

# Structural Properties of Non-Linear Cellular Automata: Permutivity, Surjectivity and Reversibility

Firas Ben Ramdhane<sup>1,3</sup>, Alberto Dennunzio<sup>1</sup>, Luciano Margara<sup>2</sup>, and Giuliamaria Menara<sup>1</sup>

<sup>1</sup> Department of Informatics, Systems and Communications,  
University of Milano-Bicocca, Italy  
`{firas.benramdhane,alberto.dennunzio,giuliamaria.menara}@unimib.it`

<sup>2</sup> Department of Computer Science and Engineering,  
University of Bologna, Cesena, Italy  
`luciano.margara@unibo.it`

<sup>3</sup> University of Sfax, Faculty of Sciences of Sfax, Tunisia.

**Abstract.** This paper explores the algebraic conditions under which a cellular automaton with a non-linear local rule exhibits surjectivity and reversibility. We also analyze the role of permutivity as a key factor influencing these properties and provide conditions that determine whether a non-linear CA is (bi)permutive. Through theoretical results and illustrative examples, we characterize the relationships between these fundamental properties, offering new insights into the dynamical behavior of non-linear CA.

## 1 Introduction

A cellular automaton (CA) is a discrete dynamical system in which each cell updates its state according to local rules, allowing complex global behavior to emerge from simple interactions. CA have been widely employed to model intricate phenomena across diverse scientific fields, including physics [Den88], biology [EEK93], sociology [Heg96], and ecology [Hog88]. Their conceptual simplicity and modeling flexibility have also attracted considerable interest in computer science, particularly in the domain of *cryptology* (see [MMM25] for a comprehensive survey of cryptographic applications).

Among the different classes of CA, linear [DFGM20a,DFGM21,DFM24] and additive [Den24,DFGM20b] CA have received considerable attention due to their well-understood algebraic structure and predictable behavior. In contrast, non-linear CA remain much less explored, although some attempts have been made to study both qualitatively and quantitatively the characteristics of such CA [Lan90,Wue94,Wue99]: this lack of characterization presents both a challenge and an opportunity.

From a theoretical perspective, studying non-linear CA is compelling, as their non-linearity introduces a level of dynamical complexity not present in

their linear counterparts. This complexity opens new avenues for analysis and classification, and may reveal behaviors that are fundamentally different from those observed in well-studied classes.

In addition, this complexity and unpredictability make non-linear CA promising candidates for applications where such properties are desirable - most notably in cryptography: while linear CA have already been employed in the construction of various cryptographic primitives, the potential of non-linear CA in this domain remains largely untapped.

The goal of this paper is to take a step toward bridging this gap by initiating a deeper theoretical study of non-linear CA, starting from classical results addressing the injectivity and surjectivity questions. It is widely acknowledged that characterizing local rules which make a CA injective or surjective proves arduous in the unrestricted case [Kar00] therefore, given the complexity of the issue at hand, we limit our analysis to the class of non-linear  $j$ -separated CA, i.e. CA with diameter  $d$  and local rule  $f$  defined as:

$$f(x_1, \dots, x_{d+1}) = a_j x_j^{q_j} + \pi(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_{d+1}),$$

where  $a_j \in \mathbb{Z}_m^*$ ,  $q_j$  is a non negative integer, and  $\pi : \mathbb{Z}_m^d \rightarrow \mathbb{Z}_m$  is any map (for more details see Definition 1).

Exploiting the structural properties of  $j$ -separated CA, we are able to provide a permutivity characterization in Lemma 3 and Proposition 1. Then, building on these results and restricting to the class of  $LR$ -separated CA, where the local rule  $f$  can be written, for  $1 \leq \ell \leq r \leq d+1$ , as

$$f(x_1, \dots, x_{d+1}) = a_\ell x_\ell^{q_\ell} + \pi(x_{\ell+1}, \dots, x_{r-1}) + a_r x_r^{q_r},$$

we prove first in Theorem 3 that a  $LR$ -separated  $F$  is surjective if and only if it is either  $\ell$ -permutive or  $r$ -permutive, and then in Theorem 4 that  $F$  is reversible if and only if it is reversible shift-like.

**Theorem (cf. Theorems 3 and 4).** Let  $F$  be a  $LR$ -separated CA over the finite ring  $\mathbb{Z}_m$ , for any integer  $m \geq 3$ , and let  $\ell$  (resp.  $r$ ) be the leftmost (resp. rightmost) positions of  $F$ . Then:

1.  $F$  is surjective if and only if  $\gcd(q_\ell, \varphi(m)) = 1$  or  $\gcd(q_r, \varphi(m)) = 1$ .
2.  $F$  is injective if and only if  $\ell = r$  and  $\gcd(q_\ell, \varphi(m)) = 1$ .

Besides theoretical results, we also provide illustrative examples to better clarify the relationships between these fundamental properties, offering new insights into the dynamical behavior of non-linear CA.

## Outline

The paper is organized as follows. In Section 2 we recall some relevant algebraic background and notions about the dynamical properties of CA, and we introduce the class of  $j$ -separated non-linear CA, which will be essential in the remainder

of this work. Further, in Section 4 we proceed by exhibiting algebraic conditions for the local rule  $f$  under which the CA is leftmost (or rightmost) permutive. Finally, in Sections 5 and 6 we present the core results of the paper, providing characterization theorems for surjective and reversible  $j$ -separated CA.

### Acknowledgements

This work was partially supported by the PRIN 2022 PNRR project ‘‘Cellular Automata Synthesis for Cryptography Applications (CASCA)’’ (P2022MPFRT) funded by the European Union – Next Generation EU, and by the HORIZON-MSCA-2022-SE-01 project 101131549 ‘‘Application-driven Challenges for Automata Networks and Complex Systems (ACANCOS)’’.

## 2 Terminology and Background

In this section, we give the preliminary definitions and results needed for the rest of the paper. For a comprehensive introduction on the theory of CA see [BKR12, Section 1] and [Kur03, Chapter 5].

