_q$ is*

$$|\mathcal{LP}_q| = q! \cdot (q-1)! \cdot |\mathcal{RLP}_q|.$$

From (1), (2) and (9), the only reduced polynomial in both $\mathcal{RLP}_2$ and $\mathcal{RLP}_3$ is $x + y$. For $q > 3$, the next result holds readily from Lemma 3.1 and Definition 3.1.

Proposition 3.4 *The algebraic set of the zero-dimensional radical ideal*

$$\mathcal{J}_q + \langle x_{00}, x_{10} - 1, x_{01} - 1 \rangle + \langle x_{0i}, x_{i0} : 2 \leq i \leq q-2 \rangle \subset \mathbb{F}_q[\overline{X}_q].$$

is identified with the set $\mathcal{RLP}_q$. If $\mathcal{J}_q$ is replaced by $\mathcal{J}_{q,d}$, then the resulting zero-dimensional radical ideal is identified with $\mathcal{RLP}_{q,d}$.

Based on our algebraic approach, we show in Table 2 the cardinality of the sets $\mathcal{LP}_{q,d}$, $\mathcal{SLP}_{q,d}$ and $\mathcal{RLP}_{q,d}$ for $q \in \{4, 5\}$. As an illustrative example, we detail this procedure to characterize all polynomials in $\mathcal{SLP}_4$ and $\mathcal{RLP}_4$.

Theorem 3.2 *Every polynomial in $\mathcal{SLP}_4$ is of the form*

$$(s_{22}xy + s_{21}(x+y) + s_{11})xy + s_{20}(x^2 + y^2) + s_{10}(x+y) + s_{00},$$

with $s_{22}, s_{21}, s_{20}, s_{10}, s_{00} \in \mathbb{F}_4$ satisfying the next five constraints.

$$\begin{cases} s_{10}^3 + s_{20}^3 = 1, \\ s_{11}(s_{22}^3 + 1) = 0, \\ s_{21}(s_{22}^3 + 1) = 0, \\ s_{20}s_{21} + s_{10}s_{22} + s_{22}^2 = 0, \\ s_{11}s_{21} + s_{22}^2 = 0. \end{cases}$$

Table 2 Cardinality of $\mathcal{LP}_{q,d}$.

q	d	$ \mathcal{LP}_{q,d} $	$ \mathcal{SLP}_{q,d} $	$ \mathcal{RLP}_{q,d} $
4	1	36	12	1
	2	108	12	0
	4	432	72	3
5	1	80	20	1
	3	3,200	200	0
	5	22,000	100	19
	6	135,920	400	36

Proof The reduced Gröbner basis of the ideal described in Proposition 3.3 for $q = 4$, with respect to the lexicographical order, is formed by the following 16 generators.

$$\begin{aligned}
& x_{12} + x_{21}, & x_{02} + x_{20}, & x_{01} + x_{10}, & x_{10}x_{20}, & x_{11}^2 + x_{21}x_{22}, \\
& x_{21}^2 + x_{11}x_{22}, & x_{11}x_{21} + x_{22}^2, & x_{11}(x_{22}^3 + 1), & x_{21}(x_{22}^3 + 1), & x_{10}^3 + x_{20}^3 + 1, \\
& x_{10}x_{21}(x_{10} + x_{22}), & x_{10}x_{22}(x_{10} + x_{22}), & x_{20}x_{21} + x_{10}x_{22} + x_{22}^2, \\
& x_{11}x_{20} + x_{10}x_{21} + x_{21}x_{22}, & x_{10}x_{11} + x_{11}x_{22} + x_{20}x_{22}, & x_{22}(x_{20}^2 + x_{10}x_{21} + x_{21}x_{22}).
\end{aligned}$$

Their zeros give rise to the constraints of the statement. $\square$

Theorem 3.3 *Every polynomial in $\mathcal{RLP}_4$ is of the form*

$$(a^3xy + a(x+y) + a^2)xy + x + y \in \mathbb{F}_4[x, y] \quad (10)$$

with $a \in \mathbb{F}_4$. If $a = 0$, then we get the polynomial $x + y \in \mathcal{LP}_{4,1}$. If $a \neq 0$, then we get three reduced polynomials in $\mathcal{LP}_{4,4}$. Moreover, if u denotes a primitive element of $\mathbb{F}_4$, with minimum polynomial $u^2 + u + 1$, then all the four reduced Latin squares in $\mathcal{L}_4$ are represented by the following array.

0	1	u	u^2
1	$a^3 + a^2$	$(a^3 + 1)u^2 + a^2u + a$	$(a^3 + 1)u + a^2u^2 + a$
u	$(a^3 + 1)u^2 + a^2u + a$	$a^3u + a^2u^2$	$(a + 1)^3$
u^2	$(a^3 + 1)u + a^2u^2 + a$	$(a + 1)^3$	$a^3u^2 + a^2u$

Proof The reduced Gröbner basis of the ideal described in Proposition 3.4 for $q = 4$, with respect to the lexicographical order, is the set

$$\{x_{22}^2 + x_{22}, x_{21}(x_{22} + 1), x_{21}^3 + x_{22}, x_{20}, x_{12} + x_{21}, x_{11} + x_{21}^2, x_{10} + 1, x_{02}, x_{01} + 1, x_{00}\}.$$

Then, the result follows readily from the zeros of these generators. $\square$

It is clear that the constraints satisfied by the coefficients of any polynomial in $\mathcal{P}_q$, $\mathcal{LP}_q$ or $\mathcal{RLP}_q$ become much more convoluted as the order q increases. Determining them from this algebraic approach becomes even harder because, as we have already mentioned in the introductory section, the calculation of Gröbner bases is extremely sensitive to the number of variables and the length and degree of the generators. In any case, it becomes much easier when some kind of symmetry is imposed in the polynomials under consideration. The next section delves into this aspect by translating the notions of isotopism of Latin square to the context of LPPs.

