Electronic Research Archive

http://www.aimspress.com/journal/era

ERA, 31(6): 3245–3263.
DOI: 10.3934/era.2023164
Received: 02 February 2023
Revised: 14 March 2023
Accepted: 28 March 2023
Published: 30 March 2023

Research article

A computational approach to analyze the Hadamard quasigroup product

Raúl M. Falcón*, Víctor Álvarez, José Andrés Armario, María Dolores Frau, Félix Gudiel and María Belén Güemes

Department of Applied Mathematics I, Universidad de Sevilla, Spain

* **Correspondence:** Email: rafalgan@us.es.

Abstract: Based on the binary product described by any Latin square, the Hadamard quasigroup product is introduced in this paper as a natural generalization of the classical Hadamard product of matrices. The successive iteration of this new product is endowed with a cyclic behaviour that enables one to define a pair of new isomorphism invariants of Latin squares. Of particular interest is the set of Latin squares for which this iteration preserves the Latin square property, which requires the existence of successive localized Latin transversals within the Latin square under consideration. In order to enumerate and classify, up to isomorphism, these Latin squares, we propose a computational algebraic geometry approach based on the computation of reduced Gröbner bases. To illustrate this point, we obtain the classification of the sought Latin squares, for order up to six, by using the open computer algebra system for polynomial computations Singular.

Keywords: Hadamard product; quasigroup; Latin square; Latin transversal; isomorphism; computer algebra system

1. Introduction

From now on, let $\mathcal{A}(n)$ denote the set of $n \times n$ arrays in which each cell contains a symbol in the set $[n] \cup \{\cdot\}$, where $[n] := \{1, \ldots, n\}$. The set of entries of any array $A \in \mathcal{A}(n)$ is the set $\mathrm{Ent}(A) := \{(i, j, A[i, j]) \colon i, j \in [n]\}$, where $A[i, j]$ denotes the symbol appearing in the cell (i, j) in A. Cells containing the symbol $\{\cdot\}$ are termed *empty*. The number of non-empty cells in the array A constitutes its *weight* $|A|$. Further, a *transversal* in the array A is any set of n cells containing exactly one cell per row and one cell per column. It is said to be a *Latin transversal* if all the n cells are non-empty and no two cells contain the same symbol.

An array $A \in \mathcal{A}(n)$ is a *partial Latin square* if each symbol in $[n]$ appears, at most, once per row, and, at most, once per column. If $|A| = n^2$, then it is a *Latin square*. That is, an $n \times n$ array such that each symbol in $[n]$ appears precisely once per row, and precisely once per column. This condition is usually known as the *Latin square property*. Every Latin square constitutes the multiplication table of a *quasigroup* $([n], *)$ of the same order. That is, the set $[n]$ is endowed with a binary operation $*$, so that both equations $i * x = j$ and $y * i = j$ have unique solutions $x, y \in [n]$, for all $i, j \in [n]$.

From now on, let $\mathcal{PL}(n)$ and $\mathcal{L}(n)$ respectively denote the subset of partial Latin squares and that of Latin squares in the set $\mathcal{A}(n)$. A partial Latin square $P \in \mathcal{PL}(n)$ is *completable* to a partial Latin square $Q \in \mathcal{PL}(n)$ if $\mathrm{Ent}(P) \cap [n]^3 \subseteq \mathrm{Ent}(Q)$. By abuse of notation, we denote this fact by $P \subseteq Q$. Further, let S_n be the symmetric group on the set $[n]$. Two (partial) Latin squares P, $P' \in \mathcal{PL}(n)$ are *isomorphic* if there exists a permutation $\pi \in S_n$ such that $P'[\pi(i), \pi(j)] = \pi(P[i, j])$, for all $i, j \in [n]$ such that $P[i, j] \in [n]$. In such a case, the permutation π is an *isomorphism* from P to P'. To be isomorphic is an equivalence relation among (partial) Latin squares. Currently, the number of isomorphism classes is only known for Latin squares of order up to eleven [1–3] and for partial Latin squares of order up to six [4]. Recently, the number of isomorphism classes has also been established [5,6] for some families of Latin squares of order up to 15. In order to deal with higher orders, new isomorphism invariants of (partial) Latin squares are being described in the recent literature [6–10]. This paper delves into this topic by focusing on the description and subsequent computational analysis of some new invariants resulting from a generalization of the Hadamard product of matrices.

Recall here that the *Hadamard product* of two $m \times n$ matrices A and B, with entries in a field $\mathbb{K}$, is the $m \times n$ matrix $A \odot B = (A[i, j] \cdot B[i, j])$, where $\cdot$ refers to the multiplication in $\mathbb{K}$. Our approach is based on a similar element-wise product on the set $\mathcal{A}(n)$ by means of the binary product described by a Latin square $L \in \mathcal{L}(n)$. It is formally introduced in Section 4 as the *Hadamard L-product*. The discrete structure of L endows the successive iteration of this product with a cyclic behaviour. Of particular interest is the characterization, construction and classification of those Latin squares for which this iteration always preserves the Latin square property. We prove that this condition requires the existence of successive localized Latin transversals within the Latin square under consideration. They can be identified with the algebraic set of a zero-dimensional radical ideal in a multivariate polynomial ring, which can explicitly be determined in turn from the computation of the reduced Gröbner basis of this ideal. In this paper, we compute this basis by using the open computer algebra system for polynomial computations Singular [11].

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. Then, in Section 3, we define three distinct zero-dimensional radical ideals in multivariate polynomial rings, whose algebraic sets can respectively be identified with: (a) the set of Latin squares to which a given partial Latin squares is completable; (b) a partial Latin square that results after filling the cells of a transversal with empty cells in a given partial Latin square; and (c) the set of isomorphisms between two given Latin squares. In Section 4, we describe the Hadamard quasigroup product and a pair of associated isomorphism invariants of Latin squares. Then, we characterize those Latin squares for which the successive iteration of the Hadamard quasigroup product is also a Latin square. In order to determine explicitly the set of these Latin squares, we describe an algorithm that is based on the computation of reduced Gröbner bases of the above ideals. Then, this algorithm is implemented in Singular to obtain the classification, up to isomorphism, of these Latin squares, for order up to six. Finally, since this work has a high dependence on notation, a Glossary of Symbols is shown at the end of the paper.

2. Preliminaries

In this section, we describe some basic concepts and results on partial Latin squares and computational algebraic geometry that are used throughout the paper. See [12, 13] for more details on both topics.

2.1. Partial Latin squares

A partial Latin square $P \in \mathcal{PL}(n)$ is *symmetric* if $P[i, j] = P[j, i]$, for all $i, j \in [n]$. It is *idempotent* if $P[i, i] = i$, for all $i \in [n]$. To be symmetric or idempotent are isomorphism invariants of Latin squares. Further, let $\mathcal{DPL}(n)$ denote the subset of partial Latin squares in $\mathcal{PL}(n)$ whose main diagonal is a Latin transversal. For each partial Latin square $P \in \mathcal{DPL}(n)$, let $\pi_P \in S_n$ be defined so that $\pi_P(i) := P[i, i]$. It is well-defined, because all the elements of the main diagonal of P are pairwise distinct. Lemma 1 shows that the cycle structure of this permutation is an isomorphism invariant of partial Latin squares in $\mathcal{DPL}(n)$. Recall here that the *cycle structure* of a permutation $\pi \in S_n$ is the expression $z_\pi := n^{d_n} \dots 1^{d_1}$, where, for each $l \in [n]$, we denote by d_l the number of cycles of length l in the unique decomposition of the permutation π into disjoint cycles. Thus, for instance, the cycle structure of the permutation $\pi = (123)(456)(78)(9) \in S_9$ is $z_{\pi_1} = 3^2 21$. Particularly, if two permutations π_1 and π_2 in S_n are *conjugate* (that is, if there exists a third permutation $\pi_3 \in S_n$ such that $\pi_1 = \pi_3 \pi_2 \pi_3^{-1}$), then $z_{\pi_1} = z_{\pi_2}$.

