Designs, Codes and Cryptography (2020) 88:391–411
https://doi.org/10.1007/s10623-019-00689-8

Mutually orthogonal latin squares based on cellular automata

Luca Mariot[1] · Maximilien Gadouleau[2] · Enrico Formenti[3] · Alberto Leporati[1]

Received: 19 June 2019 / Revised: 31 August 2019 / Accepted: 12 October 2019 /
Published online: 29 October 2019

Abstract

We investigate sets of mutually orthogonal latin squares (MOLS) generated by cellular automata (CA) over finite fields. After introducing how a CA defined by a bipermutive local rule of diameter d over an alphabet of q elements generates a Latin square of order q^{d-1}, we study the conditions under which two CA generate a pair of orthogonal Latin squares. In particular, we prove that the Latin squares induced by two Linear Bipermutive CA (LBCA) over the finite field $\mathbb{F}_q$ are orthogonal if and only if the polynomials associated to their local rules are relatively prime. Next, we enumerate all such pairs of orthogonal Latin squares by counting the pairs of coprime monic polynomials with nonzero constant term and degree n over $\mathbb{F}_q$. Finally, we present a construction for families of MOLS based on LBCA, and prove that their cardinality corresponds to the maximum number of pairwise coprime polynomials with nonzero constant term. Although our construction does not yield all such families of MOLS, we show that the resulting lower bound is asymptotically close to their actual number.

Communicated by C. J. Colbourn.

This work has been partially supported by COST Action IC1405, "Reversible Computation—Extending the Horizons of Computing".

✉ Luca Mariot
luca.mariot@unimib.it

Maximilien Gadouleau
m.r.gadouleau@durham.ac.uk

Enrico Formenti
enrico.formenti@unice.fr

Alberto Leporati
alberto.leporati@unimib.it

[1] Dipartimento di Informatica, Sistemistica e Comunicazione, Università degli Studi di Milano-Bicocca, Viale Sarca 336/14, 20126 Milan, Italy

[2] Department of Computer Science, Durham University, South Road, Durham DH1 3LE, UK

[3] Laboratoire d'Informatique, Signaux et Systèmes de Sophia-Antipolis (I3S), Université Côte d'Azur, 2000, route des Lucioles - Les Algorithmes, bât. Euclide B, 06900 Sophia Antipolis, France

Keywords Mutually orthogonal latin squares · Cellular automata · Sylvester matrices · Polynomials

Mathematics Subject Classification 05B15 · 68Q80 · 11T06

1 Introduction

A *Latin square* of order $N \in \mathbb{N}$ is a $N \times N$ matrix where each number from 1 to N appears exactly once in each row and column. Two Latin squares L_1 and L_2 of order N are *orthogonal* if by *superimposing* them one obtains all ordered pairs (i, j) of numbers from 1 to N, and *mutually orthogonal latin squares* (MOLS) are sets of Latin squares that are pairwise orthogonal.

Despite their simple definition, the construction of MOLS is a notoriously difficult combinatorial problem and it is one of the most studied research topics in design theory. This interest is also due to the numerous applications that MOLS have in other fields such as cryptography (for example in the design of authentication codes [28] and multipermutations [30]), coding theory (see e.g. the Golomb–Posner code [9]) and statistics (particularly in the design of experiments [23]). Some of the best known constructions of MOLS include MacNeish's theorem [16] and Wilson's construction [31] (see [3,14] for a more complete overview of construction methods).

The goal of this paper is to investigate a new construction of MOLS based on *Cellular Automata* (CA), a particular kind of discrete dynamical system described by a regular lattice of *cells*, where each cell synchronously updates its state by applying a local rule to itself and its neighboring cells. The motivation for studying this construction of MOLS spawned from the question of designing a threshold secret sharing scheme based on CA without adjacency constraints on the shares, as in the schemes proposed in [4,19].

To this end, we first isolate a particular subclass of CA—namely, those defined by bipermutive local rules of diameter d—and remark that the Cayley tables of their global rules are Latin squares of order s^{d-1}, where s is the size of the CA alphabet. We then narrow our attention to the case where the local rules are linear over the finite field $\mathbb{F}_q$, characterizing the pairs of Linear Bipermutive CA (LBCA) that produce orthogonal Latin squares. In particular, we prove that the Latin squares generated by two LBCA are orthogonal if and only if the polynomials associated to their local rules are relatively prime over $\mathbb{F}_q$. This is done by observing that the orthogonality of the squares is equivalent to the invertibility of the Sylvester matrix obtained from the transition matrices of the LBCA. Subsequently, we determine the number of pairs of orthogonal Latin squares generated by LBCA with rules of a fixed diameter d. Due to the aforementioned characterization, this actually amounts to counting the number of pairs of coprime monic polynomials with nonzero constant term and degree $n = d - 1$ over $\mathbb{F}_q$. Although the enumeration of coprime polynomial pairs over finite fields is a well-studied problem [2,27], to the best of our knowledge the case where both polynomials have a nonzero constant term has not been addressed before. We thus solve this counting problem through a recurrence equation, remarking that for $q = 2$ the resulting integer sequence is already known in the OEIS for other combinatorial and number-theoretic facts [29].Finally, we present a construction of MOLS based on LBCA whose rules are defined by the product of two irreducible polynomials and prove its optimality, meaning that the resulting MOLS families cannot be extended by adding another Latin square generated by LBCA. More precisely, we show that the size of the MOLS families derived by our construction is equal to the maximum number of pairwise coprime polynomials with nonzero constant term. Further, we count how many sets of MOLS can be obtained by our construction, and we prove that the corresponding lower bound is asymptotically close to the actual number of MOLS families of maximum cardinality generated by LBCA.

The present paper is an extended version of [17], a work that was informally presented at AUTOMATA 2016. In particular, the new original contributions of this paper concern the counting results of coprime polynomials and the construction of MOLS based on irreducible polynomials.

The rest of this paper is organized as follows. Section 2 covers the basic background definitions about Latin squares and cellular automata. Section 3 focuses on the characterization of orthogonal Latin squares generated by linear bipermutive CA. Section 4 addresses the enumeration of coprime polynomials with nonzero constant term, which are in one-to-one correspondence with orthogonal Latin squares generated by LBCA. Section 5 describes a construction of MOLS based on LBCA with irreducible polynomials, proves the optimality of the size of the resulting MOLS families and provides a lower bound for their number. Finally, Sect. 6 summarizes the contributions of this paper, and discusses some interesting avenues for future research on this topic.

2 Preliminaries on latin squares and cellular automata

In this section, we gather all the basic definitions that will be used to describe our results, referring the reader to [14] and [13] for further information about Latin squares and cellular automata, respectively.

We start by giving the formal definition of a Latin square:

Definition 1 Let X be a finite set of cardinality $|X| = N \in \mathbb{N}$, and let $[N] = \{1, \ldots, N\}$. A *Latin square* of order N is a $N \times N$ square matrix L with entries from X such that, for all $i, j, k \in [N]$ with $k \neq j$, it holds that $L(i, j) \neq L(i, k)$ and $L(j, i) \neq L(k, i)$.

In other words, Definition 1 states that each row and each column of a Latin square is a permutation of the support set X. The concept of Latin square is equivalent to that of *quasigroup*:

Definition 2 A *quasigroup* of order $N \in \mathbb{N}$ is a pair $\langle X, \circ \rangle$ where X is a finite set of N elements and $\circ$ is a binary operation over X such that:

- For all $x, y \in X$ the equation $x \circ z = y$ has a unique solution $z \in X$
- For all $x, y \in X$ the equation $z \circ x = y$ has a unique solution $z \in X$.

Indeed, an algebraic structure $\langle X, \circ \rangle$ is a quasigroup if and only if its *Cayley table* is a Latin square [14]. In what follows, we will assume that the support set is always $X = [N] = \{1, \ldots, N\}$.

We now introduce the orthogonality property of Latin squares:

Definition 3 Two Latin squares L_1 and L_2 of order N are called *orthogonal Latin squares* (OLS) if

$$(L_1(i_1, j_1), L_2(i_1, j_1)) \neq (L_1(i_2, j_2), L_2(i_2, j_2)) \tag{1}$$

for all distinct pairs of coordinates $(i_1, j_1), (i_2, j_2) \in [N] \times [N]$.

Equivalently, L_1 and L_2 are orthogonal if their *superposition* yields all the ordered pairs of the Cartesian product $[N] \times [N]$. A set of k Latin squares which are pairwise orthogonal is denoted as a k-MOLS, where the acronym stands for *Mutually Orthogonal Latin Squares*.

