Chaos and ergodicity are decidable for linear cellular automata over (Z/mZ)n

Chaos and ergodicity are decidable for linear cellular automata over $(\mathbb{Z}/m\mathbb{Z})^n$

Alberto Dennunzio[a], Enrico Formenti[b], Darij Grinberg[c], Luciano Margara[d]

[a]*Dipartimento di Informatica, Sistemistica e Comunicazione, Università degli Studi di Milano-Bicocca, Viale Sarca 336/14, 20126 Milano, Italy*
[b]*Université Côte d'Azur, CNRS, I3S, France*
[c]*Mathematisches Forschungsinstitut Oberwolfach, Schwarzwaldstr. 9-11, 77709 Oberwolfach-Walke, Germany*
[d]*Department of Computer Science and Engineering, University of Bologna, Cesena Campus, Via Sacchi 3, Cesena, Italy*

Abstract

We prove that important properties describing complex behaviours as ergodicity, chaos, topological transitivity, and topological mixing, are decidable for one-dimensional linear cellular automata (LCA) over $(\mathbb{Z}/m\mathbb{Z})^n$ (Theorem 6 and Corollary 7), a large and important class of cellular automata (CA) which are able to exhibit the complex behaviours of general CA and are used in applications. In particular, we provide a decidable characterization of ergodicity, which is known to be equivalent to all the above mentioned properties, in terms of the characteristic polynomial of the matrix associated with LCA. We stress that the setting of LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ with $n > 1$ is more expressive, gives rise to much more complex dynamics, and is more difficult to deal with than the already investigated case $n = 1$. The proof techniques from [23, 25] used when $n = 1$ for obtaining decidable characterizations of dynamical and ergodic properties can no longer be exploited when $n > 1$ for achieving the same goal. Indeed, in order to get the decision algorithm (Algorithm 1) we need to prove a non trivial result of abstract algebra (Theorem 5) which is also of interest in its own.

We also illustrate the impact of our results in real-world applications concerning the important and growing domain of cryptosystems which are often based on one-dimensional LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ with $n > 1$. As a matter of facts, since cryptosystems have to satisfy the so-called confusion and diffusion properties (ensured by ergodicity and chaos, respectively, of the involved LCA) Algorithm 1 turns out to be an important tool for building chaotic/ergodic one-dimensional linear CA over $(\mathbb{Z}/m\mathbb{Z})^n$ and, hence, for improving the existing methods based on them.

Keywords: Cellular Automata, Linear Cellular Automata, Decidability, Symbolic dynamics, Complex Systems

1. Introduction

We study the class of one-dimensional *linear cellular automata (LCA)* over the alphabet $(\mathbb{Z}/m\mathbb{Z})^n$, i.e., one-dimensional *cellular automata (CA)* with local rule defined by $n \times n$ matrices with elements in $\mathbb{Z}/m\mathbb{Z}$. Despite their simplicity, they are able to exhibit the complex behaviors of general CA (for recent results and an up-to date bibliography on CA, see for instance [19, 12, 10, 1], while for related models we refer the reader to [16, 18, 17, 15]). Moreover, they are used in many applications in several scientific domains [5, 21]. We recall that LCA over the alphabet $(\mathbb{Z}/m\mathbb{Z})^n$ with $n = 1$ have been extensively studied. In that case, all the dynamical and ergodic properties, including those we will deal with in this paper, have been characterized and proved to be decidable [23, 25, 6, 7, 11].

Although LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ with $n > 1$ are used in many important applications such as design of secret sharing schemes, data encryption, data compression and image processing, there are few results regarding decidable characterizations of the dynamical properties for such LCA. Actually, the setting $n > 1$, which is more expressive and gives rise to much more complex dynamics than $n = 1$ (see, for instance [14, 13]), is more difficult

Email addresses: alberto.dennunzio@unimib.it (Alberto Dennunzio), enrico.formenti@unice.fr (Enrico Formenti), darijgrinberg@gmail.com (Darij Grinberg), luciano.margara@unibo.it (Luciano Margara)

to deal with. The proof techniques from [23, 25] used when $n = 1$ for obtaining decidable characterizations of dynamical and ergodic properties can no longer be exploited when $n > 1$ for achieving the same goal. Only injectivity and surjectivity have been characterized (in terms of decidable conditions on the matrix associated with the LCA [4, 24]).