Lemma 1. *If P and P' are two partial Latin squares in $\mathcal{DPL}(n)$ such that $z_{\pi_P} \neq z_{\pi_{P'}}$, then P and P' are not isomorphic. If $|P| = |P'| = n$, then the converse also holds.*

Proof. In order to prove the first statement, let us suppose the existence of an isomorphism $\pi \in S_n$ from P to P'. Then, $\pi_{P'}(i) = P'[i, i] = \pi(P[\pi^{-1}(i), \pi^{-1}(i)]) = \pi\pi_P\pi^{-1}(i)$, for all $i \in [n]$. That is, $\pi_{P'} = \pi\pi_P\pi^{-1}$. Thus, π_P and $\pi_{P'}$ are conjugate and hence, they have the same cycle structure. It contradicts the fact that $z_{\pi_P} \neq z_{\pi_{P'}}$.

Concerning the second statement, if $z_{\pi_P} = z_{\pi_{P'}}$, then there exists a permutation $\pi \in S_n$ such that $\pi_{P'} = \pi\pi_P\pi^{-1}$. In particular, for each positive integer $i \in [n]$, we have that

$$P'[\pi(i), \pi(i)] = \pi_{P'}(\pi(i)) = \pi\pi_P\pi^{-1}(\pi(i)) = \pi\pi_P(i) = \pi(P[i, i]).$$

Hence, π is an isomorphism from P to P', because, since $|P| = |P'| = n$, the only non-empty cells of both partial Latin squares P and P' are those of their respective main diagonal.

2.2. Computational algebraic geometry

Let $\mathbb{Q}[X]$ be a multivariate polynomial ring over the field $\mathbb{Q}$ of rational numbers, on a set of variables $X = \{x_1, \dots, x_n\}$. A subset $I \subseteq \mathbb{Q}[X]$ is an *ideal* if $0 \in I$; $p + q \in I$, for all $p, q \in I$; and $pq \in I$, for all $(p, q) \in I \times \mathbb{Q}[X]$. It is *radical* if every polynomial $p \in \mathbb{Q}[X]$ belongs to I, whenever there exists a positive integer m such that $p^m \in I$. The ideal *generated by* a subset $\{p_1, \dots, p_m\} \subset \mathbb{Q}[X]$ is the set

$$\langle\, p_1, \dots, p_m \,\rangle := \left\{ \sum_{i=1}^{m} q_i\, p_i \colon\; q_i \in \mathbb{Q}[X],\ \text{for all } i \leq m \right\}.$$

The *algebraic set* of an ideal I in $\mathbb{Q}[X]$ is the set of common zeros of all its polynomials. That is, the set $\{a \in \mathbb{Q}^n \colon\; p(a) = 0,\ \text{for all } p \in I\}$. If its Krull dimension is zero, then the ideal I is *zero-dimensional.*

The *degree inverse lexicographical order* $\prec_{\text{degrevlex}}$ on $\mathbb{Q}[X]$ is a monomial term ordering such that, for each pair of monomials $\mathbf{x}^a = x_1^{a_1} \dots x_n^{a_n}$ and $\mathbf{x}^b = x_1^{b_1} \dots x_n^{b_n}$ in $\mathbb{Q}[X]$, we have that $\mathbf{x}^a \prec_{\text{degrevlex}} \mathbf{x}^b$ if and only if one of the following two conditions hold.

- $\sum_{i=1}^n a_i < \sum_{i=1}^n b_i$; or
- $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$, and there is a positive integer $m \leq n$ such that $a_i = b_i$, whenever $m < i \leq n$, and $a_m > b_m$.

Let I be an ideal in $\mathbb{Q}[X]$. The largest monomial of a polynomial $f \in I$, with respect to $\prec_{\text{degrevlex}}$, is its *leading monomial*. The ideal generated by all the leading monomials in I is the *initial ideal* $I_{\prec_{\text{degrevlex}}}$. A *Gröbner basis* of the ideal I, with respect to $\prec_{\text{degrevlex}}$, is any generating set of I whose leading monomials generate the initial ideal $I_{\prec_{\text{degrevlex}}}$. This basis is *reduced* if all its polynomials are monic, and no monomial in a generator belongs to the span of the leading monomials of the remaining generators. The reduced Gröbner basis of an ideal is unique. Its computation is extremely sensitive to the number of variables, and also to the length and degree of generators [14]. Thus, for instance, the complexity to compute the reduced Gröbner basis of a zero-dimensional radical ideal over the field of rational numbers is $d^{O(n)}$, where d is the maximal degree of the generators of the ideal, and n is the number of variables [15].

Throughout this paper, we compute reduced Gröbner bases of zero-dimensional radical ideals over the field of rational numbers, with respect to $\prec_{\text{degrevlex}}$. The complexity of this computation is, therefore, established by the last statement of the previous paragraph. For all practical purposes, we have used the open computer algebra system for polynomial computations Singular [11], which is particularly specialized in computing Gröbner bases. The library *HQP.lib* in Singular containing all the procedures described in this paper is available as suplementary material to the paper.

3. Using Gröbner bases to construct Latin squares

Gröbner bases can be used to construct the set of Latin squares in $\mathcal{L}(n)$ to which a given partial Latin square $P \in \mathcal{PL}(n)$ is completable [16, 17]. To this end, let $\mathbb{Q}[X_P]$ be the multivariate polynomial ring over the field of rational numbers, with $X_P := \{x_{ij} \colon\ i, j \in [n] \text{ such that } P[i, j] \notin [n]\}$. Then, the sought set can be identified with the algebraic set of the ideal

$$I_P := \left\langle F_n(x_{ij}),\ G_n(x_{ij}, x_{i'j}),\ G_n(x_{ij}, x_{ij'}),\ G_n(x_{ij}, P[i'', j]),\ G_n(x_{ij}, P[i, j'']) \colon \begin{cases} i, i', i'', j, j', j'' \in [n], \\ i \neq i' \text{ and } j \neq j', \\ \{P[i, j],\ P[i', j],\ P[i, j']\} \cap [n] = \emptyset, \\ \{P[i'', j],\ P[i, j'']\} \subset [n]. \end{cases} \right\rangle$$

in the multivariate polynomial ring $\mathbb{Q}[X_P]$, where

$$F_n(x) := \prod_{m=1}^{n} (x - m) \qquad \text{and} \qquad G_n(x, y) := \frac{F_n(x) - F_n(y)}{x - y}.$$

If a polynomial $F_n(x_{ij})$ lies in I_P, then x_{ij} only can take values in $[n]$. Hence, this ideal is zero-dimensional. Moreover, Seidenberg's Lemma (see Proposition 3.7.15 in [13]) implies that this ideal is radical, because, for each variable $x \in X_P$, the polynomial $F_n(x) \in I \cap \mathbb{Q}[x]$ satisfies $\gcd(F_n(x), F'_n(x)) = 1$. As a consequence, since the maximal degree of the generators of this ideal is n, and the set X_P contains $n^2 - |P|$ variables, the complexity to compute the reduced Gröbner basis of this ideal is $n^{O(n^2-|P|)}$. Furthermore, each zero of this ideal is uniquely related to an array $L \in \mathcal{A}(n)$ such that

$$L[i,j] = \begin{cases} P[i,j], & \text{if } P[i,j] \in [n], \\ l_{ij}, & \text{otherwise.} \end{cases}$$

where l_{ij} is the coordinate of the zero under consideration that corresponds to the variable x_{ij}. Notice here that each polynomial associated to the function G_n in the ideal implies that two symbols appearing either in the same row or in the same column of the array are different. Hence, $L \in \mathcal{L}(n)$.

We have implemented this procedure in our library *HQP.lib* in Singular by means of the function *LS*. It receives the partial Latin square $P \in \mathcal{PL}(n)$ as input. (Empty cells are introduced as zeros.) After computing the reduced Gröbner basis of the corresponding ideal, the output is the required set of Latin squares.

