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

Firas Ben Ramdhane[1], Alberto Dennunzio[1,*], Luciano Margara[2] and Giuliamaria Menara[1]

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

[2]Department of Computer Science and Engineering, University of Bologna, Cesena, Italy

Abstract

We provide the conditions under which a cellular automaton defined by certain classes of non-linear local rules exhibits surjectivity and reversibility. For the latter, the condition turns out to be a characterization. We also analyze the role of permutivity as a key factor influencing these properties and provide conditions that determine whether a non-linear CA in such classes is (bi)permutive.

Keywords

Discrete Dynamical Systems, Cellular Automata, Non-linear Cellular Automata,

1. Introduction

A cellular automaton (CA) is a discrete dynamical system consisting of a regular grid of cells where each cell updates its own state according to a local rule on the basis of the states of the neighboring cells and in a synchronous way with all the other cells, allowing complex global behavior of the system to emerge from simple interactions. CA have been extensively studied from a theoretical point of view(see for instance [1, 2]. Moreover, CA have been widely used to model intricate phenomena in different scientific fields, including physics [3], biology [4], sociology [5], ecology [6], and *cryptography* [7]. Their conceptual simplicity and modeling flexibility have also attracted considerable interest in computer science, particularly in the domain of *cryptography* (see [7] for a comprehensive survey of cryptographic applications).

Among the different classes of CA, linear CA have received considerable attention due to their well-understood algebraic structure and predictable behavior (see [8] for a comprehensive bibliography and recent results on linear CA). Such CA have a local rule which can be expressed as a linear combination of the involved variables. In contrast, non-linear CA, *i.e.,* , CA that are not linear, remain much less explored, although some attempts have been made to study both qualitatively and quantitatively the characteristics of such CA [9, 10, 11]. This lack 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 which is 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.

In this paper we present the beginning of the theoretical study of a class 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 [12]. Therefore, given the complexity of the issue at hand, we limit our analysis to the class of non-linear j-separated CA (see Definition 1). Exploiting the structural properties of j-separated CA, we

ICTCS 2025: Italian Conference on Theoretical Computer Science, September 10–12, 2025, Pescara, Italy

*Corresponding author.

firas.benramdhane@unimib.it (F. Ben Ramdhane); alberto.dennunzio@unimib.it (A. Dennunzio); luciano.margara@unibo.it (L. Margara); giuliamaria.menara@unimib.it (G. Menara)

are able to provide a permutivity characterization. Then, building on these results and restricting to the class of LR-separated CA, *i.e.,* non-linear CA that are separated in their both leftmost and rightmost positions (see Definition 1), we state in Theorem 2 that if a LR-separated non-linear CA F is either ℓ-permutive or r-permutive then it is surjective, while in Theorem 3, we state that F is reversible if and only if it is a reversible shift-like. Besides theoretical results, we also provide some illustrative examples to better clarify the relationships between these fundamental properties, offering new insights into the dynamical behavior of non-linear CA.

We stress that this short paper is an extended abstract of [13] to which the reader is referred for a complete version that includes all the proofs.

2. Terminology and Background

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 λ. 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 $x_{[\![n,m]\!]} = x_n x_{n+1} \cdots x_{m-1}x_m$ the subword of x from position n to m, where $[\![n, m]\!] = [n, m] \cap \mathbb{Z}$; further, we will indicate by u^∞ 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.

Formally, a CA is a map $F\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ such that there exist an integer $\rho \geq 0$ and a local rule $f\colon A^{2\rho+1} \to A$ satisfying, for all $x \in A^{\mathbb{Z}}$ and $i \in \mathbb{Z} : F(x)_i = f(x_{[\![i-\rho,i+\rho]\!]})$. We refer to ρ as the *radius* and $d = 2\rho$ as the *diameter* of the CA.

A distinct and particularly relevant class of CA 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 [14, 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* [15], 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 $\mathbb{F}$.

As mentioned in the introduction, to manage the complexity of non-linear local rules, we 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 $f : \mathbb{Z}_m^{d+1} \to \mathbb{Z}_m$ 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_ℓ (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*

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

Remark 1. *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_ℓ (resp. a_r) is the leftmost (resp. rightmost) non-zero coefficient, and $\pi : \mathbb{Z}_m^{r-\ell-1} \to \mathbb{Z}_m$ 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 $\pi : \mathbb{Z}_m^h \to \mathbb{Z}_m$, where $h = \max\{0, r-\ell-1\}$.
We will refer to ℓ (resp. r) as the leftmost *(resp.* rightmost*) position of F.*

It is also important to stress 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, [16] and [17]).