Cellular Automata (CA) are a particular kind of discrete dynamical system defined by shift-invariant local functions. In particular, a CA is composed of a lattice of *cells* whose states range over a finite alphabet A. Each cell updates in parallel its state by applying a *local rule* $f : A^\nu \to A$ to itself and $\nu - 1$ surrounding cells. One of the most common studied settings is that of one-dimensional infinite CA, where the lattice is the full shift space $A^{\mathbb{Z}}$. The *Curtis-Hedlund-Theorem* [11] topologically characterizes such CA in terms of global maps $F : A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ that are both shift-invariant and uniformly continuous with respect to the Cantor distance.

For our work, we are interested in one-dimensional *finite* CA. This case leads to the problem of updating the cells at the boundaries, since they do not have enough neighbors upon which the local rule can be applied. In this paper we focus on *No Boundary CA* (NBCA), which we define as follows:

Definition 4 Let A be a finite alphabet and $n, d \in \mathbb{N}$ with $n \geq d$. The *No Boundary Cellular Automaton* (NBCA) $F : A^n \to A^{n-d+1}$ of length n and diameter d determined by the *local rule* $f : A^d \to A$ is the vectorial function defined for all $x \in A^n$ as

$$F(x_0, \ldots, x_{n-1}) = (f(x_0, \ldots, x_{d-1}), f(x_1, \ldots, x_d), \ldots, f(x_{n-d}, \ldots, x_{n-1})) \ . \quad (2)$$

In other words, in a NBCA of length n, each output coordinate with index $0 \leq i \leq n - d$ is determined by evaluating the local rule f of diameter d on the *neighborhood* formed by the i-th input coordinate x_i and the $d - 1$ coordinates to its right, i.e. $x_{i+1}, \ldots, x_{i+d}$.

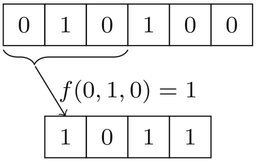
The NBCA model has been investigated in [22] for the design of S-boxes. There, the authors considered the case where the alphabet is $A = \mathbb{F}_2$, so that a NBCA corresponds to a particular kind of vectorial Boolean function defined by shift-invariant coordinate functions. When the CA alphabet is $\mathbb{F}_2$ the local rule $f : \mathbb{F}_2^d \to \mathbb{F}_2$ can be represented by its truth table, and its decimal representation is referred to as the *Wolfram code* of the rule. In this paper, we will mainly consider the setting where the alphabet is the finite field $\mathbb{F}_q$, with q being any power of a prime number. In order to avoid burdening notation we will use CA and NBCA interchangeably, since NBCA is the only model considered in the remainder of this work.

The following example grounds Definition 4 for the case of binary CA (i.e. when $A = \mathbb{F}_2$):

Example 1 Let $A = \mathbb{F}_2$, and consider a CA $F : \mathbb{F}_2^6 \to \mathbb{F}_2^4$ of length $n = 6$ and diameter $d = 3$ with local rule $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ defined as $f(x_0, x_1, x_2) = x_0 \oplus x_1 \oplus x_2$. Figure 1 depicts the application of the CA global function F over the vector $x = (0, 1, 0, 1, 0, 0)$ and reports the truth table of the local rule f. The Wolfram code of f is 150, since it corresponds to the decimal encoding of the output column $(0, 1, 1, 0, 1, 0, 0, 1)$ of the table, read in least significant bit order.

This paper focuses on the class of *bipermutive CA*, formally defined below:

Definition 5 A CA $F : A^n \to A^{n-d+1}$ induced by a local rule $f : A^d \to A$ is called *left permutive* (respectively, *right permutive*) if, for all $z \in A^{d-1}$, the restriction $f_{R,z} : A \to A$ (respectively, $f_{L,z} : A \to A$) obtained by fixing the first (respectively, the last) $d - 1$ coordinates of f to the values specified in z is a permutation on A. A CA which is both left and right permutive is said to be a *bipermutive* CA (BCA).



x_0, x_1, x_2	$f(x_0, x_1, x_2)$
000	0
100	1
010	1
110	0
001	1
101	0
011	0
111	1

Fig. 1 Example of CA of length $n = 6$ defined by rule 150

Remark that when $A = \mathbb{F}_2 = \{0, 1\}$ a local rule $f : \mathbb{F}_2^d \to \mathbb{F}_2$ is left permutive if and only if there exists a *generating function* $\varphi : \mathbb{F}_2^{d-1} \to \mathbb{F}_2$ such that

$$f(x_0, x_1, \dots, x_{d-1}) = x_0 \oplus \varphi(x_1, \dots, x_{d-1}) \ , \tag{3}$$

and symmetrically for right permutive rules. Thus, bipermutive CA over $\mathbb{F}_2$ are those induced by local rules of the form

$$f(x_0, x_1, \dots, x_{d-1}) = x_0 \oplus \varphi(x_1, \dots, x_{d-2}) \oplus x_{d-1} \ , \tag{4}$$

where φ is a Boolean function of $d - 2$ variables. Considering Example 1, one can see that rule 150 is bipermutive, since it corresponds to the case where φ is the identity function over the second variable of the neighborhood.

Most of the results stated in this paper concern CA that, beside being bipermutive, are also *linear* over the finite field $\mathbb{F}_q$. A CA $F : \mathbb{F}_q^n \to \mathbb{F}_q^{n-d+1}$ of diameter d is called linear if its local rule $f : \mathbb{F}_q^d \to \mathbb{F}_q$ is a linear combination of the cells in the neighborhood, i.e. there exist $a_0, \dots, a_{d-1} \in \mathbb{F}_q$ such that

$$f(x_0, \dots, x_{d-1}) = a_0 x_0 + a_1 x_1 + \cdots + a_{d-1} x_{d-1} \ , \tag{5}$$

for all $x \in \mathbb{F}_q^d$, where sum and product are the field operations of $\mathbb{F}_q$. For $q = 2$, these respectively correspond to the logical operations XOR ($\oplus$) and AND ($\wedge$). A linear CA can be seen as a linear transformation over $\mathbb{F}_q$-vector spaces described by the following $n \times (n - d + 1)$ *transition matrix*:

$$M_F = \begin{pmatrix} a_0 & \cdots & a_{d-1} & 0 & \cdots\cdots\cdots\cdots & & & & 0 \\ 0 & a_0 & \cdots & a_{d-1} & 0 & \cdots\cdots\cdots & & & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_0 & \cdots & a_{d-1} \end{pmatrix} . \tag{6}$$

In particular, the CA global rule is defined as the matrix-vector multiplication $F(x) = M_F \cdot x^\top$ for all $x \in \mathbb{F}_q^n$. As remarked in [20], the matrix M_F in Eq. (6) is the generator matrix of a *cyclic code*. Hence, one can naturally define the polynomial $p_f(X) \in \mathbb{F}_q[X]$ associated to a linear CA F as the generator polynomial of degree $n \leq d - 1$ of the corresponding cyclic code:

$$p_f(X) = a_0 + a_1 X + \cdots + a_{d-1} X^{d-1} \in \mathbb{F}_q[X] \ . \tag{7}$$

It is easy to see that a linear CA is bipermutive if and only if both a_0 and a_{d-1} are not null. Indeed, the inverse functions of the right and left restrictions $f_{R,z}$ and $f_{L,z}$ can be defined for all $z \in \mathbb{F}_q^{d-1}$ and $y \in \mathbb{F}_q$ as follows:

$$x_{d-1} = a_{d-1}^{-1}(y - a_0 z_0 - \cdots - a_{d-2} z_{d-2}) \ , \tag{8}$$

$$x_0 = a_0^{-1}(y - a_1 z_0 - \cdots - a_{d-1} z_{d-2}) \ . \tag{9}$$

Following the notation in [21], we denote by LBCA a CA F which is defined by a rule which is both linear and bipermutive. In what follows, we will consider mainly the situation where $a_{d-1} = 1$, which means that the polynomial $p_f(X)$ associated to the LBCA is monic of degree $n = d - 1$.

3 Characterization results

In this section, we first observe that any bipermutive CA can be used to generate a Latin square. We then prove a necessary and sufficient condition which characterizes orthogonal Latin squares generated by pairs of LBCA.

3.1 Latin squares from bipermutive CA

We begin by showing that any BCA of diameter d and length $2(d-1)$ generates a Latin square of order $N = q^{d-1}$, where q is the size of the CA alphabet. To this end, we first need some additional notation and definitions.

Given an alphabet A of q symbols, in what follows we assume that a total order $\leq$ is defined over A^{d-1} and $\phi : A^{d-1} \to [N]$ is a monotone one-to-one mapping between A^{d-1} and $[N] = \{1, \ldots, q^{d-1}\}$, where $[N]$ is endowed with the usual order of natural numbers. We denote by ψ the inverse mapping of ϕ.