Example 2. *Let us consider the partial Latin square*

$$P \equiv \begin{array}{|c|c|c|c|} \hline 2 & \cdot & \cdot & \cdot \\ \hline \cdot & 1 & \cdot & \cdot \\ \hline \cdot & \cdot & 4 & \cdot \\ \hline \cdot & \cdot & \cdot & 3 \\ \hline \end{array} \in \mathcal{DPL}(4).$$

The reduced Gröbner basis of the ideal I_P, with respect to $<_{\text{degrevlex}}$, is the set

$$\left\{x_{43}^2 - 3x_{43} + 2,\ x_{12} + x_{43} - 5,\ x_{13} + 2x_{43} - 5,\ x_{14} - 3x_{43} + 2,\ x_{21} - x_{43} - 2,\ x_{23} - x_{43} - 1\right\} \cup$$
$$\cup \{x_{24} + 2x_{43} - 6, x_{31} - 2x_{43} + 1, x_{32} + x_{43} - 4, x_{34} + x_{43} - 3, x_{41} + 3x_{43} - 7,\ x_{42} - 2x_{43}\}.$$

This basis and its zeros (already expressed as Latin squares) are computed in Singular *as follows.*

```
> LIB "HQP.lib";
> intmat P[4][4]=2,0,0,0,0,1,0,0,0,0,4,0,0,0,0,3;
> LS(P);
  [1]:                          [2]:
     2,4,3,1,                      2,3,1,4,
     3,1,2,4,                      4,1,3,2,
     1,3,4,2,                      3,2,4,1,
     4,2,1,3                       1,4,2,3
```

In a similar way, it is possible to construct partial Latin squares satisfying certain conditions. Thus, for example, Section 4 requires to deal with the following question.

Question 3. *Given a partial Latin square $P \in \mathcal{PL}(n)$ with a transversal T having, at least, one empty cell, determine the set*

$$\mathcal{PL}_T(P) := \left\{ Q \in \mathcal{PL}(n) \colon \begin{cases} \text{Ent}(Q) \setminus \{(i,j,Q[i,j]) \colon (i,j) \in T\} = \text{Ent}(P) \setminus \{(i,j,P[i,j]) \colon (i,j) \in T\}, \\ T \textit{ is a Latin transversal in } Q. \end{cases} \right\}.$$

That is, we want to determine the set of partial Latin squares $Q \in \mathcal{PL}(n)$ that result after filling the cells of a transversal T, which has at least one empty cell, in a partial Latin square $P \in \mathcal{PL}(n)$. In order to solve this question, let $X_T := \{x_{ij} \colon\ (i,j) \in T$ such that $P[i,j] \notin [n]\}$. Then, the set $\mathcal{PL}_T(P)$ can be identified with the algebraic set of the ideal

$$I_{P,T} := \left\langle F_n\left(x_{ij}\right), G_n\left(x_{ij}, x_{kl}\right), G_n\left(x_{ij}, P\left[i', j'\right]\right), G_n\left(x_{ij}, P\left[i, j''\right]\right), G_n\left(x_{ij}, P\left[i'', j\right]\right) \colon \begin{cases} \{x_{ij},\ x_{kl}\} \subseteq X_T, (i,j) \neq (k,l), \\ P[i',j'] \in [n],\ (i',j') \in T, \\ P[i'',j] \in [n],\ i \neq i'', \\ P[i,j''] \in [n],\ j \neq j''. \end{cases} \right\rangle$$

in the multivariate polynomial ring $\mathbb{Q}[X_T]$. Similarly to the reasoning that has been carried out for the ideal I_P, it can be deduced that the ideal $I_{P,T}$ is zero-dimensional and radical, and that the complexity to compute its reduced Gröbner basis is $n^{O(n-|T|)}$. We have implemented in our library *HQP.lib* in Singular the function *PLT* to solve Question 3. This function receives two arrays as inputs: the partial Latin square $P \in \mathcal{PL}(n)$ and an $n \times 2$ array whose rows indicate the cells of the transversal T. (Again, empty cells in P are indicated by zeros.)

Example 4. *Let us consider the partial Latin square $P \in \mathcal{DPL}(4)$ in Example 2 and its transversal of empty cells $T = \{(1,2), (2,1), (3,4), (4,3)\}$. The reduced Gröbner basis of the ideal $I_{P,T}$, with respect to $\prec_{\text{degrevlex}}$, is the set*

$$\left\{x_{21}^2 - 7x_{21} + 12,\ x_{43}^2 - 3x_{43} + 2,\ x_{12} + x_{21} - 7,\ x_{34} + x_{43} - 3\right\}.$$

This basis and its zeros (already expressed as partial Latin squares) are computed in Singular *as follows.*

```
> LIB "HQP.lib";
> intmat P[4][4]=2,0,0,0,0,1,0,0,0,0,4,0,0,0,0,3;
> intmat T[4][2]=1,2,2,1,3,4,4,3;
> PLT(P,T);
  [1]:         [2]:         [3]:         [4]:
     2,4,0,0,     2,3,0,0,     2,4,0,0,     2,3,0,0,
     3,1,0,0,     4,1,0,0,     3,1,0,0,     4,1,0,0,
     0,0,4,2,     0,0,4,2,     0,0,4,1,     0,0,4,1,
     0,0,1,3      0,0,1,3      0,0,2,3      0,0,2,3
```

Finally, Gröbner bases can also be used to determine whether two Latin squares are isomorphic or not. To this end, let $X_n := \{x_1, \ldots, x_n\}$. Then, the set of isomorphisms between two Latin squares L and L' in $\mathcal{L}(n)$ can be identified with the algebraic set of the ideal

$$I_{L,L'} := \left\langle F_n\left(x_i\right), G_n\left(x_i, x_{i'}\right), G_n(x_i, k) \cdot G_n(x_j, l) \cdot \left(x_{L[i,j]} - L'[k,l]\right) \colon\ i,\ i',\ j,\ k \in [n],\ i \neq i' \right\rangle$$

in the multivariate polynomial ring $\mathbb{Q}[X_n]$. To see it, let $(a_1, \ldots, a_n)$ be a zero of its algebraic set,where a_i is assigned to x_i, for all $i \in [n]$. The set of polynomials $\{F_n(x_i),\ G_n(x_i, x_{i'}) \colon\ i \in [n]\}$ in the ideal implies that this zero is uniquely associated to a permutation $\pi \in S_n$ such that $\pi(i) = a_i$, for all $i \in [n]$.

The remaining generators of the ideal make that $\pi(L[i,j]) = L'[\pi(i),\pi(j)]$, for all $i, j \in [n]$. That is, the permutation π is indeed an isomorphism from L to L'.

Similarly to the reasoning carried out for the ideal I_P, it can be observed that the ideal $I_{L,L'}$ is zero-dimensional and radical, and that the complexity to compute its reduced Gröbner basis is $n^{O(n)}$. We have implemented this procedure in our library *HQP.lib* in SINGULAR by means of the function *Isom*. It receives the Latin squares L and L' as input. After computing the reduced Gröbner basis of the ideal $I_{L,L'}$, the output is the set of isomorphisms from L to L'.

Example 5. *In this example, we are interested in knowing whether the two Latin squares that we have obtained in Example 2 are isomorphic or not. The reduced Gröbner basis of the ideal $I_{L,L'}$, with respect to $\prec_{\text{degrevlex}}$, is the set*

$$\{x_1 + x_2 + x_3 + x_4 - 10,\ x_2 + x_4 - 5,\ 2x_3x_4 - 5x_3 - 5x_4 + 11\} \cup$$

$$\cup \left\{x_3^2 + 8x_2x_4 + 9x_4^2 - 10x_2 - 5x_3 - 55x_4 + 60,\ 2x_4^3 + x_3x_4 - 15x_4^2 - x_3 + 30x_4 - 17\right\}.$$

This basis and its zeros are computed in SINGULAR *as follows.*

```
> LIB "HQP.lib";
> intmat L1[4][4]=2,4,3,1,3,1,2,4,1,3,4,2,4,2,1,3;
> intmat L2[4][4]=2,3,1,4,4,1,3,2,3,2,4,1,1,4,2,3;
> isom(L1,L2);
[1]:
   3,4,2,1
[2]:
   4,3,1,2
[3]:
   1,2,4,3
[4]:
   2,1,3,4
```

Thus, the required set of isomorphisms is the set $\{(1324), (1423), (34), (12)\} \subset S_4$. *Notice that it does not constitute a subgroup of* S_4.