We start with some terminology from word combinatorics. An *alphabet*  $A$  is a finite set of symbols, called *letters*. In this paper, we take  $A = \mathbb{Z}_m$ , the set of integers modulo  $m$ . A *finite word* over an alphabet  $A$  is a finite sequence of letters from  $A$ . The length of a finite word  $u$ , denoted by  $|u|$ , is the number of letters it contains. The unique word of length 0 is called the *empty word* and is denoted by  $\lambda$ . A *configuration* (or *bi-infinite word*)  $x = \dots x_{-2}x_{-1}x_0x_1x_2\dots$  over  $A$  is an infinite concatenation of letters from  $A$  indexed by  $\mathbb{Z}$ . For integers  $n \leq m$ , we denote by  $x_{[n,m]} = x_nx_{n+1}\dots x_{m-1}x_m$  the subword of  $x$  from position  $n$  to  $m$ , where  $[n,m] = [n,m] \cap \mathbb{Z}$ ; further, we will indicate by  $u^\infty$  the *constant word*, i.e. the word constructed by concatenating the same letter  $u$  infinitely many times. The set of all finite (resp. bi-infinite) words over  $A$  is denoted by  $A^*$  (resp.  $A^\mathbb{Z}$ ), and for each  $n \in \mathbb{N}$ , the set of words of length  $n$  is denoted by  $A^n$ . Most classically, the set  $A^\mathbb{Z}$  is endowed with the product topology of the discrete topology on each copy of  $A$ . The topology defined on  $A^\mathbb{Z}$  is metrizable, corresponding to the *Cantor distance* defined as follows:

$$\mathfrak{d}_C(x, y) = 2^{-\min\{|n||x_n \neq y_n, n \in \mathbb{Z}\}}, \forall x \neq y \in A^\mathbb{Z}, \text{ and } \mathfrak{d}_C(x, x) = 0, \forall x \in A^\mathbb{Z}.$$

This space, called the *Cantor space*, is compact, totally disconnected and perfect.

This topological framework naturally leads to the definition of a *topological dynamical system*, which provides a formal setting for studying the evolution of configurations under continuous transformations. Recall that a *topological dynamical system* is a pair  $(X_d, F)$ , where  $X_d = (X, d)$  is a compact metric space and  $F: X \rightarrow X$  is a continuous map. When  $X$  consists of symbolic configurations, such as elements of  $A^\mathbb{Z}$ , the system is called a *symbolic dynamical system*.

CA are a classical example of such systems. Formally, a CA is a map  $F: A^\mathbb{Z} \rightarrow A^\mathbb{Z}$  such that there exist an integer  $\rho \geq 0$  and a local rule  $f: A^{2\rho+1} \rightarrow A$

satisfying, for all  $x \in A^{\mathbb{Z}}$  and  $i \in \mathbb{Z} : F(x)_i = f(x_{\llbracket i-\rho, i+\rho \rrbracket})$ . We refer to  $\rho$  as the *radius* and  $d = 2\rho$  as the *diameter* of the CA. A fundamental example of a CA is the *shift map*, defined on  $A^{\mathbb{Z}}$  by  $\sigma(x)_i = x_{i+1}$  for all  $i \in \mathbb{Z}$ . This map plays a central role in the theory of symbolic dynamics, particularly in the characterization of CA. In fact, a classical result by Curtis, Hedlund, and Lyndon [Hed69] states that a function  $F: A^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}}$  is a CA if and only if it is continuous (with respect to the product topology) and commutes with the shift, that is,  $F(\sigma(x)) = \sigma(F(x))$  for all  $x \in A^{\mathbb{Z}}$ . Another result by Hedlund characterizes surjective CA. Recall that a CA is said to be *surjective* (resp. *injective*) if its global rule  $F$  is onto (resp. one-to-one) and *bijective* if  $F$  is both onto and one-to-one.

To state this result, we define the extension of the local rule  $f$ , denoted by  $f^*$ , of a CA  $F$  with diameter  $d$ , on  $A^*$  as follows:  $f^*(u)_i = f(u_{\llbracket i, i+d \rrbracket})$  if  $i < |u| - d$  and the empty word otherwise.

**Theorem 1 ([Hed69]).** *A CA  $F$  with local rule  $f$  and diameter  $d$  is surjective if and only if for all  $u \in A^* \setminus \{\lambda\}$ ,  $\#f^{*-1}(u) = (\#A)^d$ .*

Building on the previously mentioned result, one can determine whether a CA is surjective by analyzing the number of preimages of each finite word. However, this method typically involves a very high computational complexity. In this paper, we provide a necessary and sufficient condition, based on the local rule, for the global rule of a specific class of non-linear CA to be surjective (resp. injective), while avoiding the high computational complexity of exhaustive preimage analysis.

A well-known result states that every injective CA is also surjective [Kur03, Corollary 5.27]. As a consequence, a CA is bijective if and only if it is injective. Moreover, the inverse of a bijective CA is itself a CA and thus a CA  $F$  is injective if and only if it is *reversible*, i.e. there is a CA  $G$  such that  $F \circ G = G \circ F = id$ , where  $id$  is the identity function, for more details one can see [Kar05].

A distinct and particularly relevant class of CA also ensures surjectivity: these are the so-called *permutive* CA. We say that a CA  $F$  of diameter  $d$  and local rule  $f$  is *permutive at position  $i$*  (with  $1 \leq i \leq d+1$ ) if, for every  $u \in A^{i-1}$ , every  $v \in A^{d-i+1}$ , and every  $b \in A$ , there exists a unique  $a \in A$  such that  $f(uav) = b$ . In other words, when all variables except the  $i$ -th are fixed, the function  $f$  acts as a permutation in the  $i$ -th variable. In particular, if  $i = 1$  (respectively,  $i = d+1$ ), we say that  $F$  is *left* (respectively, *right*) permutive. A CA is said to be *bipermutive* if it is both left and right permutive, and simply *permutive* if it satisfies at least one of these conditions. According to [Kur03, Proposition 5.22], every permutive CA is surjective.

We now turn our attention to an algebraic notion and a result which we will rely on in the upcoming results. Recall that the *Euler's totient function* [EDA12], denoted  $\varphi(n)$ , is defined as the number of positive integers less than or equal to  $n$  that are coprime to  $n$ . Formally,

$$\varphi(n) = \#\{k \in \mathbb{Z} \text{ such that } 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\}.$$

Also, recall that every function from a finite field  $\mathbb{F}$  to itself can be represented as a polynomial over  $\mathbb{F}$ . For completeness, we include a proof of this fact.