We now formally define the notion of the square associated to a CA:

Definition 6 Let A be an alphabet of q symbols. The *square* associated to the CA $F : A^{2(d-1)} \to A^{d-1}$ defined by the rule $f : A^d \to A$ is the square matrix $\mathcal{S}_F$ of size $q^{d-1} \times q^{d-1}$ with entries from $[q^{d-1}]$ defined for all $1 \leq i, j \leq q^{d-1}$ as

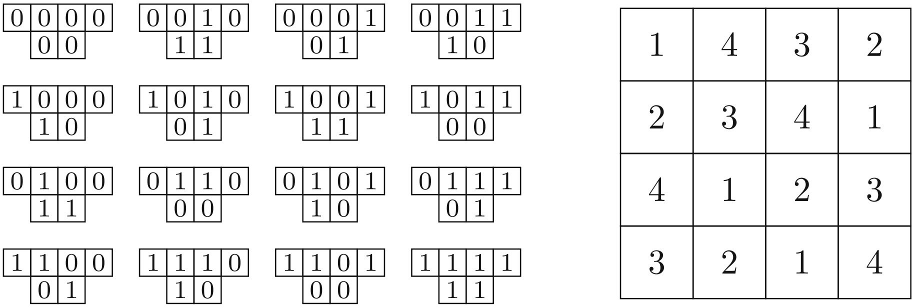
$$\mathcal{S}_F(i, j) = \phi(F(\psi(i)||\psi(j))) \ , \tag{10}$$

where $\psi(i)||\psi(j) \in A^{2(d-1)}$ denotes the *concatenation* of $\psi(i), \psi(j) \in A^{d-1}$.

Hence, the square $\mathcal{S}_F$ is defined by encoding the first half of the CA configuration as the row coordinate i, the second half as the column coordinate j and the output $F(\psi(i)||\psi(j))$ as the entry at (i, j).

As an example, for $A = \mathbb{F}_2$ and diameter $d = 3$, Fig. 2 depicts the square $\mathcal{S}_F$ associated to the CA $F : \mathbb{F}_2^4 \to \mathbb{F}_2^2$ defined by rule 150. The mapping ϕ is defined as $\phi(00) \mapsto 1$, $\phi(10) \mapsto 2$, $\phi(01) \mapsto 3$ and $\phi(11) \mapsto 4$. Notice that in this particular case $\mathcal{S}_F$ is a Latin square.

We remark that this representation has been adopted in several works in the CA literature, even though under a different guise. Indeed, one can consider the square associated to a CA as the Cayley table of an algebraic structure $\langle S, \circ \rangle$, where S is a set of size $|A|^{d-1}$ isomorphic to A^{d-1}, and $\circ$ is a binary operation over S. The two operands $x, y \in S$ are represented by the vectors respectively composed of the leftmost and rightmost $d-1$ input cells of the CA, while the $d-1$ output cells represent the result $z = x \circ y$. To the best of our knowledge, the first researchers who employed this algebraic characterization of cellular automata were



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

Fig. 2 Example of square of order $2^{3-1} = 4$ induced by rule 150

Pedersen [26] and Eloranta [6], respectively for investigating their periodicity and partial reversibility properties. Other works in this line of research include Moore and Drisko [25], who studied the algebraic properties of the square representation of CA, and Moore [24], who considered the computational complexity of predicting CA whose local rules define solvable and nilpotent groups.

As noticed above, the square associated to the CA defined by rule 150 is actually a Latin square. We will now show that this holds in general for all bipermutive CA. To this end, we first recall a Lemma proved in [19], which states that fixing $d-1$ adjacent cells in a bipermutive CA yields a permutation between the remaining variables and the output:

Lemma 1 *Let $F : A^n \rightarrow A^{n-d+1}$ be a BCA defined by local rule $f : A^d \rightarrow A$. Given $\tilde{x} \in A^{d-1}$ and i with $0 \leq i \leq n-d+1$, let $F|_{\tilde{x},i} : A^{n-d+1} \rightarrow A^{n-d+1}$ be the restriction of F obtained by fixing to $\tilde{x}$ the block of $d-1$ consecutive coordinates starting in i of the BCA input vector, i.e. $x_i = \tilde{x}_0$, $x_{i+1} = \tilde{x}_1, \ldots, x_{i+d-2} = \tilde{x}_{d-2}$. Then, $F|_{\tilde{x},i}$ is a permutation over A^{n-d+1}.*

On account of Lemma 1, we can prove that the squares associated to bipermutive CA are indeed Latin squares:

Lemma 2 *Let A be an alphabet of q symbols, and $d \geq 2$. Then, the square L_F of the BCA $F : A^{2(d-1)} \rightarrow A^{d-1}$ defined by local rule $f : A^d \rightarrow A$ is a Latin square of order $N = q^{d-1}$.*

Proof Let $i \in [N]$ be a row of L_F, and let $\psi(i) = (x_0, \ldots, x_{d-2}) \in A^{d-1}$ be the vector associated to i with respect to the total order $\leq$ on A^{d-1}. Consider now the set $C = \{c \in A^{2(d-1)} : (c_0, \ldots, c_{d-2}) = \psi(i)\}$, i.e. the set of configurations of length $2(d-1)$ whose first $d-1$ coordinates coincide with $\psi(i)$, and let $F_{\psi(i),0} : A^{d-1} \rightarrow A^{d-1}$ be the restriction of F determined by $\psi(i)$. By Lemma 1, the function $F_{\psi(i),0}$ is a permutation over A^{d-1}. So, the i-th row of L_F is a permutation of $[N]$. A symmetric argument holds for any column j of L_F, with $1 \leq j \leq N$, which fixes the rightmost $d-1$ variables of F to $\psi(j)$. Hence, every column of L_F is also a permutation of $[N]$, and thus L_F is a Latin square of order q^{d-1}. □

3.2 Orthogonal latin squares from linear bipermutive CA

In the next result, we prove a characterization of orthogonal Latin squares generated by LBCA in terms of their associated polynomials:

Theorem 1 *Let $F, G : \mathbb{F}_q^{2(d-1)} \to \mathbb{F}_q^{d-1}$ be two LBCA of length $2(d-1)$, respectively defined by the local rules $f, g : \mathbb{F}_q^d \to \mathbb{F}_q$ defined as:*

$$f(x_0, \dots, x_{d-1}) = a_0x_0 + \cdots + a_{d-1}x_{d-1} \ , \tag{11}$$

$$g(x_0, \dots, x_{d-1}) = b_0x_0 + \cdots + b_{d-1}x_{d-1} \ . \tag{12}$$

Then, the Latin squares L_F and L_G of order q^{d-1} generated by F and G are orthogonal if and only if the polynomials $p_f(X), p_g(X) \in \mathbb{F}_q[X]$ associated to f and g are relatively prime.

Proof Denote by $z = x||y$ the concatenation of vectors x and y. We show that the function $\mathcal{H} : \mathbb{F}_q^{2(d-1)} \times \mathbb{F}_q^{2(d-1)} \to \mathbb{F}_q^{2(d-1)} \times \mathbb{F}_q^{2(d-1)}$, defined for all $(x, y) \in \mathbb{F}_q^{2(d-1)} \times \mathbb{F}_q^{2(d-1)}$ as

$$\mathcal{H}(x, y) = (F(z), \mathcal{G}(z)) = (\tilde{x}, \tilde{y}) \tag{13}$$

is bijective if and only if the polynomials $p_f(X)$ and $p_g(X)$ associated to F and G are coprime. Given the transition matrices M_F and M_G respectively associated to F and G, one can rewrite Eq. (13) as a system of two equations:

$$\begin{cases} F(z) = M_F z^\top = \tilde{x} \\ \mathcal{G}(z) = M_G z^\top = \tilde{y} \end{cases} . \tag{14}$$

Since both M_F and M_G have size $(d-1) \times 2(d-1)$, Eq. (14) is a linear system of $2(d-1)$ equations and $2(d-1)$ unknowns, defined by the following $2(d-1) \times 2(d-1)$ square matrix:

$$M = \begin{pmatrix} a_0 & \cdots & a_{d-1} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_0 & \cdots & a_{d-1} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_0 & \cdots & a_{d-1} \\ b_0 & \cdots & b_{d-1} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & b_0 & \cdots & b_{d-1} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & b_0 & \cdots & b_{d-1} \end{pmatrix} , \tag{15}$$

i.e., M is obtained by placing the transition matrix M_F above M_G. Thus $\mathcal{H}(x, y) = Mz^\top$ and $\mathcal{H}$ is bijective if and only if the determinant of M is not null. Remark that matrix M in Eq. (15) is a *Sylvester matrix*, and its determinant is the *resultant* of the two polynomials $p_f(X)$ and $p_g(X)$ associated to the LBCA F and G, respectively. It is well known (see for instance [15]) that the resultant of two polynomials is nonzero if and only if they are relatively prime. Hence, $\mathcal{H}$ is bijective (or equivalently, the Latin squares L_F and L_G are orthogonal) if and only if the polynomials $p_f(X)$ and $p_g(X)$ are relatively prime. □

The next result immediately follows from the above theorem:

Corollary 1 *A family $p_1(X), \dots, p_k(X) \in \mathbb{F}_q[X]$ of $k \in \mathbb{N}$ pairwise coprime polynomials of degree $n = d-1$ is equivalent to a set of k MOLS of order q^n generated by LBCA.*

For alphabet $A = \mathbb{F}_2$ and diameter $d = 3$ there exist only two linear bipermutive rules, i.e. rule 150 and rule 90, the latter defined as $f_{90}(x_0, x_1, x_2) = x_0 \oplus x_2$. As shown in Fig. 3, the Latin squares of order $N = 4$ defined by the LBCA F_{150} and F_{90} respectively induced by f_{150} and f_{90} are orthogonal, since the associated polynomials $p_{150}(X) = 1 + X + X^2$ and $p_{90}(X) = 1 + X^2$ are coprime over $\mathbb{F}_2$.