4. The Hadamard quasigroup product

In this section, we generalize the classical Hadamard product for the set $\mathcal{A}(n)$. To this end, let $L \in \mathcal{L}(n) \subset \mathcal{A}(n)$ be a Latin square of order n describing the multiplication table of a quasigroup $([n], *)$. Then, for each pair of arrays $A,\ B \in \mathcal{A}(n)$, we define the *Hadamard L-product* $A \odot_L B \in \mathcal{A}(n)$ so that, for each pair of positive integers $i, j \in [n]$, we have that

$$(A \odot_L B)\,[i,j] := \begin{cases} \cdot, & \text{if } \{A[i,j], B[i,j]\} \cap \{\cdot\} \neq \emptyset, \\ L\,[A[i,j], B[i,j]] = A[i,j] * B[i,j], & \text{otherwise.} \end{cases} \tag{4.1}$$

More generally, we use the term *Hadamard quasigroup product* to denote any Hadamard L-product, where $L \in \mathcal{L}(n)$. We have implemented this product in our library *HQP.lib* in SINGULAR by means of the function *HadProd*.

Example 6. *Let us consider the following Latin squares in $\mathcal{L}(3)$.*

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

The Hadamard quasigroup product $L_1 \odot_{L_2} L_3$ is computed in Singular *as follows.*

```
> LIB "HQP.lib";
> intmat L1[3][3]=1,2,3,3,1,2,2,3,1;
> intmat L2[3][3]=1,3,2,3,2,1,2,1,3;
> intmat L3[3][3]=1,2,3,2,3,1,3,1,2;
> HadProd(L1,L3,L2);
1,2,3,
1,2,3,
1,2,3
```

If $A = B = L$ in (4.1), then we also define the products

$$\odot_\ell^k L := L \odot_L \left(\odot_\ell^{k-1} L\right) \qquad \text{and} \qquad \odot_\rho^k L := \left(\odot_\rho^{k-1} L\right) \odot_L L,$$

where $\odot_\ell^1 L := \odot_\rho^1 L := L$ and $\odot_\ell^2 L := \odot_\rho^2 L := L^2 := L \odot_L L$. The next lemma shows how these products are related under matrix transposition. (From here on, A^t denotes the transpose of an array $A \in \mathcal{A}(n)$.)

Lemma 7. *If $L \in \mathcal{L}(n)$, then $\odot_\ell^k L^t = \left(\odot_\rho^k L\right)^t$, for every positive integer k.*

Proof. We prove this lemma by mathematical induction. For $k = 1$, the result is immediate. Now, if the result holds for some positive integer k, then

$$\begin{aligned}\left(\odot_\ell^{k+1} L^t\right)[i,j] &= L^t \odot_{L^t} \left(\odot_\ell^k L^t\right)[i,j] = \\ &= \left(L^t \odot_{L^t} \left(\odot_\rho^k L\right)^t\right)[i,j] = \\ &= L^t\left[L^t[i,j], \left(\left(\odot_\rho^k L\right)^t\right)[i,j]\right] = \\ &= L\left[\left(\odot_\rho^k L\right)[j,i], L[j,i]\right] = \\ &= \left(\odot_\rho^k L \odot_L L\right)[j,i] = \\ &= \left(\odot_\rho^{k+1} L\right)[j,i],\end{aligned}$$

for all $i, j \in [n]$. As a consequence, $\odot_\ell^{k+1} L^t = \left(\odot_\rho^{k+1} L\right)^t$.

The discrete structure of the Latin square L under consideration endows the product described in (4.1) with a cyclic behaviour. More specifically, one can ensure the existence of a pair of positive integers $k_1, k_2 \geq 2$ such that $\odot_\ell^{k_1} L = \odot_\rho^{k_2} L = L$. Let $\ell(L)$ and $\rho(L)$ denote, respectively, the minimum positive integers k_1 and k_2 satisfying this condition. In particular, Lemma 7 implies that $\ell(L) = \rho(L^t)$. Moreover, $\ell(L)$ and $\rho(L)$ are isomorphism invariants of Latin squares. In order to prove it, a technical lemma is required. In its statement, and from now on, if $A \in \mathcal{A}(n)$ and $\pi \in S_n$, then A^π denotes the array in $\mathcal{A}(n)$ such that, for each pair of positive integers $i, j \in [n]$,

$$A^\pi[i,j] := \begin{cases} \pi\left(A\left[\pi^{-1}(i), \pi^{-1}(j)\right]\right), & \text{if } A\left[\pi^{-1}(i), \pi^{-1}(j)\right] \in [n], \\ \cdot, & \text{otherwise.} \end{cases}$$

Lemma 8. *If L and L^π are two isomorphic Latin squares in $\mathcal{L}(n)$ by means of an isomorphism $\pi \in S_n$, then $\left(\odot_\alpha^k L\right)^\pi = \odot_\alpha^k L^\pi$, for $\alpha \in \{\ell, \rho\}$ and every positive integer k.*

Proof. From Lemma 7, it is enough to prove the case $\alpha = \rho$. We prove this case by mathematical induction. For $k = 1$, the result is immediate. Now, if the result holds for some positive integer k, then

$$\begin{aligned} \left(\odot_\rho^{k+1} L\right)^\pi [i,j] &= \left(\left(\odot_\rho^k L\right) \odot_L L\right)^\pi [i,j] = \\ &= \pi\left(\left(\left(\odot_\rho^k L\right) \odot_L L\right)\left[\pi^{-1}(i), \pi^{-1}(j)\right]\right) = \\ &= \pi\left(L\left[\left(\odot_\rho^k L\right)\left[\pi^{-1}(i), \pi^{-1}(j)\right], L\left[\pi^{-1}(i), \pi^{-1}(j)\right]\right]\right) = \\ &= \pi\left(L\left[\pi^{-1}\left(\left(\odot_\rho^k L\right)^\pi [i,j]\right), \pi^{-1}\left(L^\pi[i,j]\right)\right]\right) = \\ &= L^\pi\left[\left(\odot_\rho^k L\right)^\pi [i,j], L^\pi[i,j]\right] = \\ &= L^\pi\left[\left(\odot_\rho^k L^\pi\right)[i,j], L^\pi[i,j]\right] = \\ &= \left(\odot_\rho^{k+1} L^\pi\right)[i,j], \end{aligned}$$

for all $i, j \in [n]$. As a consequence, $\left(\odot_\rho^{k+1} L\right)^\pi = \odot_\rho^{k+1} L^\pi$.

Proposition 9. *Let L and L^π be two isomorphic Latin squares in $\mathcal{L}(n)$ by means of an isomorphism $\pi \in S_n$. Then, $\ell(L) = \ell(L^\pi)$ and $\rho(L) = \rho(L^\pi)$.*

Proof. From Lemma 7, it is enough to prove that $\rho(L) = \rho(L^\pi)$. To this end, Lemma 8 implies that

$$L^\pi[i,j] = \pi\left(L\left[\pi^{-1}(i), \pi^{-1}(j)\right]\right) = \pi\left(\left(\odot_\rho^{\rho(L)} L\right)\left[\pi^{-1}(i), \pi^{-1}(j)\right]\right) = \left(\odot_\rho^{\rho(L)} L^\pi\right)[i,j],$$

for all $i, j \in [n]$. Hence, $\rho(L^\pi) \leq \rho(L)$. In a similar way, we can prove that $\rho(L) \leq \rho(L^\pi)$ by making use of the isomorphism $\pi^{-1} \in S_n$ from L^π to L. As a consequence, $\rho(L) = \rho(L^\pi)$.

We have implemented in our library *HQP.lib* in Singular the computation of the isomorphism invariant ρ by means of the function *rho*.