3. Quadratic CA on finite fields

Among non-linear CA, a particularly notable subclass is that of quadratic CA. It directly turns out that no quadratic CA can be surjective over a finite field $\mathbb{Z}_p$.

Definition 2. *A CA F with diameter d and local rule $f : \mathbb{Z}_m^{d+1} \to \mathbb{Z}_m$ 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 1. *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 $i \in [\![1, d+1]\!]$, then the global map F is not surjective.

We can specialize Lemma 1 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 $p \geq 3$.*

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.*

4. Permutivity

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

Lemma 2. *Let F be a j-separated CA over $\mathbb{Z}_m$ and with diameter d , where m is a positive integer and its local rule f can be written as*

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

where $a \in \mathbb{Z}_m$ is invertible and $g : \mathbb{Z}_m^d \to \mathbb{Z}_m$ is any map.
It holds that F is permutive in position j if and only if $\gcd(n, \varphi(m)) = 1$.

Remark 2. *In particular, if F is $(d+1)$-separated [resp. 1-separated] then F is right-permutive [resp. left-permutive] if and only if* $\gcd(n, \varphi(m)) = 1$.

Remark 3. *Making reference to Lemma 2, it holds that if m is a prime number, 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 Hermitein [18] that a polynomial f over a finite field $\mathbb{F}_p$ is invertible if and only if f has exactly one root in $\mathbb{F}_p$ and for each integer t with $1 < t < p-2$, $t \not\equiv 0 \mod p$, the reduction of $[f(x)]^t \mod (x^p - x)$ has degree less than $p-2$. Therefore, a CA over $\mathbb{Z}_p$ with local rule $f(x_1, \ldots, x_{d+1}) = \pi(x_{d+1}) + g(x_1, \ldots, x_d)$ [resp. $f(x_1, \ldots, x_{d+1}) = \pi(x_1) + g(x_2, \ldots, x_{d+1})$] is right-permutive [resp. left-permutive] if and only if the two aforementioned conditions hold for the polynomial $\pi(x)$.

Hermite's criterion can be simplified in the context of the finite field on p elements $\mathbb{Z}_p$ [19], where it holds that a polynomial $f \in \mathbb{Z}_p[x]$ is invertible on $\mathbb{Z}_p$ if and only if $\gcd(f'(x), x^p - x) = 1$, where $f'(x)$ is the first derivative of $f(x)$, and $x^p - x$ is the polynomial whose roots are all elements of $\mathbb{Z}_p$. We thus have the following characterization of permutive CA over the finite field $\mathbb{Z}_p$.

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

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

where $\pi(x) \in \mathbb{Z}_p[x]$ is a polynomial and g is any map $g : \mathbb{Z}_p^d \to \mathbb{Z}_p$. Then F is permutive in position j if and only if $\deg(\pi) < p$ *and* $\gcd(\pi'(x), x^p - x) = 1$.

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 [20].

Definition 3 ([20, Def. 8.2.1]). *Let $\mathbb{F}_p$ be the finite field with p elements. A polynomial $f \in \mathbb{F}_p[x_1, ..., x_n]$ is a permutation polynomial in n variables over $\mathbb{F}_p$ if the equation $f(x_1, ..., x_n) = \alpha$ has exactly p^{n-1} solutions in $\mathbb{F}_p^n$ for each $\alpha \in \mathbb{F}_p$.*

Theorem 1 ([20, Theorem 8.2.9]). *Let $f \in \mathbb{F}_p[x_1, ..., x_n]$ be of the form*

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

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 ℓ (resp. r) be the leftmost (resp. rightmost) position of F.*

1. *If the polynomial π (defined as in Remark 1) 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 $j \in [\![\ell, r]\!]$ such that* $\gcd(q_j, p-1) = 1$.

The following result is a direct consequence of Lemma 2 and provides a partial characterization of surjective LR-separated CA.

Theorem 2. *Let F be a LR-separated CA over the finite ring $\mathbb{Z}_m$, for any integer $m \geq 3$, and let ℓ (resp. r) be the leftmost (resp. rightmost) position of F. If either* $\gcd(q_\ell, \varphi(m)) = 1$ *or* $\gcd(q_r, \varphi(m)) = 1$, *then F is surjective.*

6. Reversibility

This section is devoted to the study of reversibility for LR-separated CA. The following results hold.