4 Isotopisms of LPPs

In the preliminary section, we have shown how isotopisms play a relevant role in studying the symmetries of a Latin square. This notion is naturally translated to quasigroups (see [37]) and hence to LPPs. This section focuses on this last aspect. Previously, we introduce some notation concerning the composition of PPs and LPPs.

Since every polynomial in $\mathcal{P}_q$ acts as a permutation on $\mathbb{F}_q$, the composition of two polynomials $f, g \in \mathcal{P}_q$ is the polynomial

$$fg := f(g(x)) \in \mathcal{P}_q \quad (11)$$

where the composition is performed modulo $x^q - x$. In particular, the inverse of a polynomial $f \in \mathcal{P}_q$ is the unique polynomial $f^{-1} \in \mathcal{P}_q$ such that $ff^{-1} = f^{-1}f = x$. Furthermore, if $f \in \mathcal{LP}_q$ and $g, h \in \mathcal{P}_q$, then we define the polynomials

$$f[g, h] := f(g(x), h(y)) \in \mathcal{LP}_q \quad (12)$$

and

$$gf := g(f(x, y)) \in \mathcal{LP}_q, \quad (13)$$

where the compositions are performed modulo $x^q - x$ and $y^q - y$. Here, we use the bracket notation in (12) to avoid confusion, because we have, for example, $f[x, x] := f(x, y)$. In addition, by abuse of notation, we assume that both the polynomial h in (12) and the polynomial g in (13) can act on the variable y even if $g, h \in \mathbb{F}_q[x]$. Both products (12) and (13) were already considered by Mullen [4] and Lee and Ko [10] to construct LPPs. The last two authors raised a multivariate version of the following problem.

Problem 4.1 *Find some polynomial in $\mathcal{LP}_q$ that cannot be constructed from a polynomial with separate variables (that is, a polynomial $h_1(x) + h_2(y) \in \mathcal{LP}_q$, with $h_1, h_2 \in \mathcal{P}_q$) and the application of the products (12) and (13).*

In what follows, we show how this question is related to the notion of isotopism of Latin squares, which is readily translated to LPPs as follows.

Definition 4.1 *A polynomial $f \in \mathcal{LP}_q$ is said to be isotopic to a polynomial $g \in \mathcal{LP}_q$ if*

$$g[h_1, h_2] = h_3 f \quad (14)$$

for some $h_1, h_2, h_3 \in \mathcal{P}_q$. The triple (h_1, h_2, h_3) is an isotopism from f to g . This is principal if $h_3 = x$. If this is the case, then f and g are said to be principal isotopic. Furthermore, if $h_1 = h_2 = h_3$, then we get an isomorphism from f to g , which are then said to be isomorphic.

These notions are justified by the next result, which holds from (4) and (14).

Lemma 4.1 *Two polynomials $f, g \in \mathcal{LP}_q$ are (principal) isotopic (respectively, isomorphic) if and only if their associated Latin squares $L_f, L_g \in \mathcal{L}_q$ are (principal) isotopic (respectively, isomorphic).*

Since every polynomial in $\mathcal{P}_q$ acts as a permutation on $\mathbb{F}_q$, it is readily verified that being isotopic is an equivalence relation among LPPs. This allows their distribution in *isotopism classes*. A relevant isotopism class of LPPs is that one containing the linear polynomial $x + y$. In order to deal with this class, we introduce here the notion of *isolinearity*.

Definition 4.2 *An LPP is called isolinear if it is isotopic to $x + y$. Otherwise, it is called non-isilinear.*

The next lemma characterizes the isolinear polynomials in $\mathcal{LP}_q$. Then, the subsequent proposition shows that the polynomial sought in Problem 4.1 is any non-isilinear.

Lemma 4.2 *A polynomial $f \in \mathcal{LP}_q$ is isolinear if and only if*

$$f := f(x, y) = h_3(h_1(x) + h_2(y))$$

for some polynomials $h_1, h_2, h_3 \in \mathcal{P}_q$. In particular, every LPP with separate variables is isolinear.

Proof The result holds readily from Definitions 4.1 and 4.2. Then, the consequence follows once we consider the trivial permutation $h_3 = x$. $\square$

Proposition 4.1 *An LPP is a solution of Problem 4.1 if and only if it is non-isilinear.*

Proof On the one hand, if $f \in \mathcal{LP}_q$ is a polynomial with separate variables, then the product $f[g, h] \in \mathcal{LP}_q$ defined in (12) is also a polynomial with separate variables. On the other hand, Lemma 4.2 implies that applying the product (13) to a polynomial with separate variables gives rise to an isolinear polynomial. Then, the result holds from the fact that applying the products (12) and (13) to an isolinear polynomial gives rise to an isotopic polynomial. $\square$

The next result deals with the isolinear polynomials in $\mathcal{LP}_q$, with $q \in \{2, 3, 4\}$.