Example 10. *Let us consider the Latin squares L_1, L_2 and L_3 described in Example 6. The isomorphism invariants $\rho(L_1) = 3$ and $\ell(L_1) = 4$ are, respectively, computed in* Singular *as follows.*

```
> LIB "HQP.lib";
> intmat L[3][3]=1,2,3,3,1,2,2,3,1;
> rho(L);
3
> rho(transpose(L));
4
```

In a similar way, it is obtained that $\rho(L_2) = \ell(L_2) = 2$ and $\rho(L_3) = \ell(L_3) = 3$. Hence, Lemma 8 implies that the Latin squares L_1, L_2 and L_3 are pairwise non-isomorphic. Furthermore, we have made use of the function HadProd *in* Singular *to compute the following Hadamard quasigroup products.*

$$L_1 = \odot_\ell^4 L_1 = \odot_\rho^3 L_1 = (L_1 \odot_{L_3} L_2) \odot_{L_3} L_3 = L_1 \odot_{L_3} (L_2 \odot_{L_3} L_3)$$

$$L_2 = L_2^2 = L_3^2 = L_2 \odot_{L_1} L_3 \qquad\qquad L_3 = \odot_\ell^3 L_3 = \odot_\rho^3 L_3 = L_3 \odot_{L_1} L_2$$

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

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

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

The Hadamard quasigroup products obtained in Example 10 also illustrate the following result, which holds readily from (4.1).

Lemma 11. *Let $L \in \mathcal{L}(n)$. Then, the following results hold.*

1). If $L[i_1, j_1] = L[i_2, j_2]$, for some $i_1, i_2, j_1, j_2 \in [n]$, then $\left(\odot_\alpha^k L\right)[i_1, j_1] = \left(\odot_\alpha^k L\right)[i_2, j_2]$, for all $\alpha \in \{\ell, \rho\}$ and every positive integer $k \geq 2$.

2). If L is idempotent, then $A \odot_L A = A$, for all $A \in \mathcal{A}(n)$. In particular, $L^2 = L$.

3). If L is symmetric, then the Hadamard L-product is commutative. In particular, $\odot_\ell^k L = \odot_\rho^k L$ is also symmetric, for all $k > 2$.

4). If L is the multiplication table of a group, then the Hadamard L-product is associative. As a consequence, $\odot_\ell^k L = \odot_\rho^k L$, for all $k > 2$.

Example 10 also shows that the Hadamard quasigroup product does not preserve the Latin square property in general. The following result establishes a necessary and sufficient condition for ensuring that a Hadamard quasigroup product of two Latin squares is a Latin square.

Lemma 12. *Let L, L' and L'' be three Latin squares in $\mathcal{L}(n)$. Then, $L' \odot_L L'' \in \mathcal{L}(n)$ if and only if, for each positive integer $i \in [n]$, both sets of cells $\{(L'[i, j], L''[i, j]) : j \in [n]\}$ and $\{(L'[j, i], L''[j, i]) : j \in [n]\}$ are Latin transversals in L.*

Proof. Since L' and L'' are Latin squares, each set of cells in the statement contains exactly one entry per row and one entry per column in L. Moreover, these cells contain exactly one entry of each symbol, because, from the Latin square property and Definition (4.1), we have that $L' \odot_L L'' \in \mathcal{L}(n)$ if and only, for each positive integer $i \leq n$, $\{L[L'[i,j], L''[i,j]]\colon\ j \in [n]\} = \{L[L'[j,i], L''[j,i]]\colon\ j \in [n]\} = [n]$.

Example 13. *Under the assumptions of Example 6, we have seen in Example 10 that* $L_2^2 = L_2 \in \mathcal{L}(3)$. *Concerning this Hadamard quasigroup product, every set of cells described in Lemma 12 corresponds to the Latin transversal* $\{(1,1),\ (2,2),\ (3,3)\}$ *in* L_2. *We also have seen that* $L_2 \odot_{L_1} L_3 = L_2 \in \mathcal{L}(3)$. *Concerning this Hadamard quasigroup product, every set of cells described in Lemma 12 corresponds to the Latin transversal* $\{(1,1),\ (2,3),\ (3,2)\}$ *in* L_1.

From here on, let $\mathcal{DL}(n)$ denote the set of Latin squares in $\mathcal{L}(n)$ whose main diagonal is a Latin transversal. The first case described in Example 13 illustrates the following result, which holds readily from the Latin square property and Lemma 12.

Proposition 14. *A Latin square* $L \in \mathcal{L}(n)$ *satisfies that* $L^2 \in \mathcal{L}(n)$ *if and only if* $L \in \mathcal{DL}(n)$.

In what follows, we are interested in determining those Latin squares $L \in \mathcal{L}(n)$ for which the successive iterations of Hadamard L-products $\odot_\rho^k L$, with $k \geq 2$, are also Latin squares. That is, we are interested in the set

$$\mathcal{HL}_\rho(n) := \left\{L \in \mathcal{L}(n)\colon\ \odot_\rho^k L \in \mathcal{L}(n),\ \text{whenever } 2 \leq k \leq \rho(L)\right\}.$$

Notice that every idempotent Latin square $L \in \mathcal{L}(n)$ belongs to this set, because of the third statement in Lemma 11. So, our study focuses on determining those non-idempotent Latin squares in $\mathcal{HL}_\rho(n)$. In any case, the following result characterizes all the Latin squares in this set.

Proposition 15. *A Latin square* $L \in \mathcal{L}(n)$ *belongs to* $\mathcal{HL}_\rho(n)$ *if and only if the set* $\left\{\left(\left(\odot_\rho^{k-1} L\right)[i,i],\ L[i,i]\right)\colon\ i \in [n]\right\}$ *is a Latin transversal in L, whenever* $2 \leq k \leq \rho(L)$.

Proof. From Proposition 14, we must have $L \in \mathcal{DL}(n)$. Thus, each pair $(i,j) \in [n] \times [n]$ is uniquely associated to a positive integer $i_j \in [n]$ such that $L[i,j] = L[i_j, i_j]$. Then, the first statement in Lemma 11 implies that $\left(\odot_\rho^k L\right)[i,j] = \left(\odot_\rho^k L\right)[i_j, i_j]$, for all $k \leq \rho(L)$. The result holds because Lemma 12 implies that $\odot_\rho^k L \in \mathcal{L}(n)$ if and only if the set $\left\{\left(\left(\odot_\rho^{k-1} L\right)[i,i],\ L[i,i]\right)\colon\ i \in [n]\right\}$ is a Latin transversal in L.

Whenever it is possible, Proposition 15 enables us to construct Latin squares in the set $\mathcal{HL}_\rho(n)$ to which a given partial Latin square $P \in \mathcal{DPL}(n)$, with $|P| = n$, is completable. That is, a partial Latin square whose only non-empty cells form the Latin transversal of its main diagonal. In this regard, for each partial Latin square $P \in \mathcal{DPL}(n)$, with $|P| = n$, we define the set

$$\mathcal{HL}_\rho(P) := \left\{L \in \mathcal{HL}_\rho(n)\colon\ P \subseteq L\right\}. \tag{4.2}$$

Algorithm 1 shows how computational algebraic geometry can be used to ensure the existence of the Latin transversals described in Proposition 15, and hence, to construct the previous set. In the algorithm, we make use of both functions *LS* and *PLT*, which we have defined in Subsection 2.1. We have implemented this algorithm in our library *HQP.lib* in Singular by means of the function *HL*.