Theorem 3. *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 ℓ (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 4. *As in the case of Proposition 2, if m is a prime number, then, F is injective if and only if $\ell = r$ and $\gcd(q_\ell, m-1) = 1$.*

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 $\gcd(q_\ell, \rho(m)) = 1$.*

Example 1. *Let F be a CA with local rule: $f(a,b,c) = a^4 + 3b \mod 7$. The global rule F is not injective since $F((56)^\infty) = F((43)^\infty) = (62)^\infty$. However, $P(x) = x^4 + 3x \mod 7$, is a permutation polynomial over $\mathbb{Z}_7$.*

Example 2. *Let F be a CA with local rule: $f(a,b,c) = a^3 + 2b + c^2 \mod 5$. 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, $P(x) = x^3 + 2x + x^2 \mod 5$, is a permutation polynomial over $\mathbb{Z}_5$ (even it is the sum of two non permutation polynomials $P_1(x) = x^3 + 2x \mod 5$ and $P_2(x) = x^2 \mod 5$).*

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 provided conditions for the above mentioned properties in this class of CA.

Our findings show that permutivity plays a central role in determining surjectivity and reversibility. Specifically, we provided a condition under which a j-separated nonlinear CA is surjective. Additionally, we stated that reversibility is equivalent to the CA being surjective and with 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.

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

1. What is the complete characterization of surjectivity for LR-separated non-linear CA over $\mathbb{Z}_m$ with $m \geq 3$?
2. What can be said about the dynamical properties (like sensitivity to the initial conditions, topological transitivity, chaos, etc.) for some classes of non-linear CA?
3. In this work we focused 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)?

Acknowledgments

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

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] J. Kari, Theory of cellular automata: A survey, Theor. Comput. Sci. 334 (2005) 3–33.

[2] T. Ceccherini-Silberstein, M. Coornaert, Cellular Automata and Groups, Springer Monographs in Mathematics, Springer, 2010.

[3] B. Denby, Neural networks and cellular automata in experimental high energy physics, Computer Physics Communications 49 (1988) 429–448.

[4] G. B. Ermentrout, L. Edelstein-Keshet, Cellular automata approaches to biological modeling, Journal of theoretical Biology 160 (1993) 97–133.

[5] R. Hegselmann, Understanding social dynamics: The cellular automata approach, in: Social science microsimulation, Springer, 1996, pp. 282–306.

[6] P. Hogeweg, Cellular automata as a paradigm for ecological modeling, Applied mathematics and computation 27 (1988) 81–100.

[7] L. Manzoni, L. Mariot, G. Menara, Combinatorial designs and cellular automata: A survey, arXiv preprint arXiv:2503.10320 (2025).

[8] A. Dennunzio, Easy to check algebraic characterizations of dynamical properties for linear CA and additive CA over a finite abelian group, volume 14782 of *Lecture Notes in Computer Science*, Springer, 2024, pp. 23–34.

[9] C. G. Langton, Computation at the edge of chaos: Phase transitions and emergent computation, Physica D: nonlinear phenomena 42 (1990) 12–37.

[10] A. 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.

[11] A. Wuensche, Classifying cellular automata automatically: Finding gliders, filtering, and relating space-time patterns, attractor basins, and the z parameter, Complexity 4 (1999) 47–66.

[12] J. Kari, Linear cellular automata with multiple state variables, in: H. Reichel, S. Tison (Eds.), STACS 2000, volume 1770 of *LNCS*, Springer-Verlag, 2000, pp. 110–121.

[13] F. B. Ramdhane, A. Dennunzio, L. Margara, G. Menara, Structural properties of non-linear cellular automata: Permutivity, surjectivity and reversibility, CoRR abs/2504.15949 (2025). URL: https://doi.org/10.48550/arXiv.2504.15949. doi:10.48550/ARXIV.2504.15949. arXiv:2504.15949.

[14] P. Kůrka, Topological and symbolic dynamics (2004).

[15] L. Euler, A. Diener, A. Aycock, Theoremata arithmetica nova methodo demonstrata, arXiv preprint arXiv:1203.1993 (2012).

[16] M. Ito, N. Osato, M. Nasu, Linear cellular automata over zm, Journal of Computer and System sciences 27 (1983) 125–140.

[17] G. Manzini, L. Margara, A complete and efficiently computable topological classification of d-dimensional linear cellular automata over zm, Theoretical computer science 221 (1999) 157–177.

[18] C. Hermite, Sur les fonctions de sept lettres., C. R. Acad. Sci. Paris 2 (1863) 750–757.

[19] R. Lidl, H. Niederreiter, Finite fields, 20, Cambridge university press, 1997.

[20] G. L. Mullen, D. Panario, Handbook of finite fields, volume 17, CRC press Boca Raton, 2013.