Proposition 4.2 *Every polynomial in $\mathcal{LP}_2$ and $\mathcal{LP}_3$ is isolinear. Moreover, a polynomial in $\mathcal{LP}_4$ is isolinear if and only if it belongs to the set $\mathcal{LP}_{4,1} \cup \mathcal{LP}_{4,2}$ described in Theorem 3.1.*

Proof From (1), (2) and (6), every polynomial in any of the sets $\mathcal{LP}_2$, $\mathcal{LP}_3$ and $\mathcal{LP}_{4,2}$ have separate variables. Hence, the first statement and the sufficient condition of the second one follow readily from Lemma 4.2. In order to prove the necessary condition, let $f \in \mathcal{LP}_4$ be isolinear. From Lemma 4.2, there exist three polynomials $h_1, h_2, h_3 \in \mathcal{P}_q$ such that $f = h_3(h_1(x) + h_2(y))$. In addition, Proposition 3.1 implies that $h_3 = s_2x^2 + x_1 + s_0$ for some $s_0, s_1, s_2 \in \mathbb{F}_4$ such that $s_1^3 + s_2^3 = 1$. Thus, since the base field has characteristic two,

$$f = s_2(h_1^2(x) + h_2^2(y)) + s_1(h_1(x) + h_2(y)) + s_0.$$

That is, f has separate variables, and hence, $f \in \mathcal{LP}_{4,2}$. $\square$

The equivalence among isotopisms of Latin squares and LPPs allows for the translation of known results of the former to the latter. In this regard, the next result readily follows from Lemma 4.1 and the fact that every Latin square is principal isotopic to a reduced Latin square by a convenient permutation of its rows and columns.

Proposition 4.3 *Every LPP is principal isotopic to a reduced LPP.*

This result plays a relevant role in describing all polynomials in $\mathcal{LP}_q$ from those in $\mathcal{P}_q$ and $\mathcal{RLP}_q$. The following theorem illustrates this fact for $q = 4$. It follows readily from Proposition 4.3, together with Proposition 3.1 and (10).

Theorem 4.1 *Every polynomial in $\mathcal{LP}_4$ is of the form $f[h, h']$, where*

$$\begin{cases} f := (a^3xy + a(x+y) + a^2)xy + x + y \in \mathcal{RLP}_4, \\ h := bx^2 + cx + d \in \mathcal{LP}_4, \\ h' := b'x^2 + c'x + d' \in \mathcal{LP}_4. \end{cases}$$

Here, $b^3 + c^3 = 1 = b'^3 + c'^3$.

Proposition 4.3 also facilitates the distribution of LPPs into isotopism classes. To do it, we associate each LPP under consideration with a reduced LPP to which the former is principal isotopic. Then, we prove whether the resulting polynomials are isotopic. The following result proposes a construction in this regard.

Proposition 4.4 *Let $f \in \mathcal{LP}_q$ and $a, b \in \mathbb{F}_q$ be such that $f(a, b) = 0$. Then, f is principal isotopic to the reduced polynomial*

$$\rho_{f,a,b} := f[p_{a,b} + a, q_{a,b} + b] \in \mathcal{RLP}_q,$$

where $p_{f,a,b} := (f(x+a, b))^{-1} \in \mathcal{P}_q$ and $q_{f,a,b} := (f(a, x+b))^{-1} \in \mathcal{P}_q$.

Proof Definition 4.1 ensures that ρ_f is principal isotopic to f by means of the principal isotopism $(p_{f,a,b}(x) + a, q_{f,a,b}(x) + b, x) \in \mathcal{P}_q \times \mathcal{P}_q \times \mathcal{P}_q$. Now, we prove that ρ_f is reduced. Developing in powers of x and y , we have

$$f(x+a, y+b) = xyh(x, y) + f(x+a, b) + f(a, y+b)$$

for some polynomial $h \in \mathbb{F}_q[x, y]$. Then,

$$\rho_{f,a,b} = p_{f,a,b}(x)q_{f,a,b}(y)h(p_{f,a,b}(x), q_{f,a,b}(y)) + x + y.$$

This is a reduced a polynomial, because $p_{f,a,b}(0) = q_{f,a,b}(0) = 0$ and hence, $x|p_{f,a,b}(x)$ and $y|q_{f,a,b}(y)$. $\square$

The following result illustrates this procedure by showing that every polynomial in the subset $\mathcal{LP}_{4,4} \subset \mathcal{LP}_4$ described in Theorem 3.1 belongs to the same isotopism class. Of course, this result holds readily from Lemma 4.1, Proposition 4.2 and the fact that $\mathcal{L}_4$ has exactly two isotopism classes. Nevertheless, in order to show the potential of our algebraic approach, we give an alternative proof based on Proposition 4.4.