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

(a) Rule 150

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

(b) Rule 90

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

(c) Overlay

Fig. 3 Orthogonal Latin squares generated by BCA with rules 150 and 90, corresponding to the pair of coprime polynomials $1 + X + X^2$ and $1 + X^2$

4 Counting coprime polynomial pairs

By Corollary 1, one can generate a set of k MOLS of order q^{d-1} through LBCA of diameter d by finding k pairwise relatively prime polynomials of degree $n = d - 1$. The problem of counting the number of pairs of relatively prime polynomials over finite fields has been investigated in several papers (see e.g. [1,2,12,27]). However, notice that determining the number of pairs of linear CA inducing orthogonal Latin squares entails counting only specific pairs of polynomials, namely those whose constant term is not null. This is due to the requirement that the CA local rules must be bipermutive. To the best of our knowledge, this particular counting problem has not been considered in the literature, for which reason we address it in this section.

Formally, for $n \geq 1$ let

$$S_n = \{f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n : a_0 \neq 0\} \tag{16}$$

be the set of monic polynomials in $\mathbb{F}_q[X]$ of degree n and with nonzero constant term. For all $n \geq 1$ we have that $s_n = |S_n| = (q-1)q^{n-1}$. Moreover, we define $S_0 = \{1\}$ (the unique monic polynomial of degree zero), and hence $s_0 = 1$.

Recall that the greatest common divisor of two polynomials $f, g \in \mathbb{F}_q[X]$ is the unique monic polynomial of highest degree h such that

$$f(X) = h(X)i(X)\,,$$
$$g(X) = h(X)j(X)\,,$$

for some $i, j \in \mathbb{F}_q[X]$. We remark that if $f, g \in S_n$, then $i, j \in S_e$ for some $0 \leq e \leq n$ and $h \in S_{n-e}$.

Additionally, let us define the following subsets of $S_n^2 = S_n \times S_n$:

$$A_n = \{(f, g) \in S_n^2 : \gcd(f, g) = 1\}\,,$$
$$B_n = \{(f, g) \in S_n^2 : \gcd(f, g) \neq 1\}\,.$$

In other words, A_n and B_n are respectively the sets of pairs of coprime and non-coprime monic polynomials of degree n with nonzero constant term. Similarly as above, let $a_n = |A_n|$ and $b_n = |B_n|$. We are interested in determining a_n, since by Theorem 1 the cardinality of A_n corresponds to the number of orthogonal Latin squares of order q^n generated by LBCA pairs of diameter $d = n + 1$. For $n = 0$, we clearly have $a_0 = 1$ and $b_0 = 0$. The following result characterizes a_n for all $n \geq 1$:

Theorem 2 *Let $n \geq 1$. Then, the number of pairs of coprime monic polynomials of degree n with nonzero constant term is*

$$a_n = q(q-1)^3 \frac{q^{2n-2}-1}{q^2-1} + (q-1)(q-2) \ . \tag{17}$$

Proof Let us first settle the case $n = 1$, for which we have

$$S_1 = \{f(X) = a_0 + X : a_0 \neq 0\} \ .$$

It is clear that $\gcd(f, g) = 1$ for any $f, g \in S_1$ if and only if $f \neq g$. Thus, it follows that

$$a_1 = (q-1)(q-2) \ ,$$

which proves Eq. (17) for the case $n = 1$. For $n > 1$, remark first that

$$s_n^2 = a_n + b_n \ . \tag{18}$$

Moreover, any pair (f, g) with $\deg(\gcd(f, g)) = n - e$ $(0 \leq e \leq n-1)$ can be uniquely expressed as a pair $(h, (i, j))$, where $h \in S_{n-e}$ and $i, j \in S_e$. Hence,

$$b_n = \sum_{e=0}^{n-1} a_e s_{n-e} \ . \tag{19}$$

Combining Eqs. (18) and (19) we have

$$a_n = s_n^2 - \sum_{e=0}^{n-1} a_e s_{n-e} \ , \tag{20}$$

$$a_{n-1} = s_{n-1}^2 - \sum_{e=0}^{n-2} a_e s_{n-1-e} \ . \tag{21}$$

Multiplying both sides of (21) by q we obtain

$$q a_{n-1} = q s_{n-1}^2 - \sum_{e=0}^{n-2} a_e s_{n-e} \ , \tag{22}$$

since $q s_{n-1-e} = q(q-1)q^{n-2-e} = (q-1)q^{n-1-e} = s_{n-e}$. Subtracting Eq. (22) from Eq. (20) we thus have

$$\begin{aligned} a_n - q a_{n-1} &= s_n^2 - \sum_{e=0}^{n-1} a_e s_{n-e} - q s_{n-1}^2 + \sum_{e=0}^{n-2} a_e s_{n-e} \\ &= s_n^2 - q s_{n-1}^2 - a_{n-1} s_1 \ . \end{aligned} \tag{23}$$

Since $s_n^2 = (q-1)^2 q^{2n-2}$, while $q s_{n-1}^2 = (q-1)^2 q^{2n-3}$ and $s_1 = (q-1)$, Eq. (23) becomes

$$a_n - q a_{n-1} = (q-1)^2 (q^{2n-2} - q^{2n-3}) - a_{n-1}(q-1) \ , \tag{24}$$

from which it follows that

$$a_n = (q-1)^2 (q^{2n-2} - q^{2n-3}) + a_{n-1}$$

$$= (q-1)^3 q q^{2n-4} + a_{n-1} \ . \tag{25}$$

By iterative use of (25), one has

$$a_n = q(q-1)^3 \sum_{t=0}^{n-2} q^{2t} + a_1$$
$$= q(q-1)^3 \frac{q^{2n-2}-1}{q^2-1} + (q-1)(q-2) \ , \tag{26}$$

from which we finally obtain the result. □

Remark 1 Notice that in Theorem 2 we count all *ordered* coprime polynomial pairs. To get the number of *distinct* pairs, one simply has to divide Eq. (17) by 2, thus obtaining $\tilde{a}_n = \frac{1}{2}a_n$. In particular, for $q = 2$ the formula for $\tilde{a}_n$ becomes

$$\tilde{a}_n = \frac{4^{n-1}-1}{3} \ . \tag{27}$$

The first terms of this sequence for $n \geq 1$ are:

$$\tilde{a}_n = 0, 1, 5, 21, 85, 341, 1365, \ldots \tag{28}$$

which is a shifted version of OEIS sequence A002450 [29], defined by

$$c_n = \frac{4^n-1}{3} \ . \tag{29}$$

It is easily seen that $c_n = \tilde{a}_{n+1}$, i.e. c_n corresponds to the number of distinct coprime pairs of polynomials of degree $n+1$ over $\mathbb{F}_2$ where both polynomials have nonzero constant term. We remark that sequence A002450 is known for several other combinatorial facts not related to polynomials or orthogonal Latin squares arising from LBCA, for which we refer the reader to [29].

5 A construction of MOLS based on LBCA

In this section, we tackle the question of determining the maximum number of MOLS generated by linear bipermutive CA over $\mathbb{F}_q$ of a given order. Given $n \in \mathbb{N}$ we consider in particular the following two problems:

Problem 1 What is the maximum number N_n of LBCA over $\mathbb{F}_q$ of diameter $n+1$ whose Latin squares are mutually orthogonal? From Sect. 3, this actually amounts to computing the maximum number of monic pairwise coprime polynomials of degree n with nonzero constant term over $\mathbb{F}_q$.

Problem 2 What is the number T_n of sets of N_n MOLS generated by LBCA?

In the remainder of this section we present a construction for sets of MOLS based on LBCA defined by pairwise coprime polynomials over $\mathbb{F}_q$. Moreover, we solve Problem 1 by proving that the size of MOLS resulting from this construction corresponds to the maximum number of pairwise coprime polynomials of degree n with nonzero constant term. We also determine the number D_n of MOLS that can be generated through this construction, and show that it is asymptotically close to T_n.