Algorithm 1 Construction of the set $\mathcal{H}\mathcal{L}_\rho(P)$.

```
procedure $HL(P)$                                        ▷ Input: $P \in \mathcal{DPL}(n)$, with $|P| = n$.
    $L$ := Empty list
    $L'$ := Empty list
    $T$ := The $n \times 2$ zero array
    for $i \leftarrow 1, n$ do
        $T[i,1] := P^2[i,i]$
        $T[i,2] := P[i,i]$
    end for
    for $Q \in PLT(P,T)$ do
        $L \leftarrow L \cup \{(Q,T)\}$
    end for
    while $L \neq \emptyset$ do
        for $(Q,T) \in L$ do
            $L := L \setminus \{(Q,T)\}$
            for $i \leftarrow 1, n$ do
                $T[i,1] := Q[T[i,1], P[i,i]]$
            end for
            if $T$ does not have empty cells then
                if $T$ is a Latin transversal in $Q$ then
                    $L' \leftarrow L' \cup \{Q\}$
                end if
            else
                for $Q' \in PLT(Q,T)$ do
                    $L \leftarrow L \cup \{(Q',T)\}$
                end for
            end if
        end for
    end while
    for $Q \in L'$ do
        $L \leftarrow L \cup LS(Q)$
    end for
    return $L$
end procedure
```

Example 16. *Let us consider the partial Latin square $P \in \mathcal{DPL}(4)$ in Example 2. The set $\mathcal{HL}_\rho(P)$ can be computed in* Singular *as follows.*

```
> LIB "HQP.lib";
> intmat P[4][4]=2,0,0,0,0,1,0,0,0,0,4,0,0,0,0,3;
> HL(P);

  [1]:                          [2]:
     2,4,3,1,                      2,3,1,4,
     3,1,2,4,                      4,1,3,2,
     1,3,4,2,                      3,2,4,1,
     4,2,1,3                       1,4,2,3
```

That is, $\mathcal{HL}_\rho(P)$ is formed by the two Latin squares to which P is completable (see Example 2), which we denote, respectively, by L_1 and L_2. Particularly, the following Hadamard quasigroup product holds.

$$L_1^2 \equiv \begin{array}{|c|c|c|c|}\hline 1&3&4&2\\\hline 4&2&1&3\\\hline 2&4&3&1\\\hline 3&1&2&4\\\hline\end{array} \qquad \odot_\rho^3 L_1 \equiv \begin{array}{|c|c|c|c|}\hline 4&2&1&3\\\hline 1&3&4&2\\\hline 3&1&2&4\\\hline 2&4&3&1\\\hline\end{array} \qquad \odot_\rho^4 L_1 = L_1$$

$$L_2^2 \equiv \begin{array}{|c|c|c|c|}\hline 1&4&2&3\\\hline 3&2&4&1\\\hline 4&1&3&2\\\hline 2&3&1&4\\\hline\end{array} \qquad \odot_\rho^3 L_2 \equiv \begin{array}{|c|c|c|c|}\hline 3&2&4&1\\\hline 1&4&2&3\\\hline 2&3&1&4\\\hline 4&1&3&2\\\hline\end{array} \qquad \odot_\rho^4 L_2 = L_2$$

Hence, $\rho(L_1) = \rho(L_2) = 4$. The equality of both values is also established because of the fact that L_1 and L_2 are indeed isomorphic, as we have already observed in Example 5.

The following result shows that the set described in (4.2) only depends on the cycle structure of the permutation π_P associated to the main diagonal of the partial Latin square under consideration, which was introduced in Subsection 2.1.

Proposition 17. *Let P and P' be two partial Latin squares in $\mathcal{DPL}(n)$, with $|P| = |P'| = n$, such that $z_{\pi_P} = z_{\pi_{P'}}$. Then, there is a one-to-one correspondence between the sets $\mathcal{HL}_\rho(P)$ and $\mathcal{HL}_\rho(P')$.*

Proof. Lemma 1 implies the existence of an isomorphism $\pi \in S_n$ from P to P'. Thus, since isomorphisms preserve the Latin square property, Lemma 8 implies that $L \in \mathcal{HL}_\rho(P)$ if and only if $L^\pi \in \mathcal{HL}_\rho(P')$.

Let $\mathcal{CS}(n) := \{z_\pi \colon \pi \in S_n\}$. In order to determine the set $\mathcal{HL}_\rho(n)$, Lemma 1 enables us to focus on computing the set $\mathcal{HL}_\rho(P)$ for a representative partial Latin square $P \in \mathcal{DLP}(n)$, with $|P| = n$ and $z_{\pi_P} = z$, for each cycle structure $z \in \mathcal{CS}(n) \setminus \{1^n\}$. (Notice here that the trivial cycle structure 1^n is associated to the set of idempotent Latin squares, which all belong to the set $\mathcal{HL}_\rho(n)$.) As an illustrative example, we have performed this computation for the case $n \leq 6$, for which the complete classification of partial Latin squares up to isomorphism is known. We indicate here those cycle structures, together with a representative permutation, for which the resulting set of Latin squares is not empty. We have made use of the function *Isom* in Singular to classify these Latin squares up to isomorphism. A representative Latin square of each isomorphism class is indicated below each cycle structure under consideration.