In this paper, we prove that important properties describing CA complex behaviours as chaos, ergodicity, topological transitivity, and topological mixing are decidable (as well as equivalent) for one-dimensional LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ (Theorem 6 and Corollary 7). In particular, we provide a decidable characterization for ergodicity in terms of the characteristic polynomial of the matrix associated to LCA. In order to get such a characterization and then the decision algorithm, namely Algorithm 1, we need to prove a non trivial result of abstract algebra which is also of interest in its own (Theorem 5).

Let us explain the importance of our results in applications by considering the growing domain of cryptosystems. Indeed, one-dimensional LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ with $n > 1$ are often involved in designing cryptographic techniques. Moreover, it is well-known that safe cryptosystems have to satisfy the so-called confusion and diffusion properties (along with some variants of them). Since ergodicity and chaotic behavior are the dynamical counterparts of confusion and diffusion [2], Corollary 7 and Algorithm 1 are important tools to be used in the applications for building chaotic/ergodic one-dimensional LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ and, hence, for improving the existing techniques which are based on them. We show how our results can be used regarding two representative applications in the domain of cryptosystems, namely, a secret sharing scheme and a data encryption method. Clearly, they turn out to be very useful in many domains and for all those numerous applications where such CA are involved and a chaotic behavior is required.

Acknowledgements

DG thanks the Mathematisches Forschungsinstitut Oberwolfach for its hospitality.

2. Basic notions

Let Q be a finite set (also called *alphabet*). A *CA configuration* (or, briefly, a *configuration*) is any function from $\mathbb{Z}$ to Q. Given a configuration $c \in Q^{\mathbb{Z}}$ and any integer $i \in \mathbb{Z}$, the value of c in position i is denoted by c_i. The set $Q^{\mathbb{Z}}$, called *configuration space*, is as usual equipped with the standard Tychonoff distance d.

A *one-dimensional CA* (or, briefly, a *CA*) over Q is a pair $(Q^{\mathbb{Z}}, \Delta)$, where $\Delta : Q^{\mathbb{Z}} \to Q^{\mathbb{Z}}$ is the uniformly continuous transformation (called *global rule*) defined as $\forall c \in Q^{\mathbb{Z}}, \forall i \in \mathbb{Z}, \Delta(c)_i = \delta(c_{i-r}, \dots c_{i+r})$, for some fixed natural number $r \in \mathbb{N}$ (called *radius*) and some fixed function $\delta : Q^{2r+1} \to Q$ (called *local rule* of radius r).

In the context of one-dimensional CA, whenever the term *linear* is involved the alphabet Q is $\mathbb{K}^n$, where $\mathbb{K} = \mathbb{Z}/m\mathbb{Z}$ for some natural $m > 1$. Both $\mathbb{K}^n$ and $(\mathbb{K}^n)^{\mathbb{Z}}$ become $\mathbb{K}$-modules in the obvious (i.e., entrywise) way. For any natural $n > 0$, I_n shall always stand for the $n \times n$ identity matrix (over whatever ring we are using). Moreover, if $\mathbb{K}$ is any commutative ring and $A \in \mathbb{K}^{n\times n}$ is an $n \times n$-matrix over $\mathbb{K}$, then χ_A shall denote the characteristic polynomial $\det(tI_n - A) \in \mathbb{K}[t]$ of A. Furthermore, we denote by $\mathbb{K}[X, X^{-1}]$ the set of Laurent polynomials with coefficients in $\mathbb{K}$. Finally, if f and g are two polynomials over a field K, then "$f \perp g$" will mean that the polynomials f and g are coprime (this makes sense, since the polynomial ring $K[t]$ is a Euclidean domain).