Recall from Sect. 4 that S_n denotes the set of all degree n monic polynomials $f \in \mathbb{F}_q[X]$ with nonzero constant term a_0. Additionally, let

$$\mathcal{M}_n = \{R_n \subseteq S_n : \forall f \neq g \in R_n, \gcd(f, g) = 1\} \ . \tag{30}$$

In other words, $\mathcal{M}_n$ is the family of subsets of S_n of pairwise coprime polynomials. In order to solve Problem 1, we have to determine the maximum cardinality of the subsets in $\mathcal{M}_n$, that is

$$N_n = \max_{R_n \in \mathcal{M}_n} |R_n| \ . \tag{31}$$

On the other hand, for Problem 2 we want to count how many sets in $\mathcal{M}_n$ have cardinality N_n:

$$T_n = |\{R_n \in \mathcal{M}_n : |R_n| = N_n\}| \ . \tag{32}$$

We begin by considering the set $\mathcal{I}_n$ of irreducible polynomials of degree n over $\mathbb{F}_q$ with nonzero constant term, all of which are trivially pairwise coprime. Hence, $\mathcal{I}_n$ is included in all subsets having maximum cardinality N_n. Denoting by I_n the cardinality of $\mathcal{I}_n$, one has that $I_0 = 1$ and $I_1 = q - 1$, while for $n \geq 2$ I_n is given by *Gauss's formula* [7]:

$$I_n = |\mathcal{I}_n| = \frac{1}{n} \sum_{d|n} \mu(d) \cdot q^{\frac{n}{d}} \ , \tag{33}$$

where d ranges over all positive divisors of n (including 1 and n), while μ denotes the *Möbius function*. Let $d = \varrho_1^{\alpha_1} \varrho_2^{\alpha_2} \ldots \varrho_k^{\alpha_k}$ be the prime factorization of $d \in \mathbb{N}$. Then, d is called *square-free* (s.f.) if $\alpha_i = 1$ for all $i \in \{1, \ldots, k\}$, i.e. if d is not divisible by any prime power with exponent higher than 1. The Möbius function of d is defined as:

$$\mu(d) = \begin{cases} 1, & \text{if } d = 1 \text{ or } d \text{ is s.f. and has an even number of prime factors} \\ -1, & \text{if } d \text{ is s.f. and has an odd number of prime factors} \\ 0, & \text{if } d \text{ is not s.f.} \end{cases} \tag{34}$$

We thus have that

$$N_n \geq I_n \ . \tag{35}$$

In order to refine this lower bound, we have to determine how many other (reducible) polynomials of degree n one can add to $\mathcal{I}_n$ so that the resulting set only includes pairwise coprime polynomials. To this end, we first need a side result which shows that the sequence of the numbers of monic irreducible polynomials is non-decreasing in the degree n. As a preliminary remark, observe that any polynomial f in S_n is either irreducible and hence belongs to $\mathcal{I}_n$, or at least one of its irreducible factors belongs to $\mathcal{J}_n = \bigcup_{k=1}^{\lfloor \frac{n}{2} \rfloor} \mathcal{I}_k$.

Lemma 3 *For all $q \geq 2$ powers of a prime number and $n \geq 1$, I_n is a non-decreasing function of n.*

Proof We want to show that $I_n \geq I_{n-1}$ for all $n \geq 2$. Note that $I_1 = q - 1$ since we do not consider the polynomial X (its constant term being null), while I_n is given by Gauss's formula for $n \geq 2$.

The claim is easily proved for $n \leq 4$, since

$$I_1 = q - 1 \ ,$$

$$
\begin{aligned}
I_2 &= \frac{1}{2}(q^2 - q) = \frac{q}{2} I_1 \geq I_1 \ , \\
I_3 &= \frac{1}{3}(q^3 - q) = \frac{2(q+1)}{3} I_2 \geq I_2 \ , \\
I_4 &= \frac{1}{4}(q^4 - q^2) = \frac{3q}{4} I_3 \geq I_3 \ .
\end{aligned}
$$

We now assume $n \geq 5$. We first prove that $I_n \geq \frac{1}{n}(q^n - q^{n-2})$. It is easily checked for $n = 5$, since $I_5 = \frac{1}{5}(q^5 - q)$; for $n \geq 6$, consider the sum

$$
q^{\lfloor \frac{n}{2} \rfloor} + q^{\lfloor \frac{n}{2} \rfloor - 1} + \cdots + q + 1 = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} q^i = \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - 1}{q - 1} \ . \tag{36}
$$

Remark that, for all $d|n$ with $d \neq 1$, the term $q^{\frac{n}{d}}$ in the sum of Gauss's formula occurs in the sum of Eq. (36), i.e. for $i = \frac{n}{d}$. Since in Gauss's formula one always adds or subtracts the term $q^{\frac{n}{d}}$ depending on the value of $\mu(d)$, by Eqs. (33) and (36) we have the following inequality:

$$
I_n \geq \frac{1}{n}\left(q^n - \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} q^i\right) = \frac{1}{n}\left(q^n - \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - 1}{q - 1}\right) \ , \tag{37}
$$

from which it follows that

$$
\begin{aligned}
I_n &\geq \frac{1}{n}\left(q^n - q^{\lfloor \frac{n}{2} \rfloor + 1}\right) \\
&\geq \frac{1}{n}\left(q^n - q^{n-2}\right) \ .
\end{aligned} \tag{38}
$$

We now prove that $I_{n-1} \leq \frac{1}{n-1} q^{n-1}$. Similarly to the previous inequality, let us denote by p the smallest prime divisor of $n - 1$. Then, in the sum of Gauss's formula for I_{n-1} we subtract $q^{\frac{n-1}{p}}$, since $\mu(p) = -1$. Consider now the sum

$$
q^{\frac{n-1}{p} - 1} + q^{\frac{n-1}{p} - 2} + \cdots + q + 1 = \sum_{i=0}^{\frac{n-1}{p} - 1} q^i = \frac{q^{\frac{n-1}{p}} - 1}{q - 1} \ . \tag{39}
$$

Again, each term $q^{\frac{n-1}{d}}$ in Gauss's formula for I_{n-1} occurs in (39) for $i = \frac{n-1}{d}$. Thus, the following inequality holds:

$$
I_{n-1} \leq \frac{1}{n-1}\left(q^{n-1} - q^{\frac{n-1}{p}} + \frac{q^{\frac{n-1}{p}} - 1}{q - 1}\right) \ . \tag{40}
$$

Therefore,

$$
I_{n-1} \leq \frac{1}{n-1} q^{n-1} \ . \tag{41}
$$

Combining the lower bound in (38) and the upper bound in (41), we obtain

$$
I_n \geq I_{n-1} \frac{n-1}{n} \cdot \frac{q^n - q^{n-2}}{q^{n-1}} \tag{42}
$$

$$= I_{n-1}\frac{n-1}{n} \cdot \left(q - \frac{1}{q}\right) \ . \tag{43}$$

Thus, since $q \geq 2$ and $n > 5$, it follows that

$$I_n \geq I_{n-1}\frac{4}{5} \cdot \frac{3}{2} \geq I_{n-1} \ . \tag{44}$$

□

Consider now the following construction for a family of pairwise coprime polynomials parameterized on the degree n:

```
CONSTRUCTION- IRREDUCIBLE($n$)
Initialization: Initialize set $\mathcal{P}_n$ to $\mathcal{I}_n$
Loop: For all $1 \leq k < \lfloor \frac{n}{2} \rfloor$ do:
    1. Build set $\mathcal{P}'_k$ by multiplying each polynomial in $\mathcal{I}_k$ with a distinct polynomial in $\mathcal{I}_{n-k}$
    2. Add set $\mathcal{P}'_k$ to $\mathcal{P}_n$
Final step: If $n$ is odd, build set $\mathcal{P}'_{(n-1)/2}$ by multiplying each polynomial in $\mathcal{I}_{(n-1)/2}$ with a distinct polynomial in $\mathcal{I}_{(n+1)/2}$, and add $\mathcal{P}'_{(n-1)/2}$ to $\mathcal{P}_n$. If $n$ is even, build set $\mathcal{P}'_{n/2}$ by squaring each irreducible polynomial in $\mathcal{I}_{n/2}$, and add $\mathcal{P}'_{n/2}$ to $\mathcal{P}_n$.
Output: return $\mathcal{P}_n$
```

Hence, set $\mathcal{P}_n$ is constructed by first adding all irreducible polynomials of degree n, then by adding the set of all irreducible polynomials of degree 1 multiplied by as many irreducible polynomials of degree $n-1$, and so on. In particular, notice that step 1 in the loop of CONSTRUCTION- IRREDUCIBLE is possible since by Lemma 3 one has that $I_{n-k} \geq I_k$ for all $k \leq \lfloor \frac{n}{2} \rfloor$. Further, all polynomials added to $\mathcal{P}_n$ through CONSTRUCTION- IRREDUCIBLE are pairwise coprime, since they all have distinct irreducible factors.