- $3 \in \mathcal{CS}(3) \rightsquigarrow (123) \in S_3$

2	1	3
1	3	2
3	2	1

$(\rho, \ell) = (3, 3)$

- $31 \in \mathcal{CS}(4) \rightsquigarrow (123)(4) \in S_4$

2	4	3	1
1	3	4	2
4	2	1	3
3	1	2	4

$(\rho, \ell) = (3, 4)$

- $2^2 \in \mathcal{CS}(4) \rightsquigarrow (12)(34) \in S_4$

2	3	1	4
4	1	3	2
3	2	4	1
1	4	2	3

$(\rho, \ell) = (4, 4)$

- $5 \in \mathcal{CS}(5) \rightsquigarrow (12345) \in S_5$

2	4	1	3	5
1	3	5	2	4
5	2	4	1	3
4	1	3	5	2
3	5	2	4	1

$(\rho, \ell) = (3, 5)$

2	1	5	4	3
4	3	2	1	5
1	5	4	3	2
3	2	1	5	4
5	4	3	2	1

$(\rho, \ell) = (5, 3)$

2	5	3	1	4
5	3	1	4	2
3	1	4	2	5
1	4	2	5	3
4	2	5	3	1

$(\rho, \ell) = (5, 5)$

- $41 \in \mathcal{CS}(5) \rightsquigarrow (1234)(5) \in S_5$

2	1	5	4	3
1	3	2	5	4
5	2	4	3	1
4	5	3	1	2
3	4	1	2	5

$(\rho, \ell) = (3, 3)$

2	5	1	4	3
1	3	5	2	4
3	2	4	5	1
5	4	3	1	2
4	1	2	3	5

$(\rho, \ell) = (3, 5)$

- $2^21 \in \mathcal{CS}(5) \rightsquigarrow (12)(34)(5) \in S_5$

2	4	3	5	1
3	1	5	4	2
1	5	4	2	3
5	2	1	3	4
4	3	2	1	5

$(\rho, \ell) = (4, 5)$

- $6 \in \mathcal{CS}(6) \rightsquigarrow (123456) \in S_6$

2	5	1	3	4	6
1	3	5	6	2	4
6	2	4	1	3	5
4	6	3	5	1	2
5	1	2	4	6	3
3	4	6	2	5	1

$(\rho, \ell) = (3, 16)$

- $51 \in \mathcal{CS}(6) \rightsquigarrow (12345)(6) \in S_6$

2	6	1	3	5	4
1	3	6	2	4	5
5	2	4	6	3	1
4	1	3	5	6	2
6	5	2	4	1	3
3	4	5	1	2	6

$(\rho, \ell) = (3, 6)$

2	4	1	6	5	3
1	3	5	2	6	4
6	2	4	1	3	5
4	6	3	5	2	1
3	5	6	4	1	2
5	1	2	3	4	6

$(\rho, \ell) = (3, 6)$

2	4	6	3	5	1
1	3	5	6	4	2
5	2	4	1	6	3
6	1	3	5	2	4
3	6	2	4	1	5
4	5	1	2	3	6

$(\rho, \ell) = (3, 6)$

2	4	6	1	5	3
1	3	2	6	4	5
5	2	4	3	6	1
6	1	3	5	2	4
3	6	5	4	1	2
4	5	1	2	3	6

$(\rho, \ell) = (3, 31)$

2	4	6	3	5	1
1	3	2	6	4	5
5	2	4	1	6	3
6	1	3	5	2	4
3	6	5	4	1	2
4	5	1	2	3	6

$(\rho, \ell) = (3, 31)$

2	4	6	1	5	3
1	3	5	2	6	4
5	2	4	6	3	1
6	1	3	5	4	2
3	6	2	4	1	5
4	5	1	3	2	6

$(\rho, \ell) = (3, 31)$

2	6	5	4	3	1
4	3	6	1	5	2
1	5	4	6	2	3
3	2	1	5	6	4
6	4	3	2	1	5
5	1	2	3	4	6

$(\rho, \ell) = (5, 4)$

2	5	3	6	4	1
5	3	1	4	6	2
6	1	4	2	5	3
1	6	2	5	3	4
4	2	6	3	1	5
3	4	5	1	2	6

$(\rho, \ell) = (5, 6)$

- $41^2 \in \mathcal{CS}(6) \rightsquigarrow (1234)(5)(6) \in S_6$

2	5	6	4	3	1
1	3	2	6	4	5
6	2	4	5	1	3
5	4	3	1	6	2
3	6	1	2	5	4
4	1	5	3	2	6

$(\rho, \ell) = (3, 11)$

2	6	1	4	3	5
1	3	5	6	2	4
3	2	4	5	6	1
6	5	3	1	4	2
4	1	6	2	5	3
5	4	2	3	1	6

$(\rho, \ell) = (3, 16)$

2	5	6	4	1	3
1	3	2	6	4	5
6	2	4	5	3	1
5	4	3	1	6	2
3	6	1	2	5	4
4	1	5	3	2	6

$(\rho, \ell) = (3, 31)$

2	1	6	4	3	5
1	3	5	6	2	4
3	2	4	5	6	1
6	5	3	1	4	2
4	6	1	2	5	3
5	4	2	3	1	6

$(\rho, \ell) = (3, 31)$

2	1	6	4	3	5
1	3	5	6	4	2
3	2	4	5	6	1
6	5	3	1	2	4
4	6	1	2	5	3
5	4	2	3	1	6

$(\rho, \ell) = (3, 31)$

2	1	6	4	3	5
1	3	5	6	2	4
5	2	4	3	6	1
6	5	3	1	4	2
4	6	1	2	5	3
3	4	2	5	1	6

$(\rho, \ell) = (3, 31)$

2	6	1	4	3	5
1	3	5	6	2	4
6	2	4	5	1	3
4	5	3	1	6	2
3	4	6	2	5	1
5	1	2	3	4	6

$(\rho, \ell) = (3, 31)$

2	6	5	4	3	1
1	3	6	5	2	4
3	2	4	6	1	5
4	5	3	1	6	2
6	4	1	2	5	3
5	1	2	3	4	6

$(\rho, \ell) = (3, 31)$

2	5	6	4	3	1
1	3	5	6	2	4
6	2	4	3	1	5
5	4	3	1	6	2
4	6	1	2	5	3
3	1	2	5	4	6

$(\rho, \ell) = (3, 31)$

- $3^2 \in \mathcal{CS}(6) \rightsquigarrow (123)(456) \in S_6$

2	1	5	3	4	6
4	3	2	6	5	1
3	6	1	4	2	5
6	4	3	5	1	2
5	2	4	1	6	3
1	5	6	2	3	4

$(\rho, \ell) = (5, 11)$

2	4	5	3	1	6
4	3	2	6	5	1
3	6	1	4	2	5
6	1	3	5	4	2
5	2	4	1	6	3
1	5	6	2	3	4

$(\rho, \ell) = (5, 11)$

- $31^3 \in \mathcal{CS}(6) \rightsquigarrow (123)(4)(5)(6) \in S_6$

2	5	3	6	1	4
1	3	6	5	4	2
4	2	1	3	6	5
3	6	5	4	2	1
6	4	2	1	5	3
5	1	4	2	3	6

$(\rho, \ell) = (3, 4)$

2	6	3	5	1	4
1	3	5	6	4	2
4	2	1	3	6	5
3	5	6	4	2	1
6	4	2	1	5	3
5	1	4	2	3	6

$(\rho, \ell) = (3, 4)$

2	5	3	6	4	1
1	3	6	5	2	4
4	2	1	3	6	5
3	6	5	4	1	2
6	4	2	1	5	3
5	1	4	2	3	6

$(\rho, \ell) = (3, 16)$

2	6	3	5	4	1
1	3	5	6	2	4
4	2	1	3	6	5
3	5	6	4	1	2
6	4	2	1	5	3
5	1	4	2	3	6

$(\rho, \ell) = (3, 16)$

- $2^3 \in \mathcal{CS}(6) \rightsquigarrow (12)(34)(56) \in S_6$

2	4	1	5	3	6
5	1	3	6	2	4
3	6	4	2	5	1
1	5	6	3	4	2
4	2	5	1	6	3
6	3	2	4	1	5

$(\rho, \ell) = (5, 16)$

2	4	5	1	3	6
5	1	3	6	4	2
3	6	4	2	5	1
1	5	6	3	2	4
4	2	1	5	6	3
6	3	2	4	1	5

$(\rho, \ell) = (5, 16)$

5. Conclusions and further work

In this paper, we have introduced the concept of Hadamard quasigroup product as a natural generalization of the classical Hadamard product of matrices. Arising from the binary operation of any given quasigroup, it constitutes an element-wise product among partial arrays. After establishing the fundamentals of this new product, and describing a pair of new isomorphism invariants of Latin squares associated to it, our study has focused on determining those conditions under which the Latin square property is preserved by the successive iteration of a Hadamard quasigroup product. This property is readily preserved, for instance, for every idempotent quasigroup, because their own Hadamard quasigroup products coincide with themselves. In a more general way, the preservation of the Latin square property requires the existence of localized Latin transversals within the multiplication table of the quasigroup under consideration. That is, within a given Latin square. To determine constructively these Latin transversals, the sought quasigroups, and the classification of the latter up to isomorphism, we have performed the computation of reduced Gröbner bases of certain zero-dimensional radical ideals in multivariate polynomial rings. Table 1 shows the main procedures that we have implemented to this end, together with the complexity that is required to compute each of the corresponding reduced Gröbner basis.

Table 1. Main procedures implemented in Singular to compute our reduced Gröbner bases.

Procedure	Output	Complexity
$isom(L_1, L_2)$	The set of isomorphisms between two Latin squares L_1, $L_2 \in \mathcal{L}(n)$.	$n^{O(n)}$
$LS(P)$	The set of Latin squares $L \in \mathcal{L}(n)$ to which a partial Latin square $P \in \mathcal{PL}(n)$ is completable.	$n^{O(n^2-\lvert P\rvert)}$
$PLT(P, T)$	The set of partial Latin squares that result after filling the cells of a transversal T, with at least one empty cell, in a partial Latin square $P \in \mathcal{PL}(n)$.	$n^{O(n-\lvert T\rvert)}$

These procedures have been implemented into the open computer algebra system for polynomial computations Singular. We have performed them for all $n \in \{3, 4, 5, 6\}$. The computation of Gröbner bases for higher orders is computationally feasible, but the number of cases of study increases considerably. As it can be deduced from Table 1, the computational bottleneck will appear in Line 28 in Algorithm 1, only for those cases requiring the completion of partial Latin squares with too many empty cells. This is not necessarily a disadvantage, because any such a partial Latin square will possibly give rise to the formal description of a particular family of sought quasigroups. This is the case, for instance, of the partial Latin square $P \in \mathcal{DPL}(n)$, with $|P| = 2n$, such that

$$P[i,j] = \begin{cases} 1, & \text{if } i = j = n, \\ i-1, & \text{if } 1 < i = j+1 \leq n, \\ i+1, & \text{if } 1 \leq i = j < n, \\ n, & \text{if } (i,j) = (1,n). \end{cases}$$