Theorem 4.2 *Every polynomial in $\mathcal{LP}_{4,4}$ belongs to the same isotopism class.*

Proof From Proposition 3.1, every polynomial in $\mathcal{P}_4$ is of the form $ax + b$ or $ax^2 + b$, with $a \in \mathbb{F}_4 \setminus \{0\}$ and $b \in \mathbb{F}_4$. In the first case, its compositional inverse is $a^2(x+b)$. Otherwise, it is $a(x+b)^2$. From (7) and (8), every polynomial in $\mathcal{LP}_{4,4}$ is of the form

$$f_1 := (axy + bx + cy + a^2bc)xy + ab^2cx + abc^2y + d,$$

$$\begin{aligned} f_2 &:= (axy + bx + cy + a^2bc)xy + ab^2cx + a^2c^2y^2 + d, \\ f_3 &:= (axy + bx + cy + a^2bc)xy + a^2b^2x^2 + abc^2y + d, \end{aligned}$$

or

$$f_4 := (axy + bx + cy + a^2bc)xy + a^2b^2x^2 + a^2c^2y^2 + d,$$

with $a, b, c \in \mathbb{F}_4 \setminus \{0\}$ and $d \in \mathbb{F}_4$. For each positive integer $i \leq 4$, let $a_i \in \mathbb{F}_4$ be such that $f_i(a_i, 0) = 0$. That is, $a_1 = a_2 = a^2bc^2d$ and $a_3 = a_4 = a^2b^2d^2$. Then,

$$p_{f_i, a_i, 0} := (f_i(x + a_i, 0))^{-1} = \begin{cases} a^2bc^2x, & \text{if } i \in \{1, 2\}, \\ a^2b^2x^2, & \text{if } i \in \{3, 4\}. \end{cases}$$

In addition,

$$\begin{aligned} f_i(a_i, x) &= \begin{cases} a^2bd(bcd + 1)x^2 + a(b^2d + bc^2 + cd^2)x, & \text{if } i \in \{1, 3\}, \\ a^2(b^2cd^2 + bd + c^2)x^2 + ad(b^2 + cd)x, & \text{if } i \in \{2, 4\}. \end{cases} \\ &= \begin{cases} abc^2x, & \text{if } \begin{cases} i \in \{1, 3\} \text{ and } d = bcd^2, \\ i \in \{2, 4\} \text{ and } bcd(bcd + 1) = 1, \end{cases} \\ a^2c^2x^2, & \text{if } \begin{cases} i \in \{1, 3\} \text{ and } bcd(bcd + 1) = 1, \\ i \in \{2, 4\} \text{ and } d = bcd^2. \end{cases} \end{cases} \end{aligned}$$

Hence,

$$q_{f_i, a_i, 0} := (f_i(a_i, x))^{-1} = \begin{cases} a^2b^2cy, & \text{if } \begin{cases} i \in \{1, 3\} \text{ and } d = bcd^2, \\ i \in \{2, 4\} \text{ and } bcd(bcd + 1) = 1, \end{cases} \\ a^2c^2y^2, & \text{if } \begin{cases} i \in \{1, 3\} \text{ and } bcd(bcd + 1) = 1, \\ i \in \{2, 4\} \text{ and } d = bcd^2. \end{cases} \end{cases}$$

In any case,

$$\rho_{f_i, a_i, 0} := (xy + b^2c^2(x + y) + bc)xy + x + y$$

Every polynomial in $\mathcal{LP}_{4,4}$ is therefore principal isotopic to a reduced polynomial

$$g_\alpha := (xy + \alpha(x + y) + \alpha^2)xy + x + y \in \mathcal{LP}_{4,4},$$

with $\alpha \in \mathbb{F}_4 \setminus \{0\}$. Particularly, if $\alpha \neq 1$, then g_α is isomorphic to g_1 by means of the polynomial $h_\alpha = \alpha x^2$, because

$$g_\alpha(h_\alpha, h_\alpha) = \alpha \left((xy + x + y + 1)xy + x^2 + y^2 \right) = h_\alpha(g_1).$$

As a consequence, every polynomial in $\mathcal{LP}_{4,4}$ is isotopic to g_1 . $\square$

Theorem 4.2 can be directly proved by defining an isotopism from each of the four polynomials $f_1, f_2, f_3, f_4 \in \mathcal{LP}_{4,4}$ to the polynomial $g_1 \in \mathcal{LP}_{4,4}$, all of them described in the previous proof. In this regard, it is straightforward to see that

$$f_i(a^2cx^{e_i}, a^2by^{f_i}) = b^2c^2g_1(x, y) + d$$

for each positive integer $i \leq 4$, where

$$(e_1, f_1) = (1, 1), \quad (e_2, f_2) = (1, 2), \quad (e_3, f_3) = (2, 1) \quad \text{and} \quad (e_4, f_4) = (2, 2).$$

The next result is an immediate consequence of Proposition 4.2 and Theorem 4.2.

Corollary 4.1 *The set $\mathcal{LP}_4$ is formed by two isotopism classes, which are respectively described by the sets $\mathcal{LP}_{4,2}$ and $\mathcal{LP}_{4,4}$ defined in Theorem 3.1.*

5 Complete mappings of LPPs

We finish our study by dealing with the natural translation to LPPs of complete mappings and orthomorphisms of quasigroups, showing their relationship with transversals and isotopisms of Latin squares. First, for each polynomial $f \in \mathcal{LP}_q$ and any pair of polynomials $g_1, g_2 \in \mathcal{P}_q$, we define the polynomial

$$\odot_f(g_1, g_2) := f(g_1(x), g_2(x)) \in \mathbb{F}_q[x], \quad (15)$$

where the composition is performed modulo $x^q - x$. This notation follows from the definition of the Hadamard quasigroup product described in (3). The following preliminary result describes the relationship among the compositions described in (11–13) and (15).