Let $\mathbb{K} = \mathbb{Z}/m\mathbb{Z}$ for some natural $m > 1$ and let $n \in \mathbb{N}$ with $n \geq 1$.

A local rule $\delta : (\mathbb{K}^n)^{2r+1} \to \mathbb{K}^n$ of radius r is said to be *linear* if it is defined by $2r+1$ matrices $A_{-r}, \dots, A_r \in \mathbb{K}^{n\times n}$ as follows: $\forall (x_{-r}, \dots, x_r) \in (\mathbb{K}^n)^{2r+1}, \delta(x_{-r}, \dots, x_r) = \sum_{i=-r}^{r} A_i \cdot x_i$.

A one-dimensional *linear CA (LCA)* over $\mathbb{K}^n$ is a CA Δ based on a linear local rule. The Laurent polynomial $M(X) = \sum_{i=-r}^{r} A_i X^{-i} \in \mathbb{K}^{n\times n}[X, X^{-1}]$ is said to be the *the matrix associated with* Δ. We recall that the dynamical behavior of LCA over $\mathbb{K}^n$ when $n = 1$ has been successfully investigated by means of $M(X)$ (see [23, 25]). In that case, all the dynamical and ergodic properties, including those we will deal with in this paper, have been characterized and, in particular, they turn out to be decidable. For this reason, in the sequel we will deal with naturals $n > 1$.

3. Deciding chaos, ergodicity, transitivity, and mixing for one-dimensional linear CA over $(\mathbb{Z}/m\mathbb{Z})^n$

This section contains the major result of the paper, namely, the decidability of chaos ergodicity, topological transitivity, and mixing for one-dimensional linear CA over $(\mathbb{Z}/m\mathbb{Z})^n$. We recall that a CA $(Q^{\mathbb{Z}}, \Delta)$ is *chaotic* if it is sensitive to the initial conditions, topologically transitive and regular (for the definitions of such standard properties, including mixing, the reader is referred for instance to [14, 13, 20, 25]), while it is *ergodic* with respect to the normalized Haar measure $\mu : \mathcal{M} \to [0,1]$ if for every set $E \in \mathcal{M}$ it holds that $\left(E = \mathcal{F}^{-1}(E)\right) \Rightarrow (\mu(E) = 0 \text{ or } \mu(E) = 1)$, where $\mathcal{M}$ is the usual collection of measurable sets of $Q^{\mathbb{Z}}$.

First of all, as an immediate consequence of our results in [14, 13], we can state that all these properties are equivalent for one-dimensional linear CA over the alphabet $Q = (\mathbb{Z}/m\mathbb{Z})^n$.

Theorem 1. *Let $\left((\mathbb{K}^n)^{\mathbb{Z}}, \Delta\right)$ be a one-dimensional LCA over $\mathbb{K}^n$, where $\mathbb{K} = \mathbb{Z}/m\mathbb{Z}$ for some natural $m > 1$. Then, Δ is ergodic iff it is transitive iff it is mixing iff it is chaotic.*

We want to stress that the following theorem has been fundamental for proving our result in [14, 13], in particular that topological transitivity implies ergodicity for the larger class of additive CA over a finite abelian group.

Theorem 2. *Let $\mathcal{F}$ be any endomorphism of a compact abelian group G with normalized Haar measure μ. Then, the following conditions are equivalent:* (1) *$\mathcal{F}$ is ergodic;* (2) *$\mathcal{F}$ is surjective and $\mathcal{F}^h - I$ is surjective for all $h \in \mathbb{N}$ (I is the identity map)*

Moreover, we want to clarify that Theorem 2 consists of an extrapolation from [26, Th. 1] which states that five conditions (namely, items (i), ..., (v) in that theorem) involving properties of the endomorphism $\mathcal{F}$ are equivalent. We have reported in Theorem 2 only two among them, since the cycle of implications (i)$\Rightarrow$ (ii) $\Rightarrow$ $\cdots$ (v) $\Rightarrow$ (i) considered in the proof of [26, Th. 1] turns out be false, while (1) and (2) are actually equivalent. Indeed, such an equivalence is ensured by [27, Th. 1.10] which states that (iii) (i.e., (1)) is equivalent to (iv) which in turn is correctly proved to be equivalent to (v) (i.e. (2)) in [26].