**Lemma 1.** *Any function from a finite field  $\mathbb{F}$  to  $\mathbb{F}$  can be represented as a polynomial over  $\mathbb{F}$ .*

*Proof.* Let  $g$  be any function from  $\mathbb{F}$  to  $\mathbb{F}$ . Since  $\mathbb{F}$  is a finite field, then we have a finite list of all the elements of  $\mathbb{F}$ , label them  $h_1, h_2, \dots, h_n$ , where  $h_i \neq h_j$  for any distinct  $i$  and  $j$ . We want to write  $g$  as an  $n$  degree polynomial  $g(x) = a_0 + a_1x + \dots + a_nx^n$  that has the value  $g(h_i)$  at  $h_i$  for every  $i$ . This is equivalent to solving the following system:

$$\begin{aligned} a_0 + a_1(h_1) + a_2(h_1)^2 + \dots + a_n(h_1)^n &= g(h_1) \\ &\dots\dots\dots \\ a_0 + a_1(h_n) + a_2(h_n)^2 + \dots + a_n(h_n)^n &= g(h_n). \end{aligned}$$

This linear system can be represented with the help of the Vandermonde matrix,  $V$ :

$$V = \begin{bmatrix} 1 & h_1 & h_1^2 & \dots & h_1^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & h_n & h_n^2 & \dots & h_n^{n-1} \end{bmatrix}.$$

Now if we let  $a = [a_0, a_1, \dots, a_n]^T$  and let  $g = [g(h_1), g(h_2), \dots, g(h_n)]^T$ , then we can find our coefficients by solving the system  $Va = g$  for  $a$ . The question of whether the polynomial exists reduces to the question of whether the determinant of  $V$  is non-zero. The determinant of the Vandermonde matrix is  $\prod_{i < j} (h_i - h_j)$ , [HJ12]. Since every one of our  $h_i$  are distinct, the determinant is non-zero and therefore a unique solution exists. So for every function from  $\mathbb{F}$  to  $\mathbb{F}$ , we can find a polynomial over  $\mathbb{F}$  that agrees with that function at every point.  $\square$

*Remark 1.* This result fails to extend to any  $\mathbb{Z}_m$  where  $m$  is not prime. Indeed, let  $p(x)$  be a polynomial in  $\mathbb{Z}_4[x]$ . Then  $p(0) \equiv p(2) \pmod 2$  and also  $p(1) \equiv p(3) \pmod 2$ . Thus it is impossible to recover any function  $g : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$  such that  $0 \rightarrow 1, 1 \rightarrow 0, 2 \rightarrow 3$  and  $3 \rightarrow 2$  by evaluating any polynomial.

While we acknowledge, from Remark 1, that restricting our focus to polynomial local rules over  $\mathbb{Z}_m$  will result in an ultimately incomplete analysis, we choose to start by studying this simpler case, as it will serve as a foundation allowing us to later address the more general scenario. However, it is worth pointing out that, because of Proposition 1, when  $m$  is prime (i.e., in the context of finite fields) the investigation of polynomial local rules amounts to an exhaustive analysis of non-linear CA.

Although we are restricting our focus to polynomial functions, the study remains complex due to the wide range of behaviors these functions exhibit. To manage this complexity, we further narrow our attention to a specific class of non-linear CA defined by a local rule  $f$  such that  $f$  is a multivariate polynomial with (at least) one variable separated from the others. We end this section by introducing this notion, which we will rely on in the remainder of the paper.

**Definition 1.** Let  $F$  be a CA over the finite ring  $\mathbb{Z}_m$  with  $m \geq 3$ , defined by a local rule  $f : \mathbb{Z}_m^{d+1} \rightarrow \mathbb{Z}_m$  of the form:

$$f(x_1, \dots, x_{d+1}) = a_j x_j^{q_j} + \pi(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_{d+1}),$$

1. We say that  $F$  is separated in position  $j$ , or simply  $j$ -separated.
2. If  $j = \ell$  (resp.  $j = r$ ), where  $a_\ell$  (resp.  $a_r$ ) is the leftmost (resp. rightmost) non-zero coefficient, then  $F$  is said to be leftmost (resp. rightmost) separated.
3. We say that  $F$  is LR-separated if it is both leftmost and rightmost separated.
4. We say that  $F$  is totally separated if the local rule is of the form

$$f(x_1, \dots, x_{d+1}) = \sum_{i=1}^{d+1} a_i x_i^{q_i},$$

*Remark 2.* If  $F$  is a LR-separated CA with local rule  $f$  and diameter  $d$ , then  $f$  necessarily takes one of the following forms:

1.  $f(x_1, \dots, x_{d+1}) = a_\ell x_\ell^{q_\ell}$ , in which case  $\ell = r$  and  $F$  is said to be *shift-like*.
2.  $f(x_1, \dots, x_{d+1}) = a_\ell x_\ell^{q_\ell} + \pi(x_{\ell+1}, \dots, x_{r-1}) + a_r x_r^{q_r}$ , where  $1 \leq \ell < r \leq d+1$ , such that  $a_\ell$  (resp.  $a_r$ ) is the leftmost (resp. rightmost) non-zero coefficient, and  $\pi : \mathbb{Z}_m^{r-\ell-1} \rightarrow \mathbb{Z}_m$  is an arbitrary map.

Notice that in both cases it is possible to write  $f(x_1, \dots, x_{d+1}) = a_\ell x_\ell^{q_\ell} + \pi(x_{\ell+1}, \dots, x_{r-1}) + a_r x_r^{q_r}$  with  $\pi : \mathbb{Z}_m^h \rightarrow \mathbb{Z}_m$ , where  $h = \max\{0, r - \ell - 1\}$ . We will refer to  $\ell$  (resp.  $r$ ) as the *leftmost* (resp. *rightmost*) position of  $F$ .

It is important to note that this work focuses on the case  $A = \mathbb{Z}_m$  with  $m \geq 3$ , as the case  $m = 2$  corresponds to linear CA, which have already been extensively studied in the literature (see, for example, [ION83] and [MM99]).

### 3 Quadratic CA on finite fields

Among non-linear CA, a particularly notable subclass is that of quadratic CA. We begin by proving that no such automaton can be surjective over a finite field  $\mathbb{Z}_p$ . Although this result follows from Theorem 3, we include it here explicitly, as the constructive argument provides valuable insight into the structural constraints specific to this class.

**Definition 2.** A CA  $F$  with diameter  $d$  and local rule  $f : \mathbb{Z}_m^{d+1} \rightarrow \mathbb{Z}_m$  is quadratic if  $f$  is a quadratic form on  $\mathbb{Z}_m^{d+1}$  (i.e.  $f(au) = a^2 f(u)$  for any  $u \in \mathbb{Z}_m^{d+1}$  and  $a \in \mathbb{Z}_m$ , and, the map  $(u, v) \mapsto f(u+v) - f(u) - f(v)$  is bilinear form that is linear in each argument separately).