Remark that the procedure CONSTRUCTION- IRREDUCIBLE can be iterated only up to $k \leq \lfloor \frac{n}{2} \rfloor$, because by symmetry the irreducible polynomials of degree $n-k$ with $k > \lfloor \frac{n}{2} \rfloor$ correspond to those of degree $k \leq \lfloor \frac{n}{2} \rfloor$. Notice also that, when n is even, the last step of the procedure consists of squaring all irreducible polynomials of degree $\frac{n}{2}$.

Hence, we have shown that the set $\mathcal{P}_n$ which is generated by procedure CONSTRUCTION-IRREDUCIBLE is indeed a member of the family $\mathcal{M}_n$. The cardinality of such set is given by

$$C_n = |\mathcal{P}_n| = I_n + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} I_k \ . \tag{45}$$

In fact, beside the initial step when one adds all irreducible polynomials of degree n to $\mathcal{P}_n$, in each iteration k of the loop the number of polynomials that one can obtain by multiplying two irreducible factors is bounded by the number of irreducible polynomials of degree k, which is I_k. We have thus obtained the following result, which gives a more precise lower bound on N_n:

$$N_n \geq C_n \ . \tag{46}$$

A natural question arising from Inequality (46) is whether the above construction is optimal, i.e. if the maximum number of pairwise coprime polynomials N_n is actually equal to C_n. In the next theorem we prove that this is indeed the case, and we characterize the families of $\mathcal{T}_n$.

Theorem 3 *For any n and q, the maximum number of MOLS generated by LBCA of diameter $d = n + 1$, or equivalently the maximum number of pairwise coprime monic polynomials of degree n with nonzero constant term is:*

$$N_n = I_n + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} I_k \ . \tag{47}$$

Moreover, let $A \subseteq S_n$. Then, $A \in \mathcal{T}_n$ if and only if the following hold:

1. *A contains $\mathcal{I}_n$;*
2. *if n is even then A contains $\{g^2 : g \in \mathcal{I}_{n/2}\}$;*
3. *for every $g \in \mathcal{I}_k$ with $k < n/2$, there exists a unique $f \in A$ such that $g|f$. This f is either of the form $f = g^a$ with $a = n/k$, or of the form $f = g^b h$ where $bk < n/2$ and $h \in \mathcal{I}_{n-bk}$, in which case h does not divide any other $f' \in A$.*

Proof We first determine the value of N_n. By inequality (46) we have that $N_n \geq C_n$. Conversely, let $A \in \mathcal{M}_n$ be a maximum collection of mutually coprime polynomials in S_n, i.e. with cardinality N_n. Clearly, A must contain all irreducible polynomials $\mathcal{I}_n$, so let $B = A \backslash \mathcal{I}_n$ be the set of reducible polynomials in A. For any $f \in B$, denote the irreducible polynomial of lowest degree in the factorization of f as T_f (if there are several, choose the first one in lexicographic order). Note that T_f has degree at most $n/2$. Now if $f, g \in B$ satisfy $T_f = T_g$, then f and g are not coprime, therefore the map $f \mapsto T_f$ is an injection from B to $\mathcal{J}_n$. Thus $|A| \leq C_n$ and $N_n = C_n$.

We now characterize the families of cardinality N_n. We begin by showing that any such family must satisfy the three properties of the theorem. Firstly, as seen above, such a family A must contain $\mathcal{I}_n$, so let us focus on $B = A \setminus \mathcal{I}_n$. This time, the mapping $f \mapsto T_f$ is a bijection from B to $\mathcal{J}_n$, hence let $g \mapsto F_g$ be its inverse. Secondly, if $g \in \mathcal{I}_{n/2}$, then $F_g = gh$ for some $h \in \mathcal{I}_{n/2}$. If $h \neq g$, then $F_h \neq F_g$ but $\gcd(F_g, F_h) = h$, which violates coprimality; thus $h = g$ and $F_g = g^2$. Thirdly, if $g \in \mathcal{I}_k$, then either $F_g = g^a$ for $a = n/k$ or $F_g = g^b H_g$ for $bk < n$ and $\gcd(H_g, g) = 1$. If H_g is reducible, then its factor of lowest degree $h \in \mathcal{J}_n$ is a common divisor of F_h and F_g, which again violates coprimality. Thus $H_g \in \mathcal{I}_{n-bk}$ for $bk < n/2$. Finally, if $H_g = H_{g'}$ for another $g' \in \mathcal{J}_n$, then again coprimality is violated. Conversely, it is easily checked that any family satisfying all three properties is a family of N_n coprime polynomials in S_n. □

We now determine how many sets of pairwise coprime polynomials of degree n one can obtain through Construction- Irreducible, thus providing a lower bound on T_n. In particular, this corresponds to the case of families $A \in \mathcal{T}_n$ where the polynomial $f \in A$ in the third condition of Theorem 3 is of the form $f = gh$ (i.e. $b = 1$) and $h \in \mathcal{I}_{n-bk}$. Moreover, we show that this lower bound is asymptotically close to the actual value of T_n. Before proving this result, we first need the following asymptotic estimate of I_n:

Lemma 4 *Let I_n be defined as in Eq. (33). Then, as n tends to infinity,*

$$I_n = \frac{1}{n}\left(q^n - \mathcal{O}\left(q^{\frac{n}{2}}\right)\right) \ . \tag{48}$$

Proof Let us rewrite Eq. (33) by extracting the terms $d = 1$ and $d = p$ from the sum, where p is the smallest prime divisor of n. Since $\mu(1) = 1$ and $\mu(p) = -1$, we have

$$I_n = \frac{1}{n}\left(q^n - q^{\frac{n}{p}} + \sum_{d|n:d\neq 1,p} \mu(d) \cdot q^{\frac{n}{d}}\right) \ . \tag{49}$$

The smallest divisor of n which is strictly greater than p must be at least $p+1$. Thus, each term in the sum of Eq. (49) is limited in absolute value by $q^{\frac{n}{p+1}}$. In particular, as d grows the value $q^{\frac{n}{d}}$ decreases, hence we can bound the sum in (49) with the geometric series $\sum_{i=0}^{\infty} q^{\frac{n}{p+1}-i}$:

$$\sum_{d|n:d\neq 1,p} \mu(d)\cdot q^{\frac{n}{d}} \leq \sum_{i=0}^{\infty} q^{\frac{n}{p+1}-i} = q^{\frac{n}{p+1}} \sum_{i=0}^{\infty} q^{-i} \ . \tag{50}$$

Since $q \geq 2$, we have that $\sum_{i=0}^{\infty} q^{-i} \leq 2$. Thus, we obtain

$$\sum_{d|n:d\neq 1,p} \mu(d)\cdot q^{\frac{n}{d}} \leq 2\cdot q^{\frac{n}{p+1}} \ . \tag{51}$$

Consider now the difference $q^{\frac{n}{p}} - 2\cdot q^{\frac{n}{p+1}}$:

$$q^{\frac{n}{p}} - 2\cdot q^{\frac{n}{p+1}} = q^{\frac{n}{p}}\left(1 - 2\cdot q^{\frac{n}{p+1}-\frac{n}{p}}\right) = q^{\frac{n}{p}}\left(1 - 2\cdot q^{-\frac{n}{p(p+1)}}\right) \ . \tag{52}$$

Clearly, it results that $q^{-\frac{n}{p(p+1)}} \to 0$ for $n \to \infty$ and fixed p. Hence, we have that $q^{\frac{n}{p}} - 2\cdot q^{\frac{n}{p+1}} = \mathcal{O}\left(q^{\frac{n}{p}}\right)$, and by Inequality (51) it follows that

$$q^{\frac{n}{p}} - \sum_{d|n:d\neq 1,p} \mu(d)\cdot q^{\frac{n}{d}} = \mathcal{O}\left(q^{\frac{n}{p}}\right) \ . \tag{53}$$

Therefore, Eq. (33) can be rewritten as

$$I_n = \left(q^n - \mathcal{O}\left(q^{\frac{n}{p}}\right)\right) = \left(q^n - \mathcal{O}\left(q^{\frac{n}{2}}\right)\right) \ , \tag{54}$$

where the rightmost equality follows from the fact that $p \geq 2$ for all $n \in \mathbb{N}$. □

We can now prove our lower bound on T_n. In what follows, we denote by D_n the number of sets produced by Construction- Irreducible.