3.1. The decision algorithm

The following result is another ingredient used in the sequel.

Theorem 3 ([4, 24])**.** *Let $\left((\mathbb{K}^n)^{\mathbb{Z}}, \Delta\right)$ be a one-dimensional LCA over $\mathbb{K}^n$, where $\mathbb{K} = \mathbb{Z}/m\mathbb{Z}$ for some natural $m > 1$, and let $M(X)$ be the matrix associated with Δ. Then, Δ is surjective if and only if $\det M(X)$ is the Laurent polynomial associated with a surjective one-dimensional LCA over $\mathbb{K}$.*

Remark 4. When $\mathbb{K} = \mathbb{Z}/p^k\mathbb{Z}$ for some prime p and some integer $k > 0$, for every matrix $M(X) \in \mathbb{K}^{n\times n}[X, X^{-1}]$ it holds that $\det M(X)$ is the Laurent polynomial associated with a surjective one-dimensional LCA over $\mathbb{K}$ iff $p \nmid \det M(X)$, i.e., equivalently, $\det(M(X) \mod p) \neq 0$, where $(M(X) \mod p)$ means that all the coefficients of $M(X)$ are taken modulo p.

We stress that Theorem 2 used in conjunction with both Theorem 3 and a generalisation of [6, Lemma 3.2] to $(\mathbb{Z}/m\mathbb{Z})^n$ already provides a semi-algorithm for deciding ergodicity for one-dimensional LCA over $\mathbb{K}^n$. However, obtaining a real algorithm is not a trivial task at all. Indeed, as illustrated in the sequel, it will require to prove the following non trivial result of abstract algebra which is also of interest in its own (the proof is located at the end of this section).

Theorem 5. *Let q be a prime power and $\mathbb{F}_q$ the corresponding finite field. Let F be a field such that $F/\mathbb{F}_q$ is a purely transcendental field extension. Let $n \in \mathbb{N}$ and let $N \in F^{n\times n}$ be a matrix. Then, the following statements are equivalent:*

- **A.1** $\det(N^h - I_n) \neq 0$ *for all* $h \in \mathbb{N} \setminus \{0\}$;
- **A.2** $\chi_N(t) \perp t^h - 1$ *for all* $h \in \mathbb{N} \setminus \{0\}$;
- **A.3** $\chi_N(t) \perp t^{q^i-1} - 1$ *for all* $i \in [1, n]$.

input : a natural $n > 1$, a prime p, and a matrix $M(X) \in \mathbb{K}^{n\times n}[X, X^{-1}]$, where $\mathbb{K} = \mathbb{Z}/p^k\mathbb{Z}$ for some $k > 0$
output : *true* iff the one-dimensional LCA having $M(X)$ as associated matrix is ergodic

if $\det(M(X) \mod p) \neq 0$ **then** // See Remark 4
  for $i \leftarrow 1$ *to* n **do** // Check Condition **A.3**
    if $\gcd(\chi_{M(X)}(t), t^{(p^k)^i - 1} - 1) \neq 1$ **then**
      return false
    end
  end
  return true
end
return false

Algorithm 1: Algorithm for deciding ergodicity for one-dimensional LCA over $\mathbb{K}^n$, with $\mathbb{K} = \mathbb{Z}/p^k\mathbb{Z}$.

We now exhibit the decision algorithm of ergodicity for one-dimensional LCA over $\mathbb{K}^n$ with $\mathbb{K} = \mathbb{Z}/p^k\mathbb{Z}$ for any prime p and any natural $k > 0$. As we will see, such an algorithm allows one to decide ergodicity also for one-dimensional LCA over $\mathbb{K}^n$ where $\mathbb{K} = \mathbb{Z}/m\mathbb{Z}$ for any natural $m > 1$.