Lemma 5.1 *Let $f \in \mathcal{LP}_q$ and $g_1, g_2, h_1, h_2, h \in \mathcal{P}_q$. The following statements hold.*

1. *If $h_1, h_2 \in \mathcal{P}_q$, then*

$$\odot_{f[g_1, g_2]}(h_1, h_2) = \odot_f(g_1 h_1, g_2 h_2).$$

2. *If $h \in \mathcal{P}_q$, then*

$$h \odot_f(g_1, g_2) = \odot_{hf}(g_1, g_2)$$

and

$$\odot_f(g_1, g_2)h = \odot_f(g_1 h, g_2 h).$$

Proof Let $a \in \mathbb{F}_q$. The first statement holds because

$$\begin{aligned} \odot_{f[g_1, g_2]}(h_1, h_2)(a) &= f[g_1, g_2](h_1(a), h_2(a)) = f(g_1(h_1(a)), g_2(h_2(a))) = \\ &= f(g_1 h_1(a), g_2 h_2(a)) = \odot_f(g_1 h_1, g_2 h_2)(a). \end{aligned}$$

The second statement holds because

$$\begin{aligned} h \odot_f(g_1, g_2)(a) &= h(\odot_f(g_1, g_2)(a)) = h(f(g_1(a), g_2(a))) = \\ &= hf(g_1(a), g_2(a)) = \odot_{hf}(g_1, g_2)(a) \end{aligned}$$

and

$$\odot_f(g_1, g_2)h(a) = \odot_f(g_1, g_2)(h(a)) = f(g_1(h(a)), g_2(h(a))) = \odot_f(g_1 h, g_2 h)(a).$$

□

The next result establishes when $\odot_f(g_1, g_2) \in \mathcal{P}_q$ by means of the transversals of the Latin square $L_f \in \mathcal{L}_q$. It constitutes the natural translation to LPPs of Lemma 4.2 in [35].

Lemma 5.2 *Let $f \in \mathcal{LP}_q$ and $g_1, g_2 \in \mathcal{P}_q$. Then, $\odot_f(g_1, g_2) \in \mathcal{P}_q$ if and only if the subset*

$$\{(g_1(a), g_2(a), \odot_f(g_1, g_2)(a))\} \subset \text{Ent}(L_f)$$

is a transversal of L_f .

Proof The polynomial $\odot_f(g_1, g_2)$ is permutational if and only if, for each pair of distinct elements $a, b \in \mathbb{F}_q$,

$$L_f[g_1(a), g_2(a)] = \odot_f(g_1, g_2)(a) \neq \odot_f(g_1, g_2)(b) = L_f[g_1(b), g_2(b)].$$

Then, the result follows readily from the fact that $g_1, g_2 \in \mathcal{P}_q$. $\square$

The case $g_1 = x$ generalizes for LPPs both notions of complete mapping and orthomorphism of quasigroups, which were recalled in the preliminary section. From Lemma 5.2, and similarly to quasigroups (see Lemma 2.1), they are equivalent to transversals of Latin squares.

Definition 5.1 *Let $f \in \mathcal{LP}_q$. A polynomial $g \in \mathcal{P}_q$ is called a complete mapping of f if $\odot_f(x, g) \in \mathcal{P}_q$. This last polynomial is called an orthomorphism of f .*

The next result shows the relationship among the complete mappings of two isotopic LPPs.

Proposition 5.1 *There is a one-to-one correspondence between the sets of complete mappings of any pair of isotopic LPPs. More precisely, if (h_1, h_2, h_3) is an isotopism from a polynomial $f_1 \in \mathcal{LP}_q$ to a polynomial $f_2 \in \mathcal{LP}_q$, then $g \in \mathcal{P}_q$ is a complete mapping of f_1 if and only if $h_2gh_1^{-1} \in \mathcal{P}_q$ is a complete mapping of f_2 .*

Proof Let $g \in \mathcal{P}_q$. From (14) and Lemma 5.1, we have

$$h_3 \odot_{f_1}(x, g) = \odot_{h_3f_1}(x, g) = \odot_{f_2[h_1, h_2]}(x, g) = \odot_{f_2}(h_1, h_2g) = \odot_{f_2}(x, h_2gh_1^{-1})h_1.$$

Then, the result holds because we have from (11) that

$$\odot_{f_1}(x, g) \in \mathcal{P}_q \Leftrightarrow \odot_{f_2}(x, h_2gh_1^{-1})h_1 = h_3 \odot_{f_1}(x, g) \in \mathcal{P}_q \Leftrightarrow \odot_{f_2}(x, h_2gh_1^{-1}) \in \mathcal{P}_q.$$

$\square$

This last result, together with Proposition 4.3, implies that determining all complete mappings in $\mathcal{LP}_q$ is derived from those of a reduced LPP of each isotopism class. We illustrate this procedure for $q = 4$.