Every Latin square $L \in \mathcal{L}(n)$ to which the partial Latin square P is completable belongs to the set $\mathcal{HL}_\rho(n)$. It is the case, for example, of the Latin square

$$L \equiv \begin{array}{|c|c|c|c|c|c|c|c|} \hline 2 & 1 & 5 & 7 & 3 & 4 & 6 & 8 \\ \hline 1 & 3 & 7 & 6 & 8 & 2 & 4 & 5 \\ \hline 8 & 2 & 4 & 3 & 7 & 1 & 5 & 6 \\ \hline 6 & 7 & 3 & 5 & 1 & 8 & 2 & 4 \\ \hline 7 & 8 & 2 & 4 & 6 & 5 & 1 & 3 \\ \hline 4 & 6 & 8 & 1 & 5 & 7 & 3 & 2 \\ \hline 3 & 5 & 1 & 2 & 4 & 6 & 8 & 7 \\ \hline 5 & 4 & 6 & 8 & 2 & 3 & 7 & 1 \\ \hline \end{array} \in \mathcal{DPL}(8),$$

for which $\rho(L) = 3$ and

$$L^2 \equiv \begin{array}{|c|c|c|c|c|c|c|c|} \hline 3 & 2 & 6 & 8 & 4 & 5 & 7 & 1 \\ \hline 2 & 4 & 8 & 7 & 1 & 3 & 5 & 6 \\ \hline 1 & 3 & 5 & 4 & 8 & 2 & 6 & 7 \\ \hline 7 & 8 & 4 & 6 & 2 & 1 & 3 & 5 \\ \hline 8 & 1 & 3 & 5 & 7 & 6 & 2 & 4 \\ \hline 5 & 7 & 1 & 2 & 6 & 8 & 4 & 3 \\ \hline 4 & 6 & 2 & 3 & 5 & 7 & 1 & 8 \\ \hline 6 & 5 & 7 & 1 & 3 & 4 & 8 & 2 \\ \hline \end{array} \in \mathcal{DPL}(8).$$

A more comprehensive study concerning the characterization of this kind of families of quasigroups is established as further work. In addition, the cycle structure of the permutation π_P that is uniquely associated to the main diagonal of each Latin square $P \in \mathcal{DPL}(n)$ has turned out to play a fundamental role to reduce the number of cases of study. In this regard, our computations for all $n \in \{3,4,5,6\}$ have shown the existence of cycle structures that are not related to any Latin square in the set $\mathcal{HL}_\rho(n)$. A much more comprehensive study of this cycle structure is, therefore, necessary.

It could also be interesting to carry out similar studies concerning the preservation by Hadamard quasigroup products of other algebraic properties such as commutativity, associativity or the existence of unit element, amongst others. The preservation of certain algebraic identities, such as Moufang or Belousov identities, is also established as further work. Finally, the element-wise product here proposed can naturally be generalized from the multiplication table of a quasigroup to that of a *magma*. That is, a finite set endowed with a binary operation with no particular restrictions. The study of conditions under which the successive iteration of this *Hadamard magma product* preserves certain algebraic properties would also constitute interesting open questions to deal with.

Acknowledgments

The authors want to express their gratitude to the anonymous referees for the comprehensive reading of the paper and their pertinent comments and suggestions, which helped improve the manuscript. This work is partially supported by the research project TED2021-130566B-I00 *"New graphical authentication schemes in Information Management Systems by means of fractal images based on Latin squares"* from the Ministry of Science and Innovation of the Government of Spain.

Conflict of interest

The authors declare there is no conflict of interest.

References

1. G. Kolesova, C. W. H. Lam, L. Thiel, On the number of 8 × 8 Latin squares, *J. Comb. Theory Ser. A*, **54** (1990), 143–148. https://doi.org/10.1016/0097-3165(90)90015-O
2. A. Hulpke, P. Kaski, P. R. J. Östergård, The number of Latin squares of order 11, *Math. Comput.*, **80** (2011), 1197–1219. https://doi.org/10.1090/S0025-5718-2010-02420-2
3. B. D. McKay, A. Meynert, W. Myrvold, Small Latin squares, quasigroups, and loops, *J. Comb. Des.*, **15** (2007), 98–119. https://doi.org/10.1002/jcd.20105
4. R. M. Falcón, R. J. Stones, Enumerating partial Latin rectangles, *Electron. J. Comb.* **27** (2020), P2.47. https://doi.org/10.37236/9093
5. B. D. McKay, I. M. Wanless, Enumeration of Latin squares with conjugate symmetry, *J. Comb. Des.*, **30** (2022), 105–130. https://doi.org/10.1002/jcd.21814
6. M. K. Kinyon, J. D. H. Smith, P. Vojtěchovský, Sylow theory for quasigroups II: Sectional action, *J. Comb. Des.* **25** (2017), 159–184. https://doi.org/10.1002/jcd.21535
7. R. M. Falcón, Recognition and analysis of image patterns based on Latin squares by means of Computational Algebraic Geometry, *Mathematics*, **9** (2021), 666. https://doi.org/10.3390/math9060666
8. R. M. Falcón, A new quasigroup isomorphism invariant arising from fractal image patterns, *Quasigroups Relat. Syst.*, **1** (2022), 81–90. Available from: https://ibn.idsi.md/vizualizare_articol/157488.
9. R. M. Falcón, V. Álvarez, F. Gudiel, A computational algebraic geometry approach to analyze pseudo-random sequences based on Latin squares, *Adv. Comput. Math.*, **45** (2019), 1769–1792. https://doi.org/10.1007/s10444-018-9654-0
10. J. D. H. Smith, S. G. Wang, Isomorphism invariants for linear quasigroups, *Sao Palo J. Math. Sci.*, **14** (2020), 152–164. https://doi.org/10.1007/s40863-019-00130-x
11. W. Decker, G.M. Greuel, G. Pfister, H. Schonemann, Singular 4-3-1, A computer algebra system for polynomial computations, 2023. Available from: http://www.singular.uni-kl.de.
12. A. D. Keedwell, J. Dénes, *Latin Squares and Their Applications*, 2^{nd} edition, Elsevier/North-Holland, Amsterdam, 2015.

13. M. Kreuzer, L. Robbiano, *Computational Commutative Algebra 1*, Springer-Verlag, Berlin, 2000. https://doi.org/10.1007/978-3-540-70628-1

14. A. Hashemi, D. Lazard, Sharper complexity bounds for zero-dimensional Grobner bases and polynomial system solving, *Int. J. Algebra Comput.*, **21** (2011), 703–713. https://doi.org/10.1142/S0218196711006364

15. Y. N. Lakshman, On the complexity of computing a Gröbner basis for the radical of a zero dimensional ideal, in *STOC '90: Proceedings of the twenty-second annual ACM symposium on Theory of Computing*, ACM, New York, (1990), 555–563. https://doi.org/10.1145/100216.100294

16. J. Gago-Vargas, I. Hartillo, J. Martín-Morales, J. M. Ucha-Enríquez, Sudokus and Gröbner bases: Not only a divertimento, in *CASC 2006: Computer Algebra in Scientific Computing*, (2006), 155–165. https://doi.org/10.1007/11870814_13

17. R. M. Falcón, J. Martín-Morales, Gröbner bases and the number of Latin squares related to autotopisms of order $\leq$ 7, *J. Symb. Comput.*, **42** (2007), 1142–1154. https://doi.org/10.1016/j.jsc.2007.07.004

Glossary of Symbols

$\lvert A\rvert$	The weight of an array $A \in \mathcal{A}(n)$.
$\mathcal{A}(n)$	The set of $n \times n$ arrays with entries in the set $[n]$.
$\mathcal{CS}(n)$	The set of cycle structures of permutation in S_n.
$\mathcal{DL}(n)$	The set of Latin squares in $\mathcal{L}(n)$, whose main diagonal is a Latin transversal.
$\mathcal{DPL}(n)$	The set of partial Latin squares in $\mathcal{PL}(n)$, whose main diagonal is a Latin transversal.
$\mathcal{HL}_\rho(n)$	The set of Latin squares $L \in \mathcal{DPL}(n) \cap \mathcal{L}(n)$ such that $\odot_\rho^k L \in \mathcal{L}(n)$, for all $k \geq 2$.
$\mathcal{HL}_\rho(P)$	The set of Latin squares $L \in \mathcal{HL}_\rho(n)$ such that $P \subseteq L$, where $P \in \mathcal{PL}(n)$.
$\mathcal{L}(n)$	The set of Latin squares with entries in the set $[n]$.
$[n]$	The set $\{1, \ldots, n\}$.
$\mathcal{PL}(n)$	The set of partial Latin squares of order n with entries in the set $[n]$.
$\mathcal{PL}_T(P)$	The set of partial Latin squares $Q \in \mathcal{PL}(n)$ that result after filling the cells of a transversal T, with at least one empty cell, in a partial Latin square $P \in \mathcal{PL}(n)$.
S_n	The symmetric group on the set $[n]$.
z_π	The cycle structure of a permutation $\pi \in S_n$.

AIMS Press