Theorem 4 *For all n, it holds that*

$$D_n = \prod_{k=1}^{\lceil \frac{n}{2}-1\rceil} \frac{I_{n-k}!}{(I_{n-k}-I_k)!} \ .$$

Moreover, as n tends to infinity, we have

$$\log_q D_n = \Theta\left(q^{\frac{n}{2}}\right) \ .$$
$$\log_q T_n = \log_q D_n + \mathcal{O}\left(q^{\frac{n}{3}}\right) = \Theta\left(q^{\frac{n}{2}}\right) \ .$$

Proof Let us first prove the formula for D_n. For all $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$, the set $\mathcal{P}'_k$ in step 1 of the loop of Construction- Irreducible is obtained by first taking an irreducible polynomial $f_1 \in \mathcal{I}_k$ and multiplying it by an irreducible polynomial $g_1 \in \mathcal{I}_{n-k}$. Hence, the choices for g_1 are I_{n-k}. Then, one takes another irreducible polynomial $f_2 \in \mathcal{I}_k$ and multiplies it by an irreducible polynomial $g_2 \in \mathcal{I}_{n-k}$, with $g_2 \neq g_1$. Thus, the possible choices for g_2 are $I_{n-k} - 1$. Since the choices for the polynomials in $\mathcal{I}_{n-k}$ are independent, and since we have to select I_k of them, we have that the number of choices for constructing $\mathcal{P}'_k$ is

$$E_k = I_{n-k}(I_{n-k}-1)\ldots(I_{n-k}-I_k+1) = \frac{I_{n-k}!}{(I_{n-k}-I_k)!} \ . \tag{55}$$

Further, since for $1 \leq k_1, k_2 \leq \lfloor \frac{n}{2} \rfloor$ with $k_1 \neq k_2$ the choices for constructing $\mathcal{P}'_{k_1}$ and $\mathcal{P}'_{k_2}$ are independent, we obtain that

$$D_n = \prod_{k=1}^{\lceil \frac{n}{2}-1 \rceil} E_k = \prod_{k=1}^{\lceil \frac{n}{2}-1 \rceil} \frac{I_{n-k}!}{(I_{n-k} - I_k)!} \ . \tag{56}$$

We now prove that $\log_q D_n = \Theta(q^{\frac{n}{2}})$, starting with some estimates for $\log_q I_{n-k}$ and $\log_q (I_{n-k} - I_k)$. As a first remark, observe that Eq. (48) in Lemma 4 shows that

$$\log_q I_{n-k} \leq n - k \ . \tag{57}$$

It is then easy to prove that for n large enough and $k < n/2$, one has

$$I_k \leq \frac{1}{k} q^k < \delta \frac{1}{n-k} q^{n-k} \ , \tag{58}$$

for $\delta < 1$, e.g. $\delta = \frac{1}{q-1/2}$. Combining Inequality (58) with Eq. (48) we obtain

$$I_{n-k} - I_k \geq \frac{1}{n-k} \left\{ (1-\delta) q^{n-k} - \mathcal{O}(q^{\frac{n-k}{2}}) \right\} \ , \tag{59}$$

and hence

$$I_{n-k} - I_k = \frac{(1 - \delta - o(1)) q^{n-k}}{n-k} \ . \tag{60}$$

Equation (60) thus yields the following estimate for $\log_q (I_{n-k} - I_k)$:

$$\begin{aligned} \log_q (I_{n-k} - I_k) &= n - k - \log_q (n-k) + \log_q (1 - \delta - o(1)) \\ &= n - k - \mathcal{O}(\log(n-k)) \ . \end{aligned} \tag{61}$$

Consider now $\log_q E_k$. By Eq. (55), it is easy to see that

$$I_k \log_q (I_{n-k} - I_k) \leq \log_q E_k \leq I_k \log_q I_{n-k} \ . \tag{62}$$

Since by (57) we have that $\log_q I_{n-k} \leq n-k$, while by (61) it holds that $\log_q E_k \geq I_k (n - k - \mathcal{O}(\log(n-k)))$, the inequalities in (62) can be rewritten as follows:

$$I_k (n - k - \mathcal{O}(\log(n-k))) \leq \log_q E_k \leq I_k \log_q I_{n-k} \ . \tag{63}$$

Consequently, we obtain the following estimate for $\log_q E_k$:

$$\begin{aligned} \log_q E_k &= I_k \left(n - k - \mathcal{O}(\log(n-k))\right) \\ &= \frac{1}{k} (q^k - \mathcal{O}(q^{\frac{k}{2}})) \left(n - k - \mathcal{O}(\log(n-k))\right) \\ &= \frac{1}{k} ((1 - o(1)) q^k)((1 - o(1))(n-k)) \\ &= \frac{1}{k} (1 - o(1)) q^k (n-k) \\ &= \frac{n-k}{k} q^k - o\left(\frac{n}{k} q^k\right) \ . \end{aligned} \tag{64}$$

Denoting $\sigma = \sum_{i=0}^{\infty} q^{-i}$, we have

$$q^{\lceil \frac{n}{2}-1 \rceil} \leq \sum_{k=\lfloor \frac{n}{3} \rfloor +1}^{\lceil \frac{n}{2}-1 \rceil} \frac{n-k}{k} q^k \leq 2\sigma q^{\lceil \frac{n}{2}-1 \rceil} \ . \tag{65}$$

Therefore,

$$\begin{aligned} \log_q D_n &= \sum_{k=1}^{\lceil \frac{n}{2}-1 \rceil} \log_q E_k \\ &= \sum_{k=\lfloor \frac{n}{3} \rfloor +1}^{\lceil \frac{n}{2}-1 \rceil} \log_q E_k + \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \log_q E_k \\ &= \Theta(q^{\frac{n}{2}}) + \mathcal{O}(nq^{\frac{n}{3}}) \ . \end{aligned} \tag{66}$$

We finally prove that $\log_q T_n = \log_q D_n + \mathcal{O}(q^{\frac{n}{3}})$. By Theorem 3, in any family of polynomials in $\mathcal{T}_n$, and any irreducible $g \in \mathcal{I}_k$ for $n/3 < k < n/2$, the corresponding f must be $f = gh$ for some $h \in \mathcal{I}_{n-k}$, thus there are E_k choices for the polynomials in the family that have an irreducible factor of degree k. If $k \leq n/3$, then for any $g \in \mathcal{I}_k$ there are at most $1 + \sum_{d=\lfloor \frac{n}{2} \rfloor +1}^{n-k} I_d$ choices for the corresponding polynomial f in the family. Altogether, we obtain

$$T_n \leq \prod_{k=\lfloor \frac{n}{3} \rfloor +1}^{\lceil \frac{n}{2}-1 \rceil} E_k \cdot \prod_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\{ 1 + \sum_{d=\lfloor \frac{n}{2} \rfloor +1}^{n-k} I_d \right\}^{I_k} \ . \tag{67}$$

Define now B_k as

$$B_k = \left\{ 1 + \sum_{d=\lfloor \frac{n}{2} \rfloor +1}^{n-k} I_d \right\}^{I_k} \leq \left\{ q^{n-k} \right\}^{\frac{1}{k}q^k} \leq q^{\frac{n-k}{k}q^k} \ . \tag{68}$$

Again, this yields $\sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \log_q B_k = \mathcal{O}(q^{\frac{n}{3}})$, which in turn gives us

$$\log_q T_n \leq \log_q D_n + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \log_q B_k = \log_q D_n + \mathcal{O}(q^{\frac{n}{3}}) \ . \tag{69}$$

□

6 Conclusions and perspectives

In this paper we undertook an investigation of mutually orthogonal Latin squares generated through linear bipermutive CA. First, we proved that any bipermutive CA of diameter d and length $2(d-1)$ can be used to generate a Latin square of order $N = q^{d-1}$, with q being the size of the CA alphabet. We then focused on orthogonal Latin squares generated by LBCA, showing a characterization result based on the Sylvester matrix induced by two linear local rules. In particular, we proved that two LBCA generate orthogonal Latin squares if and only if the polynomials associated to their local rules are relatively prime. In the second part of the paper, we determined the number of LBCA pairs over $\mathbb{F}_q$ generating orthogonal Latin squares, i.e. the number of coprime polynomial pairs (f, g) of degree n over $\mathbb{F}_q$ where both f and g have nonzero constant term. In particular, we remarked that the integer sequence generated by the closed-form formula of the recurrence equation for $q = 2$ corresponds to A002450, a sequence which is already known in the OEIS for several other facts not related to polynomials or orthogonal Latin squares. In the last part of the paper, we presented a construction of MOLS generated by LBCA based on irreducible polynomials, and we proved that the size of the resulting MOLS families corresponds to the maximum number of pairwise coprime polynomials with nonzero constant term. Finally, we also showed that the the number of MOLS families that can be obtained by the proposed construction is asymptotically close to the actual number of MOLS families that can be generated by LBCA.