**Lemma 2.** Let  $F$  be a totally separated CA over the finite field  $\mathbb{Z}_p$ , where  $p$  is prime number with  $p \geq 3$ , i.e. the local rule  $f$  is given by

$$f(x_1, \dots, x_{d+1}) = \sum_{i=1}^{d+1} a_i x_i^{q_i},$$

where each  $a_i \in \mathbb{Z}_p$ . If every  $q_i$  is an even positive integers for all  $i \in \llbracket 1, d+1 \rrbracket$ , then the global map  $F$  is not surjective.

*Proof.* Suppose that such CA  $F$  is surjective. Then, there exists  $h \in \llbracket 1, d+1 \rrbracket$  such that  $a_h \neq 0$ . For  $j \in \llbracket 1, d+1 \rrbracket$ , let us denote by  $S_j$ , the subset of  $\llbracket 0, \frac{p-1}{2} \rrbracket^{d+1}$  such that  $(x_1, \dots, x_{d+1}) \in S_j$  if and only if  $f(x_1, \dots, x_{d+1}) = a_h$  and there is  $i_1 < i_2 < \dots < i_j \in \llbracket 1, d+1 \rrbracket$  such that  $x_k = 0$  if  $k \in \{i_1, \dots, i_j\}$  and  $x_k > 0$  otherwise. Note that,  $\bigcup_{j=0}^d S_j \neq \emptyset$  since  $(0, \dots, 0, 1, 0, \dots, 0) \in S_d$  where 1 is at position  $h$ . Moreover, it is clear that if  $(x_1, \dots, x_{d+1})$  is a preimage of  $a_h$  by  $f$ , then any change in the signs of  $x_i$  still yields a preimage of  $a_h$  by  $f$  (since all  $q_i$  are positive even integers). Hence, if  $(x_1, \dots, x_{d+1}) \in S_j$  then we can find exactly  $2^{d+1-j}$  different elements of  $f^{-1}(a_h)$  by only changing signs of  $x_i$ . Thus, we can deduce that:

$$\#f^{-1}(a_h) = \sum_{j=0}^d 2^{d-j+1} \#S_j.$$

Hence,  $\#f^{-1}(a_h)$  is an even number. On the other hand, by Theorem 1 and the surjectivity of  $F$ , we obtain  $\#f^{-1}(a_h) = p^d$  which contradicts the fact that  $p^d$  is an odd number (as  $p$  is an odd prime number). Therefore, we can conclude that  $F$  is not surjective.  $\square$

We can specialize Lemma 2 to the context of quadratic local rules, yielding a corresponding result for quadratic CA.

**Corollary 1.** *There is no surjective quadratic CA over  $\mathbb{Z}_p$  for any prime  $p \geq 3$ .*

*Proof.* Let  $F$  be a CA with diameter  $d$  and quadratic local rule  $f$ . Using the classical decomposition of quadratic forms into sums of squares (see for example [Ser12, Chapter 4]),  $f$  can be expressed as:

$$f(x_1, x_2, \dots, x_{d+1}) = a_1 x_1^2 + a_2 x_2^2 + \dots + a_{d+1} x_{d+1}^2,$$

where  $a_i \in \mathbb{Z}_p$  for all  $i \in \{1, \dots, d+1\}$ . Therefore, by Lemma 2, we conclude that  $F$  is not surjective.  $\square$

**Corollary 2.** *Let  $F$  be a totally separated CA over  $\mathbb{Z}_p$  for any prime  $p \geq 3$ . If the powers  $q_i$ 's are all even positive integers, then  $F$  is not injective.*

*Proof.* Suppose all the  $q_i$ 's are all even positive integers. Then thanks to Lemma 2,  $F$  could not be surjective and thus it is not injective (since any injective CA is surjective).  $\square$

*Remark 3.* Although we do not provide formal definitions here, it follows from Corollary 2, together with [Kur03, Theorems 5.49 and 5.50] and [CM96], that CA satisfying the hypotheses of Corollary 2 are neither positively expansive nor transitive, two properties that are typically linked to chaotic behavior in symbolic dynamical systems. For precise definitions, see [Kur03, Definitions 2.39 and 1.15].

## 4 Permutivity

In this section, we focus on the study of the permutivity property of non-linear  $j$ -separated CA.

**Lemma 3.** *Take a finite ring  $\mathbb{Z}_m$ , where  $m$  is a positive integer. Let  $F$  be a  $j$ -separated CA of diameter  $d$ , so the local rule  $f$  can be written as*

$$f(x_1, \dots, x_{d+1}) = ax_j^n + g(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_{d+1}),$$

where  $a \in \mathbb{Z}_m$  is invertible and  $g : \mathbb{Z}_m^d \rightarrow \mathbb{Z}_m$  is any map.

Then  $F$  is permutive in position  $j$  if and only if  $\gcd(n, \varphi(m)) = 1$ , where  $\varphi(m)$  is the Euler's totient function of  $m$ .

*Remark 4.* In particular, if  $F$  is  $(d+1)$ -separated [resp. 1-separated] then  $F$  is right-permutive [resp. left-permutive] if and only if  $\gcd(n, \varphi(m)) = 1$ .

*Proof.* The proof of the Lemma is a consequence the Chinese Remainder Theorem and the well-known fact [DF04] that the polynomial  $h : \mathbb{Z}_{p^e} \rightarrow \mathbb{Z}_{p^e}$ , where  $p$  is a prime number and  $e$  is a positive integer, defined as

$$h(x) = ax^n + g(x_1, \dots, x_d)$$

is bijective if and only if  $a \in \mathbb{Z}_{p^e}$  is invertible and  $\gcd(n, \varphi(p^e)) = 1$ .  $\square$

*Remark 5.* Notice that it follows from Lemma 3 that is  $m$  is a prime number and  $\mathbb{Z}_m$  is the finite field with  $m$  elements, then  $F$  is permutive in position  $j$  if and only if  $\gcd(n, m-1) = 1$ , since  $\varphi(m) = m-1$  for  $m$  prime.