Theorem 5.1 *Each polynomial in $\mathcal{LP}_{4,2}$ has eighth complete mappings, whereas no complete mapping exists for any polynomial in $\mathcal{LP}_{4,4}$.*

Proof We consider the reduced polynomials

$$f_1 := x + y \in \mathcal{LP}_{4,2} \quad \text{and} \quad f_2 := (xy + x + y + 1)xy + x + y \in \mathcal{LP}_{4,4}.$$

We also consider a polynomial $g := s_2x^2 + s_1x + s_0 \in \mathcal{P}_4$. Then,

$$\odot_{f_1}(x, g) = s_2x^2 + (s_1 + 1)x + s_0$$

and

$$\odot_{f_2}(x, g) = (s_2^2 + s_1^2 + s_2 + s_1)x^3 + (s_2^2 + s_0^2 + s_2 + s_1 + s_0)x^2 + (s_1^2 + s_0^2 + s_2 + s_1 + s_0 + 1)x + s_0.$$

From Proposition 3.1,

$$g \in \mathcal{P}_4 \Leftrightarrow s_2^3 + s_1^3 = 1.$$

Then, the same result also implies that

$$\odot_{f_1}(x, g) \in \mathcal{P}_4 \Leftrightarrow \begin{cases} s_2^3 + s_1^3 = 1, \\ s_2^3 + (s_1 + 1)^3 = 1. \end{cases} \Leftrightarrow \begin{cases} s_2 = 0, \\ s_1^2 + s_1 = 1. \end{cases}$$

and

$$\begin{aligned} \odot_{f_2}(x, g) \in \mathcal{P}_4 &\Leftrightarrow \begin{cases} s_2^3 + s_1^3 = 1, \\ s_2^2 + s_1^2 + s_2 + s_1 = 0, \\ (s_2^2 + s_0^2 + s_2 + s_1 + s_0)^3 + (s_1^2 + s_0^2 + s_2 + s_1 + s_0 + 1)^3 = 1. \end{cases} \\ &\Leftrightarrow \begin{cases} s_2^3 + s_1^3 = 1, \\ s_2^2 + s_1^2 + s_2 + s_1 = 0, \\ s_1^3 + s_2 = 0. \end{cases} \end{aligned}$$

This last system of equations has no solution, so there is no complete mapping of f_2 . Then, the result follows straightforwardly from Proposition 5.1 and Corollary 4.1. $\square$

We finish our study by dealing with the generalization of the product (15) to

$$\odot_f(g_1, g_2) := f(g_1(x, y), g_2(x, y)) \in \mathbb{F}_q[x, y],$$

with $f, g_1, g_2 \in \mathcal{LP}_q$. In the context of Latin squares, this is equivalent to the Hadamard quasigroup product described in [34]. Lee and Ko already asked in [10] if $\odot_f(g_1, g_2) \in \mathcal{LP}_q$. They showed that this condition holds whenever f, g_1 and g_2 are of degree at most two. In addition, they proved in [10, Theorem 8] that ax is a complete mapping of f for some $a \in \mathbb{F}_q \setminus \{0\}$ if and only if $\odot_f(g_1, ag_1) \in \mathcal{LP}_q$. Here, $ag_1 := a \cdot g_1(x, y)$. More generally, the following result constitutes the natural translation to LPPs of Lemma 12 in [34]. It follows readily from Lemma 5.2.

Proposition 5.2 *Let $f, g_1, g_2 \in \mathcal{LP}_q$. Then, $\odot_f(g_1, g_2) \in \mathcal{LP}_q$ if and only if, for each $a \in \mathbb{F}_q$, both subsets*

$$\{(g_1(a, b), g_2(a, b), \odot_f(g_1, g_2)(a, b)) : b \in \mathbb{F}_q\} \subset \text{Ent}(L_f)$$

and

$$\{(g_1(b, a), g_2(b, a), \odot_f(g_1, g_2)(b, a)) : b \in \mathbb{F}_q\} \subset \text{Ent}(L_f)$$

are transversals of L_f .

6 Conclusion and further work

Despite the natural translation among local permutation polynomials in two variables and the set of Latin squares, there are only some preliminary results in the literature concerning this subject. This paper has delved into this topic by emphasizing how a given family of Latin squares can be represented by a single polynomial. We have described an algebraic geometry procedure to identify the constraints satisfied by the coefficients of this polynomial, and we have shown how this procedure facilitates the enumeration and classification of Latin squares, together with the study of some of their properties. We have also introduced the natural translation to LPPs of some classical notions in the theory of Latin squares like isotopisms, complete mappings and orthomorphisms. We have illustrated all these aspects for LPPs over $\mathbb{F}_4$.

Similarly to Latin squares, which can also be distributed into conjugate and main classes, a comprehensive study is required concerning the natural translation to LPPs of conjugation and paratopisms of Latin squares, which we introduce just here.

Definition 6.1 *Two polynomials $f, g \in \mathcal{LP}_q$ are called conjugate if one of the following six identities holds.*

1. $g(x, y) = f(x, y)$.
2. $g(x, y) = f(y, x)$.
3. $g(x, f(x, y)) = y$.
4. $g(f(x, y), x) = y$.
5. $g(f(x, y), y) = x$.
6. $g(y, f(x, y), x) = x$.