There are several opportunities for further improvements on the results presented in this paper. A first direction for future research is to generalize the study to MOLS generated by *nonlinear* bipermutive CA. In this case, one obviously cannot rely on the characterization result of Theorem 1, since this crucially depends on the use of the Sylvester matrix defined from the transition matrices of linear CA. Preliminary work led by some of the authors of the present paper showed that a necessary condition for a pair of BCA (either linear or nonlinear) to generate orthogonal Latin squares is that their local rules must be *pairwise balanced*, meaning that each of the four pair of bits must occur equally often in the juxtaposition of their truth tables [18]. We believe it is still possible to use the theory of resultants to characterize orthogonal Latin squares generated by nonlinear BCA. As a matter of fact, the main difference between linear and nonlinear pairs is that in the former case the system of equations (14) concerns *univariate* polynomials. On the other hand, in the nonlinear case one can associate *multivariate* polynomials to the local rules, and then use the tools of elimination theory (to which the concept of resultant belongs) to study the invertibility of the resulting systems.

A second extension worth exploring, especially concerning the possible applications related to secret sharing, is to investigate the structure of the inverse of a Sylvester matrix. As described in [17], a family of k MOLS generated by LBCA can be used to design a $(2, k)$-threshold secret where the dealing phase corresponds to evaluating the global rules of the k LBCA to an initial configuration whose left half is the secret, while the right half is randomly chosen. The outputs of the LBCA will be the shares distributed to the k players. In order to reconstruct the secret, any two out of k players must invert the Sylvester matrix associated to their CA (which are assumed to be public) and then multiply it by the vector obtained by concatenating their shares. Hence, an interesting question is whether the reconstruction phase can be carried out again by CA computation, which means that the inverse of the Sylvester matrix related to two LBCA must be of Sylvester type as well. This question has been answered in negative during the Fifth International Students' Olympiad in Cryptography—NSUCRYPTO [10] for LBCA over the finite field $\mathbb{F}_2$. In particular, it has been proved that the only Sylvester matrix over $\mathbb{F}_2$ satisfying this condition is the one defined by the polynomials X^n and $1 + X^n$, which does not correspond to a pair of LBCA since X^n has null constant term. However, the existence question for Sylvester matrices whose inverses are of Sylvester type remains open for larger finite fields.

Finally, another interesting idea would be to extend our investigation to *Mutually Orthogonal Latin Hypercubes* generated by CA, i.e. the generalization of MOLS to higher dimensions. This would be equivalent to study the conditions under which CA can be used to construct orthogonal arrays with strength higher than 2. A characterization result for such kind of orthogonal arrays would allow one to design a general (t, n)-threshold secret sharing scheme based on CA, or equivalently to design linear MDS codes through CA. A possible idea to achieve this result would be to first characterize which subclasses of bipermutive CA generate *Latin hypercubes*. From there, the next step would be to characterize sets of linear CA inducing Orthogonal Latin Hypercubes, which are equivalent to orthogonal arrays [14]. However, we note that there are no straightforward ways to generalize the concept of resultant to more than two polynomials [8]. As a matter of fact, some of the existing generalizations involve matrices which do not correspond to those related to hypercubes generated by CA. To the best of our knowledge, the only resultant matrix for several polynomials that most resemble the CA hypercube case has been defined in [5], which could thus represent a starting point for future work on the subject.

Acknowledgements The authors wish to thank Arthur Benjamin, Curtis Bennett and Igor Shparlinski for their insightful suggestions on how to count the number of pairs of coprime polynomials with nonzero constant term. Further, the authors thank the anonymous reviewers for their useful comments to improve the readability of the paper.

References

1. Allender E., Bernasconi A., Damm C., von zur Gathen J., Saks M.E., Shparlinski I.E.: Complexity of some arithmetic problems for binary polynomials. Comput. Complex. **12**((1–2)), 23–47 (2003).
2. Benjamin A.T., Bennett C.D.: The probability of relatively prime polynomials. Math. Mag. **80**(3), 196–202 (2007).
3. Colbourn C.J.: Construction techniques for mutually orthogonal latin squares. In: Combinatorics Advances, pp. 27–48. Springer, Berlin (1995).
4. del Rey Á.M., Mateus J.P., Sánchez G.R.: A secret sharing scheme based on cellular automata. Appl. Math. Comput. **170**(2), 1356–1364 (2005).
5. Deißler J.: A resultant for Hensel's lemma. arXiv:1301.4073 (2013).
6. Eloranta K.: Partially permutive cellular automata. Nonlinearity **6**(6), 1009–1023 (1993).
7. Gauß C.F.: Disquisitiones arithmeticae. Humboldt-Universität zu Berlin (1801).
8. Gelfand I.M., Kapranov M., Zelevinsky A.: Discriminants, Resultants, and Multidimensional Determinants. Springer, Berlin (2008).
9. Golomb S.W., Posner E.C.: Rook domains, latin squares, affine planes, and error-distributing codes. IEEE Trans. Inf. Theory **10**(3), 196–208 (1964).
10. Gorodilova A., Agievich S., Carlet C., Hou X., Idrisova V., Kolomeec N., Kutsenko A., Mariot L., Oblaukhov A., Picek S., Preneel B., Rosie R., Tokareva N.N.: The Fifth International Students' Olympiad in Cryptography—NSUCRYPTO: Problems and their Solutions. CoRR, arXiv:1906.04480 (2019).
11. Hedlund G.A.: Endomorphisms and automorphisms of the shift dynamical systems. Math. Syst. Theory **3**(4), 320–375 (1969).
12. Hou X., Mullen G.L.: Number of irreducible polynomials and pairs of relatively prime polynomials in several variables over finite fields. Finite Fields Appl. **15**(3), 304–331 (2009).
13. Kari J.: Theory of cellular automata: a survey. Theor. Comput. Sci. **334**(1–3), 3–33 (2005).
14. Keedwell A.D., Dénes J.: Latin Squares and their Applications. Elsevier, Amsterdam (2015).
15. Lidl R., Niederreiter H.: Introduction to Finite Fields and their Applications. Cambridge University Press, Cambridge (1994).
16. MacNeish H.F.: Euler squares. Ann. Math. **23**, 221–227 (1922).
17. Mariot L., Formenti E., Leporati A.: Constructing orthogonal latin squares from linear cellular automata. CoRR, arXiv:1610.00139 (2016).
18. Mariot L., Formenti E., Leporati A.: Enumerating orthogonal latin squares generated by bipermutive cellular automata. In: Proceedings of the Cellular Automata and Discrete Complex Systems—23rd IFIP WG 1.5 International Workshop, AUTOMATA 2017, Milan, Italy, 7–9 June 2017, pp. 151–164 (2017).
19. Mariot L., Leporati A.: Sharing secrets by computing preimages of bipermutive cellular automata. In: Proceedings of the Cellular Automata—11th International Conference on Cellular Automata for Research and Industry, ACRI 2014, Krakow, Poland, 22–25 Sept 2014, pp. 417–426 (2014).
20. Mariot L., Leporati A.: A cryptographic and coding-theoretic perspective on the global rules of cellular automata. Nat. Comput. **17**(3), 487–498 (2018).
21. Mariot L., Leporati A., Dennunzio A., Formenti E.: Computing the periods of preimages in surjective cellular automata. Nat. Comput. **16**(3), 367–381 (2017).

22. Mariot L., Picek S., Leporati A., Jakobovic D.: Cellular automata based S-boxes. Cryptogr. Commun. **11**(1), 41–62 (2019).
23. Montgomery D.C.: Design and Analysis of Experiments. Wiley, Hoboken (2017).
24. Moore C.: Predicting nonlinear cellular automata quickly by decomposing them into linear ones. Phys. D: Nonlinear Phenom. **111**(1–4), 27–41 (1998).
25. Moore C., Drisko A.A., et al.: Algebraic properties of the block transformation on cellular automata. Complex Syst. **10**(3), 185–194 (1996).
26. Pedersen J.: Cellular automata as algebraic systems. Complex Syst. **6**(3), 237–250 (1992).
27. Reifegerste A.: On an involution concerning pairs of polynomials over $\mathbb{F}_2$. J. Comb. Theory Ser. A **90**(1), 216–220 (2000).
28. Stinson D.R.: Combinatorial characterizations of authentication codes. Des. Codes Cryptogr. **2**(2), 175–187 (1992).
29. The Online Encyclopedia of Integer Sequences (OEIS). Sequence A002450. http://oeis.org/A002450. Accessed 12 Apr 2019
30. Vaudenay S.: On the need for multipermutations: Cryptanalysis of MD4 and SAFER. In: Proceedings of the Fast Software Encryption: Second International Workshop, Leuven, Belgium, 14–16 Dec 1994, pp. 286–297 (1994).
31. Wilson R.M.: Concerning the number of mutually orthogonal latin squares. Discret. Math. **9**(2), 181–198 (1974).