It was shown by Hermite<sup>4</sup> in [Her63] that a polynomial  $f$  over a finite field  $\mathbb{Z}_p$  is invertible if and only if  $f$  has exactly one root in  $\mathbb{Z}_p$  and for each integer  $t$  with  $1 < t < p-2$ ,  $t \not\equiv 0 \pmod{p}$ , the reduction of  $[f(x)]^t \pmod{(x^p - x)}$  has degree less than  $p-2$ . Therefore, a CA over  $\mathbb{Z}_p$  with local rule  $f(x_1, \dots, x_{d+1}) = \pi(x_{d+1}) + g(x_1, \dots, x_d)$  [resp.  $f(x_1, \dots, x_{d+1}) = \pi(x_1) + g(x_2, \dots, x_{d+1})$ ] is right-permutive [resp. left-permutive] if and only if the two aforementioned conditions hold for the polynomial  $\pi(x)$ .

We now prove a different characterization of permutive CA over finite fields that, while not a sufficient condition, only relies on the local rule  $f$  being reducible in  $\mathbb{Z}_p$ .

**Proposition 1.** *Let  $F$  be a CA over the finite field  $\mathbb{Z}_p$  with diameter  $d$  defined by the local rule*

$$f(x_1, \dots, x_{d+1}) = \pi(x_j) + g(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_{d+1}),$$

where  $\pi(x) \in \mathbb{Z}_p[x]$  is a reducible polynomial and  $g$  is any map  $g : \mathbb{Z}_p^d \rightarrow \mathbb{Z}_p$ . Then  $F$  is permutive in position  $j$  if  $\gcd(\pi'(x), x^p - x) = 1$ , where  $\pi'(x)$  is the formal derivative of  $\pi(x)$ , and  $x^p - x$  is the polynomial whose roots are all elements of  $\mathbb{Z}_p$ .

<sup>4</sup> This result was later extended by Dickson in [Dic96] to polynomials over  $\mathbb{Z}_q$  for general  $q$ .

*Proof.* For  $x_1, \dots, x_d \in \mathbb{Z}_p$ , let  $h : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  be the map defined as

$$h(x) = \pi(x) + g(x_1, \dots, x_d).$$

Assume that  $\gcd(\pi'(x), x^p - x) = 1$ . We want to show that the map  $h$  is injective.

1. *No repeated roots:* Since  $\gcd(\pi'(x), x^p - x) = 1$ , the polynomials  $\pi'(x)$  and  $x^p - x$  have no common roots. This means that the derivative  $\pi'(x)$  does not vanish at any element of  $\mathbb{Z}_p$ , implying that  $h(x)$  has no repeated roots in  $\mathbb{Z}_p$ .
2. *Injectivity:* Because from the previous point  $\pi'(x) \neq 0$  for any  $x \in \mathbb{Z}_p$ , the polynomial  $h(x)$  does not map any two distinct elements of  $\mathbb{Z}_p$  to the same value. If it did, say  $h(x_1) = h(x_2)$  for some  $x_1 \neq x_2 \in \mathbb{Z}_p$ , then  $h(x) - h(x_1)$  would have a repeated root, implying that  $\pi'(x)$  would share a root with  $x^p - x$ , contradicting the assumption that  $\gcd(\pi'(x), x^p - x) = 1$ .

Thus,  $h(x)$  is injective because it maps distinct elements of  $\mathbb{Z}_p$  to distinct values.  $\square$

*Remark 6.* Under the hypotheses of Proposition 1, if the polynomial  $\pi(x)$  is irreducible then in particular  $h(x)$  cannot be permutive. Therefore, a CA  $F$  with local rule an irreducible polynomial is never permutive in  $\mathbb{Z}_p$ .

## 5 Surjectivity

We now provide some alternative characterization results on surjectivity for the class of  $LR$ -separated CA. We start by recalling some useful facts from [MP13].

**Definition 3 ([MP13, Def. 8.2.1]).** Let  $\mathbb{F}_p$  be a finite field of characteristic  $p$ . A polynomial  $f \in \mathbb{F}_p[x_1, \dots, x_n]$  is a permutation polynomial in  $n$  variables over  $\mathbb{F}_p$  if the equation  $f(x_1, \dots, x_n) = \alpha$  has exactly  $p^{n-1}$  solutions in  $\mathbb{F}_p^n$  for each  $\alpha \in \mathbb{F}_p$ .

**Theorem 2 ([MP13, Theorem 8.2.9]).** Let  $f \in \mathbb{F}_p[x_1, \dots, x_n]$  be of the form

$$f(x_1, \dots, x_n) = g(x_1, \dots, x_m) + h(x_{m+1}, \dots, x_n), \quad 1 \leq m < n.$$

If at least one of  $g$  and  $h$  is a permutation polynomial over  $\mathbb{F}_p$  then  $f$  is a permutation polynomial over  $\mathbb{F}_p$ . If  $p$  is prime, then the converse also holds.

The following is a direct consequence of the results above.

**Proposition 2.** Let  $F$  be a  $LR$ -separated CA with local rule  $f$  over  $\mathbb{Z}_p$ , for any prime  $p \geq 3$  and let  $\ell$  (resp.  $r$ ) be the leftmost (resp. rightmost) position of  $F$ .

1. If the polynomial  $\pi$  (defined as in Remark 2) is any non-permutation polynomial, then  $F$  is surjective if and only if  $\gcd(q_\ell, p-1) = 1$  or  $\gcd(q_r, p-1) = 1$ .
2. If  $F$  is a totally separated surjective CA, then there is at least one  $j \in \llbracket \ell, r \rrbracket$  such that  $\gcd(q_j, p-1) = 1$ .

The following result provides a complete characterization of surjective  $LR$ -separated CA.

**Theorem 3.** *Let  $F$  be a  $LR$ -separated CA over the finite ring  $\mathbb{Z}_m$ , for any integer  $m \geq 3$ , and let  $\ell$  (resp.  $r$ ) be the leftmost (resp. rightmost) position of  $F$ . Then  $F$  is surjective if and only if  $\gcd(q_\ell, \varphi(m)) = 1$  or  $\gcd(q_r, \varphi(m)) = 1$ .*

*Remark 7.* As in the case of Lemma 3, if  $m$  is a prime number it turns out that  $F$  is surjective if and only if  $\gcd(q_\ell, m-1) = 1$  or  $\gcd(q_r, m-1) = 1$ .

*Proof.* We will prove the two implications separately.