If all the six identities hold for $f = g$, then the polynomial f is called totally symmetric.

All the notions and results considered in this paper may naturally be generalized to LPPs in more variables, which are equivalent to multiary quasigroups and Latin hypercubes. Some preliminary results on this topic have already been described in [6, 11–14], but a comprehensive study is required in this regard.

References

- [1] Lidl, R., Niederreiter, H.: Finite Fields, 2nd edn. Encyclopedia of Mathematics and its Applications, vol. 20, p. 755. Cambridge University Press, Cambridge (1997)
- [2] Hou, X.-d.: Permutation polynomials over finite fields—a survey of recent advances. *Finite Fields Appl.* **32**, 82–119 (2015) <https://doi.org/10.1016/j.ffa.2014.10.001>
- [3] Shcherbacov, V.: Elements of Quasigroup Theory and Applications. Monographs and Research Notes in Mathematics, p. 576. CRC Press, Boca Raton, FL (2017). <https://doi.org/10.1201/9781315120058>
- [4] Mullen, G.L.: Local permutation polynomials over finite fields. *Det Kong. Norske Vid. Selskab, Series Skrifter*, 1:1–4, 1981. **1**, 1–4 (1981)
- [5] Mullen, G.L.: Local permutation polynomials over Z_p . *Fibonacci Quart.* **18**(2), 104–108 (1980)
- [6] Mullen, G.L.: Local permutation polynomials in three variables over Z_p . *Fibonacci Quart.* **18**(3), 208–214 (1980)
- [7] Hulpke, A., Kaski, P., Östergård, P.R.J.: The number of Latin squares of order 11. *Math. Comp.* **80**(274), 1197–1219 (2011) <https://doi.org/10.1090/S0025-5718-2010-02420-2>

- [8] Kolesova, G., Lam, C.W.H., Thiel, L.: On the number of 8×8 Latin squares. *J. Combin. Theory Ser. A* **54**(1), 143–148 (1990) [https://doi.org/10.1016/0097-3165\(90\)90015-O](https://doi.org/10.1016/0097-3165(90)90015-O)
- [9] McKay, B.D., Meynert, A., Myrvold, W.: Small Latin squares, quasigroups, and loops. *J. Combin. Des.* **15**(2), 98–119 (2007) <https://doi.org/10.1002/jcd.20105>
- [10] Lee, J.B., Ko, H.J.: Permutation polynomials over finite fields. *Com. Korean Math. Soc.* **9**(3), 539–545 (1994)
- [11] Diestelkamp, W.S., Hartke, S.G., Kenney, R.H.: On the degree of local permutation polynomials. *J. Combin. Math. Combin. Comput.* **50**, 129–140 (2004)
- [12] Gutiérrez, J., Jiménez Urroz, J.: Local permutation polynomials and the action of e-Klenian groups. *Finite Fields Appl.* **91**, 102261–22 (2023) <https://doi.org/10.1016/j.ffa.2023.102261>
- [13] Gutiérrez, J., Jiménez Urroz, J.: Permutation and local permutation polynomials of maximum degree. *Afr. Mat.* **36**(1), 45–11 (2025) <https://doi.org/10.1007/s13370-025-01247-3>
- [14] Gutierrez, J., Jiménez Urroz, J.: Local permutation polynomials of maximum degree over prime finite fields. *Bull. Malays. Math. Sci. Soc.* **48**(2), 40–10 (2025) <https://doi.org/10.1007/s40840-025-01825-5>
- [15] Hasan, S.U., Kumar, H.: Local permutation polynomials and their companions. *Finite Fields Appl.* **109**, 102717–34 (2026) <https://doi.org/10.1016/j.ffa.2025.102717>
- [16] Hou, X.-d.: A survey of permutation binomials and trinomials over finite fields. In: *Topics in Finite Fields. Contemp. Math.*, vol. 632, pp. 177–191. Amer. Math. Soc., Providence, RI (2015). <https://doi.org/10.1090/conm/632/12628>
- [17] Jarali, V., Poojary, P., Bhatta, G.R.V.: A recent survey of permutation trinomials over finite fields. *AIMS Math.* **8**(12), 29182–29220 (2023) <https://doi.org/10.3934/math.20231495>
- [18] Tu, Z., Liu, X., Zeng, X.: A revisit to a class of permutation quadrinomials. *Finite Fields Appl.* **59**, 57–85 (2019) <https://doi.org/10.1016/j.ffa.2019.04.008>
- [19] Özbudak, F., Gülmez Temür, B.: Classification of some quadrinomials over finite fields of odd characteristic. *Finite Fields Appl.* **87**, 102158–15 (2023) <https://doi.org/10.1016/j.ffa.2022.102158>
- [20] Zhang, T., Zheng, L., Hao, X.: More classes of permutation hexanomials and pentanomials over finite fields with even characteristic. *Finite Fields Appl.* **91**, 102250–19 (2023) <https://doi.org/10.1016/j.ffa.2023.102250>