$\Leftarrow$  Suppose without loss of generality that  $\gcd(q_r, \varphi(m)) = 1$  (in case  $\gcd(q_\ell, \varphi(m)) = 1$  the proof is similar). Let  $G$  be the CA with the local rule  $g : \mathbb{Z}_m^{r-\ell+1} \rightarrow \mathbb{Z}_m$  defined as

$$g(x_\ell, \dots, x_r) = a_\ell x_\ell^{q_\ell} + \pi(x_{\ell+1}, \dots, x_{r-1}) + a_r x_r^{q_r}.$$

Since  $\gcd(q_r, \varphi(m)) = 1$ , then by Lemma 3,  $g$  is right-permutive, and thus  $G$  is surjective. Therefore for every  $y \in \mathbb{Z}_m^{\mathbb{Z}}$  there exists  $x \in \mathbb{Z}_m^{\mathbb{Z}}$  such that  $G(x) = y$ . Finally, because of the definition of the local rule  $f$  we can conclude that  $F(x) = y$ , meaning  $F$  is surjective.

$\Rightarrow$  Suppose now that  $F$  is surjective. In order to show that at least one between the exponents  $q_\ell$  and  $q_r$  has to be coprime with  $\varphi(m)$  we will proceed through the following steps:

1. first we will assume, by contradiction, that both  $\gcd(q_\ell, \varphi(m))$  and  $\gcd(q_r, \varphi(m))$  are strictly bigger than 1;
2. then, given any letter  $a$  on the alphabet  $\mathbb{Z}_m$  we will count the preimages of the words  $\gamma\alpha a\beta\delta$ , where  $\alpha, \beta, \gamma, \delta$  are letters in  $\mathbb{Z}_m$ ;
3. using the assumption that  $q_\ell$  and  $q_r$  and both not coprime with  $\varphi(m)$  we will obtain that the number of preimages of some words  $\gamma\alpha a\beta\delta$  is strictly less than  $m^d$ , thus contradicting Hedlund's Theorem 1.

Let  $a \in \mathbb{Z}_m$ . Since  $\gcd(q_\ell, \varphi(m)) > 1$  and  $\gcd(q_r, \varphi(m)) > 1$ , for every  $u \in f^{-1}(a)$ , there exist  $\alpha, \beta \in \mathbb{Z}_m$  such that

$$\# \left\{ w \in f^{*-1}(\alpha a \beta) \mid w_{[1, n]} = u \right\} \geq 4.$$

Moreover, since  $F$  is surjective and thanks to Hedlund's theorem, we obtain,  $\#f^{-1}(a) = m^d$ , and thus, for  $f^{-1}(a) = \{u^{(i)} \mid 1 \leq i \leq m^d\}$ , there exists a sequence of words  $(\alpha^{(i)}, \beta^{(i)})_{1 \leq i \leq m^d}$  such that for all  $1 \leq i \leq m^d$ ,

$$\# \left\{ w \in f^{*-1}(\alpha^{(i)} a \beta^{(i)}) \mid w_{[1, n]} = u^{(i)} \right\} \geq 4.$$

On the other hand, since  $\# \{(\alpha^{(i)}, \beta^{(i)}) \mid \alpha^{(i)}, \beta^{(i)} \in \mathbb{Z}_m, 1 \leq i \leq m^d\} \leq m^2$ , there exists  $1 \leq j \leq m^d$  such that:

$$\# \left\{ u \in f^{-1}(a) \mid f(\gamma u \delta) = \alpha^{(j)} a \beta^{(j)} \text{ for } \gamma, \delta \in \mathbb{Z}_m \right\} \geq m^{d-2}.$$

Then for every  $a$  there exist  $\alpha, \beta \in \mathbb{Z}_m$  such that

$$\#f^{-1}(\alpha a \beta) \geq 4m^{d-2}. \quad (1)$$

Thus, from Equation 1 and from the fact that, by Hedlund's theorem, the number of preimages of the word  $\alpha a \beta$  is  $m^{d+2}$ , we have that for every  $(\alpha', \beta') \neq (\alpha, \beta)$  it holds that

$$\#f^{-1}(\alpha' a \beta') \leq \frac{m^{d+2} - 4m^{d-2}}{m^2 - 1}.$$

So, for every  $\alpha, \beta \in \mathbb{Z}_m$  we have

$$4m^{d-3} \leq \#f^{-1}(\alpha a \beta) \leq \frac{m^{d+2} - 4m^{d-2}}{m^2 - 1} \leq m^d.$$

Repeating this construction, we see that for every  $v = \alpha a \beta$  there exist  $\gamma, \delta \in \mathbb{Z}_m$  such that

$$\#f^{-1}(\gamma v \delta) \geq 16m^{d-4},$$

and such that for every  $(\gamma', \delta') \neq (\gamma, \delta)$  it holds that

$$\#f^{-1}(\gamma' v \delta') \leq \frac{\frac{m^{d+2} - 4m^{d-2}}{m^2 - 1} - 16m^{d-4}}{m^2 - 1} < m^d,$$

which is a contradiction.  $\square$

We conclude this section with an example that highlights an important point: although there is a strong connection between surjectivity and permutivity, a CA being surjective does not necessarily imply that it is permutive also in the non-linear case.

*Example 1.* Let  $F$  be the CA over  $\mathbb{Z}_7$  with local rule  $f$  given by:

$$f(a, b, c) = b + c^2 \pmod{3}, \forall a, b, c \in \mathbb{Z}_7.$$

It is clear that  $F$  could not be right (resp. left) permutive since for all  $a \neq b \in \mathbb{Z}_7$  and all  $c, d \in \mathbb{Z}_7$ ,  $f(a, c, d) = f(b, c, -d)$ . However,  $F$  is a surjective CA thanks to Theorem 3.

## 6 Reversibility

This section is devoted to the study of reversibility of  $LR$ -separated CA.

**Lemma 4.** *Let  $F$  be a  $LR$ -separated CA over  $\mathbb{Z}_m$ , for any integer  $m \geq 3$ , and let  $\ell$  (resp.  $r$ ) be the leftmost (resp. rightmost) position of  $F$  with  $\ell < r$ . If  $F$  is  $\ell$ -permutive and  $r$ -permutive, then  $F$  is not injective.*

*Remark 8.* The authors are aware that the validity of the result can be deduced as an implication of the fact that bipermutive CA are positively expansive, and therefore cannot be injective. Nevertheless, we decide to include an alternative proof, as it offers a constructive approach that highlights the dynamics involved.

*Proof.* Let  $F$  be a  $LR$ -separated CA with diameter  $d$  and local rule  $f$  over  $\mathbb{Z}_m$ . Following the idea of Remark 2,  $f$  can be written as follows:

$$f(x_1, \dots, x_{d+1}) = a_\ell x_\ell^{q_\ell} + \pi(x_{\ell+1}, \dots, x_{r-1}) + a_r x_r^{q_r}.$$

Since  $F$  is  $\ell$ -permutive and  $r$ -permutive, the maps  $g(x) = a_\ell x^{q_\ell}$  and  $h(x) = a_r x^{q_r}$  are invertible. Hence, there is  $b_\ell, c_r \in \mathbb{Z}_m \setminus \{0\}$  such that  $g(b_\ell) \equiv 1 \pmod{m}$  and  $h(c_r) \equiv -1 \pmod{m}$ . Let us denote  $a = \pi(0, \dots, 0)$ . Since  $g$  and  $h$  are invertible, one can construct two configurations  $y \neq y'$  such that:

- $y_{[\ell, r]} = b_\ell 0 \dots 0 c_r$  and  $y'_{[\ell, r]} = 00 \dots 00$ .
- For all  $i > r$ : the letter  $y_i$  (resp.  $y'_i$ ) is the solution of the equation  $h(x) + \pi(y_{i-r+\ell+1}, \dots, y_{i-1}) + g(y_{i-r+\ell}) = a$ , (resp.  $h(x) + \pi(y'_{i-r+\ell+1}, \dots, y'_{i-1}) + g(y'_{i-r+\ell}) = a$ ).
- For all  $i < \ell$ : the letter  $y_i$  (resp.  $y'_i$ ) is the solution of the equation  $g(x) + \pi(y_{i+1}, \dots, y_{i+r-\ell-1}) + h(y_{i+r-\ell}) = a$ , (resp.  $g(x) + \pi(y'_{i+1}, \dots, y'_{i+r-\ell-1}) + h(y'_{i+r-\ell}) = a$ ).

By construction,  $F(y) = F(y') = a^\infty$ . Hence,  $F$  is not injective since  $y \neq y'$ .  $\square$

**Theorem 4.** *Let  $F$  be a  $LR$ -separated CA with diameter  $d = 2\rho$  and local rule  $f$  over  $\mathbb{Z}_m$ , for any integer  $m \geq 3$ , and let  $\ell$  (resp.  $r$ ) be the leftmost (resp. rightmost) position of  $F$ . Then  $F$  is injective if and only if  $\ell = r$  and  $\gcd(q_\ell, \varphi(m)) = 1$ .*

*Remark 9.* As in the case of Proposition 3, if  $m$  is a prime number, then,  $F$  is injective if and only if  $\ell = r$  and  $\gcd(q_\ell, m-1) = 1$ .

*Proof.* We will prove the two implications separately.

- $\Leftarrow$  If  $\ell = r$ , then  $f$  is the monomial  $f(x_1, \dots, x_{d+1}) = a_\ell x_\ell^{q_\ell}$ , and being  $\gcd(q_\ell, \varphi(m)) = 1$  the injectivity of  $F$  follows directly.
- $\Rightarrow$  Suppose  $F$  is injective, and assume by contradiction that  $\ell < r$ . If both  $\gcd(q_r, \varphi(m)) = 1$  and  $\gcd(q_\ell, \varphi(m)) = 1$  then  $F$  cannot be injective thanks to Lemma 4, so say  $\gcd(q_r, \varphi(m)) \neq 1$ . Let  $y \in \mathbb{Z}_m^{\mathbb{Z}}$  and set for all  $n \in \mathbb{N}$ , for  $k = n + \rho$ :

$$X_n = \{x \in \mathbb{Z}_m^{\mathbb{Z}} \mid x_{[-k, k]} \neq y_{[-k, k]} \text{ and } f^*(x_{[-k, k]}) = f^*(y_{[-k, k]})\}.$$

Note that for every  $n \in \mathbb{N}$ ,  $X_n$  is non-empty since  $\gcd(q_r, \varphi(m)) \neq 1$ . Moreover, for all  $n \in \mathbb{N}$  we can rewrite  $X_n$  as the intersection of two closed sets: the set of finite words of length  $2(n + \rho) + 1$  different from  $y_{[-n-\rho, n+\rho]}$ ,

and the set of configurations  $x$  such that  $f^*(x_{\llbracket -n-\rho, n+\rho \rrbracket}) = f^*(y_{\llbracket -n-\rho, n+\rho \rrbracket})$ . That is, for all  $n \in \mathbb{N}$ , for  $k = n + \rho$ :

$$X_n = \left( \bigcup_{u \in \mathbb{Z}_m^{2k+1} \setminus \{y_{\llbracket -k, k \rrbracket}\}} [u] \right) \cap \{x \in \mathbb{Z}_m^{\mathbb{Z}} \mid f^*(x_{\llbracket -k, k \rrbracket}) = f^*(y_{\llbracket -k, k \rrbracket})\}.$$

Therefore, it holds for every  $n \in \mathbb{N}$ , that  $X_n$  is a non-empty closed set. In addition, since clearly  $X_{n+1} \subseteq X_n$ , then by the compactness of the Cantor space, there exists  $x \in \bigcap_{n \in \mathbb{N}} X_n$ . Hence, there exists  $x \neq y$  such that  $F(x) = F(y)$ , contradicting the hypothesis that  $F$  is injective.  $\square$

**Corollary 3.** *Let  $F$  be a LR-separated CA over  $\mathbb{Z}_m$ , where  $m$  is an integer with  $m \geq 3$ . Then  $F$  is bijective if and only if  $\ell = r$  and  $\gcd(q_\ell, p - 1) = 1$ .*

*Example 2.* Let  $F$  be a CA with local rule:  $f(a, b, c) = a^4 + 3b \pmod{7}$ . The global rule  $F$  is not injective since  $F((56)^\infty) = F((43)^\infty) = (62)^\infty$ . However,  $P(x) = x^4 + 3x \pmod{7}$ , is a permutation polynomial over  $Z_7$ .

*Example 3.* Let  $F$  be a CA with local rule:  $f(a, b, c) = a^3 + 2b + c^2 \pmod{5}$ . The global rule  $F$  is not injective since  $F((10)^\infty) = F((3)^\infty) = 2^\infty$ . We can take also  $F((30)^\infty) = F((41)^\infty) = (34)^\infty$ . However,  $P(x) = x^3 + 2x + x^2 \pmod{5}$ , is a permutation polynomial over  $Z_5$  (even it is the sum of two non permutation polynomials  $P_1(x) = x^3 + 2x \pmod{5}$  and  $P_2(x) = x^2 \pmod{5}$ ).