- [21] Mollin, R.A., Small, C.: On permutation polynomials over finite fields. *Internat. J. Math. Math. Sci.* **10**(3), 535–543 (1987) <https://doi.org/10.1155/S0161171287000644>
- [22] Lidl, R., Mullen, G.L.: Unsolved Problems: When Does a Polynomial Over a Finite Field Permute the Elements of the Field? *Amer. Math. Monthly* **95**(3), 243–246 (1988) <https://doi.org/10.2307/2323626>
- [23] Das, P.: The number of permutation polynomials of a given degree over a finite field. *Finite Fields Appl.* **8**(4), 478–490 (2002) <https://doi.org/10.1006/ffa.2002.0355>
- [24] Kim, K.Y., Kim, R., Kim, J.S.: On the number of permutation polynomials over a finite field. *Int. J. Number Theory* **12**(6), 1519–1528 (2016) <https://doi.org/10.1142/S1793042116500949>
- [25] Konyagin, S., Pappalardi, F.: Enumerating permutation polynomials over finite fields by degree. *Finite Fields Appl.* **8**(4), 548–553 (2002) <https://doi.org/10.1006/ffa.2002.0363>
- [26] Winterhof, A.: Generalizations of complete mappings of finite fields and some applications. *J. Symbolic Comput.* **64**, 42–52 (2014) <https://doi.org/10.1016/j.jsc.2013.12.006>
- [27] Cox, D.A., Little, J., O’Shea, D.: *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 4th edn. Undergraduate Texts in Mathematics, p. 646. Springer, Cham (2015). <https://doi.org/10.1007/978-3-319-16721-3>
- [28] Keedwell, A.D., Dénes, J.: *Latin Squares and Their Applications*, 2nd edn., p. 424. Elsevier, North-Holland, Amsterdam (2015)
- [29] Montgomery, R.: Transversals in Latin squares. In: *Surveys in Combinatorics 2024*. London Math. Soc. Lecture Note Ser., vol. 493, pp. 131–158. Cambridge Univ. Press, Cambridge (2024)
- [30] Wanless, I.M.: Transversals in Latin squares: a survey. In: *Surveys in Combinatorics 2011*. London Math. Soc. Lecture Note Ser., vol. 392, pp. 403–437. Cambridge Univ. Press, Cambridge (2011)
- [31] Kreuzer, M., Robbiano, L.: *Computational Commutative Algebra*. 1, p. 321. Springer, Berlin (2000). <https://doi.org/10.1007/978-3-540-70628-1>
- [32] Hashemi, A., Lazard, D.: Sharper complexity bounds for zero-dimensional Gröbner bases and polynomial system solving. *Internat. J. Algebra Comput.* **21**(5), 703–713 (2011) <https://doi.org/10.1142/S0218196711006364>

- [33] Decker, W., Greuel, G.-M., Pfister, G., Schönemann, H.: SINGULAR 4-4-1 — A computer algebra system for polynomial computations. <http://www.singular.uni-kl.de> (2025)
- [34] Falcón, R.M., Álvarez, V., Armario, J.A., Frau, M.D., Gudiel, F., Güemes, M.B.: A computational approach to analyze the Hadamard quasigroup product. *Electron. Res. Arch.* **31**(6), 3245–3263 (2023) <https://doi.org/10.3934/era.2023164>
- [35] Falcón, R.M., Mella, L., Vojtěchovský, P.: The Hadamard multiary quasigroup product. In: *Loops'23: Nonassociative Algebra*. Banach Center Publ., vol. 129, pp. 85–101. Inst. Math., Polish Acad. Sci., Warsaw (2025)
- [36] Niederreiter, H., Robinson, K.H.: Complete mappings of finite fields. *J. Austral. Math. Soc. Ser. A* **33**(2), 197–212 (1982) <https://doi.org/10.1017/S1446788700018346>
- [37] Albert, A.A.: Quasigroups. I. *Trans. Amer. Math. Soc.* **54**, 507–519 (1943) <https://doi.org/10.2307/1990259>
- [38] Bayer, D.A.: The Division Algorithm and the Hilbert Scheme, p. 163. ProQuest LLC, Ann Arbor, MI (1982). Thesis (Ph.D.)—Harvard University
- [39] Adams, W.W., Loustaunau, P.: An Introduction to Gröbner Bases. *Graduate Studies in Mathematics*, vol. 3, p. 289. American Mathematical Society, Providence, RI (1994). <https://doi.org/10.1090/gsm/003>
- [40] Falcón, R.M., Martín-Morales, J.: Gröbner bases and the number of Latin squares related to autotopisms of order ≤ 7 . *J. Symbolic Comput.* **42**(11-12), 1142–1154 (2007) <https://doi.org/10.1016/j.jsc.2007.07.004>
- [41] Falcón, R.M.: The set of autotopisms of partial Latin squares. *Discrete Math.* **313**(11), 1150–1161 (2013) <https://doi.org/10.1016/j.disc.2011.11.013>
- [42] Falcón, R.M.: Enumeration and classification of self-orthogonal partial Latin rectangles by using the polynomial method. *European J. Combin.* **48**, 215–223 (2015) <https://doi.org/10.1016/j.ejc.2015.02.022>
- [43] 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.* **41**(17), 7236–7262 (2018) <https://doi.org/10.1002/mma.4820>
- [44] Falcón, R.M., Stones, R.J.: Enumerating partial Latin rectangles. *Electron. J. Combin.* **27**(2), 2–4741 (2020) <https://doi.org/10.37236/9093>