## 7 Conclusions and Future Directions

In this work, we analyzed the structural properties of non-linear CA, focusing on permutivity, surjectivity, and reversibility. We introduced the class of  $j$ -separated non-linear CA and established algebraic characterizations of the above mentioned properties for this class of CA.

Our findings show that permutivity plays a central role in determining surjectivity and reversibility. Specifically, we showed that a  $j$ -separated non-linear CA is surjective if and only if it is either left- or right-permutive. Additionally, we proved that reversibility is equivalent to the CA being surjective with the local rule  $f$  depending only on one variable. These results contribute to a deeper understanding of non-linear CA dynamics and provide a framework for identifying their computational potential.

Beyond theoretical results, we presented illustrative examples to clarify the interplay between permutivity, surjectivity, and reversibility.

Although our analysis (Theorem 4 in particular) shows that the class of  $j$ -separated non-linear CA is not especially suited for cryptographic applications, it is the authors' belief that future investigation of broader classes of non-linear CA should lead to a complete exploitation of the non-linear rules computational complexity to produce secure cryptographic primitives.

We conclude by proposing some questions, related to the above discussion, that we find particularly interesting and worth exploring:

1. In the case of finite rings it holds that every non-linear function is a polynomial, thus restricting significantly the possible non-linearity structures. We noticed in Remark 1 that this does not hold, for example, for finite rings: what happens in the case of a general alphabet  $A$ ?
2. In this work we focus on uniform CA, meaning all local interactions are determined by the same rule. How do our results transform in the case of non-uniform CA (i.e. a CA allowing different local rules)?

## References

- BKR12. Thomas Bäck, Joost N Kok, and G Rozenberg. *Handbook of natural computing*. Springer, Heidelberg, 2012.
- CM96. Bruno Codenotti and Luciano Margara. Transitive cellular automata are sensitive. *The American Mathematical Monthly*, 103(1):58–62, 1996.
- Den88. BH1988CoPhC Denby. Neural networks and cellular automata in experimental high energy physics. *Computer Physics Communications*, 49(3):429–448, 1988.
- Den24. Alberto Dennunzio. Easy to check algebraic characterizations of dynamical properties for linear ca and additive ca over a finite abelian group. In *International Workshop on Cellular Automata and Discrete Complex Systems*, pages 23–34. Springer, 2024.
- DF04. David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.
- DFGM20a. Alberto Dennunzio, Enrico Formenti, Darij Grinberg, and Luciano Margara. Chaos and ergodicity are decidable for linear cellular automata over  $(\mathbb{Z}/m\mathbb{Z})^n$ . *Information Sciences*, 539:136–144, 2020.
- DFGM20b. Alberto Dennunzio, Enrico Formenti, Darij Grinberg, and Luciano Margara. Dynamical behavior of additive cellular automata over finite abelian groups. *Theoretical Computer Science*, 843:45–56, 2020.
- DFGM21. Alberto Dennunzio, Enrico Formenti, Darij Grinberg, and Luciano Margara. An efficiently computable characterization of stability and instability for linear cellular automata. *Journal of computer and system sciences*, 122:63–71, 2021.
- DFM24. Alberto Dennunzio, Enrico Formenti, and Luciano Margara. An efficient algorithm deciding chaos for linear cellular automata over  $(\mathbb{Z}/m\mathbb{Z})^n$  with applications to data encryption. *Information Sciences*, 657:119942, 2024.
- Dic96. Leonard Eugene Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *The Annals of Mathematics*, 11(1/6):65–120, 1896.
- EDA12. Leonhard Euler, Artur Diener, and Alexander Aycock. Theoremata arithmetica nova methodo demonstrata. *arXiv preprint arXiv:1203.1993*, 2012.
- EEK93. G Bard Ermentrout and Leah Edelstein-Keshet. Cellular automata approaches to biological modeling. *Journal of theoretical Biology*, 160(1):97–133, 1993.
- Hed69. Gustav A Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Mathematical systems theory*, 3(4):320–375, 1969.
- Heg96. Rainer Hegselmann. Understanding social dynamics: The cellular automata approach. In *Social science microsimulation*, pages 282–306. Springer, 1996.

- Her63. Charles Hermite. Sur les fonctions de sept lettres. *C. R. Acad. Sci. Paris*, 2(57):750–757, 1863.
- HJ12. Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge university press, 2012.
- Hog88. Paulien Hogeweg. Cellular automata as a paradigm for ecological modeling. *Applied mathematics and computation*, 27(1):81–100, 1988.
- ION83. Masanobu Ito, Nobuyasu Osato, and Masakazu Nasu. Linear cellular automata over  $\mathbb{Z}_m$ . *Journal of Computer and System sciences*, 27(1):125–140, 1983.
- Kar00. Jarkko Kari. Linear cellular automata with multiple state variables. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 110–121. Springer, 2000.
- Kar05. Jarkko Kari. Reversible cellular automata. In *Developments in Language Theory: 9th International Conference, DLT 2005, Palermo, Italy, July 4-8, 2005. Proceedings 9*, pages 57–68. Springer, 2005.
- Kur03. P Kurka. Topological and symbolic dynamics. *Cours Specialises*, 11, 2003.
- Lan90. Chris G Langton. Computation at the edge of chaos: Phase transitions and emergent computation. *Physica D: nonlinear phenomena*, 42(1-3):12–37, 1990.
- MM99. Giovanni Manzini and Luciano Margara. A complete and efficiently computable topological classification of  $d$ -dimensional linear cellular automata over  $\mathbb{Z}_m$ . *Theoretical computer science*, 221(1-2):157–177, 1999.
- MMM25. Luca Manzoni, Luca Mariot, and Giuliamaria Menara. Combinatorial designs and cellular automata: A survey. *arXiv preprint arXiv:2503.10320*, 2025.
- MP13. Gary L Mullen and Daniel Panario. *Handbook of finite fields*, volume 17. CRC press Boca Raton, 2013.
- Ser12. Jean-Pierre Serre. *A course in arithmetic*, volume 7. Springer Science & Business Media, 2012.
- Wue94. Andrew Wuensche. *Complexity in one-D cellular automata: Gliders, basins of attraction and the Z parameter*. University of Sussex, School of Cognitive and Computing Sciences, 1994.
- Wue99. Andrew Wuensche. Classifying cellular automata automatically: Finding gliders, filtering, and relating space-time patterns, attractor basins, and the  $z$  parameter. *Complexity*, 4(3):47–66, 1999.