The correctness of Algorithm 1 is ensured by the following

Theorem 6. *Algorithm 1 decides ergodicity for one-dimensional LCA over $\mathbb{K}^n$, where $\mathbb{K} = \mathbb{Z}/p^k\mathbb{Z}$ for any natural $n > 1$, any prime p, and any natural $k > 0$. In other words, the following decidable condition characterizes ergodicity for any LCA Δ: Δ is surjective and $\chi_{M(X)}(t) \perp t^{q^i - 1} - 1$ for all $i \in [1, n]$, where $q = p^k$ and $M(X)$ is the matrix associated with Δ.*

Proof. Let Δ any one-dimensional LCA over $\mathbb{K}^n$, where $\mathbb{K} = \mathbb{Z}/p^k\mathbb{Z}$ for some n, p, and k as in the statement. Let $M(X)$ be the matrix associated to Δ. By Theorem 2, Δ is ergodic iff Δ is surjective and, for all naturals $h > 0$, the 1-dimensional LCA $H^{(h)} = \Delta^h - I$ is surjective. Equivalently, by Remark 4, Δ is ergodic iff $\det(M(X) \mod p) \neq 0$ and, for all naturals $h > 0$, $\det((M(X)^h - I_n) \mod p) \neq 0$. The first requirement is clearly decidable. Since the second one is nothing but an instance of Condition **A.1** of Theorem 5, it is equivalent to Condition **A.3** of Theorem 5 itself and, hence, it is decidable. Algorithm 1 just consists of testing both the requirements to decide if Δ is ergodic. □

Theorem 6 leads to the following result.

Corollary 7. *Chaos, ergodicity, transitivity, and mixing are decidable properties for one-dimensional LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ for any natural $m > 1$ and any natural $n > 1$.*

Proof. By Theorem 1 it is enough to show that ergodicity is decidable. Consider a one-dimensional LCA Δ over $(\mathbb{Z}/m\mathbb{Z})^n$ for arbitrary naturals $m > 1$ and $n > 1$. By a generalisation of [6, Lemma 3.2] to $(\mathbb{Z}/m\mathbb{Z})^n$, if $m = p_1^{k_1} \dots p_l^{k_l}$ is the prime factor decomposition of m, then Δ is topologically conjugated to a product of one-dimensional LCAs, each of them having global rule Δ_i over $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^n$. Since topological transitivity is preserved under topological conjugacy and the product of CA is topological transitive iff each CA is, by Theorem 1 it follows that Δ is ergodic iff each one-dimensional LCA Δ_i over $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^n$ is ergodic. Algorithm 1 just allows one to establish whether each of such one-dimensional LCA is ergodic. Therefore, ergodicity is decidable. □

Remark 8. An incremental version of Algorithm 1 that is able to decide ergodicity for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ for any natural $m > 1$ and any natural $n > 1$ can be easily obtained by the proof of Corollary 7.

3.2. Proof of Theorem 5

The rest of the section is devoted to the proof of Theorem 5. We need the following two lemmata.

Lemma 9. *Let q, $\mathbb{F}_q$ and F be as in Theorem 5 and $n \in \mathbb{N}$. Let $f \in F[t]$ be a polynomial with $\deg f \leq n$. Assume that $f \perp t^{q^i-1}-1$ for all $i \in [1,n]$. Then, $f \perp t^h - 1$ for all integers $h > 0$.*

Proof. Let h be a positive integer. We must prove that $f \perp t^h - 1$. Indeed, assume the contrary. Then, the polynomials f and $t^h - 1$ have a non-constant common divisor $g \in F[t]$. Then, $g \mid f$ and $g \mid t^h - 1$. Thus, the roots of g are h-th roots of unity, and therefore are algebraic over the field $\mathbb{F}_q$. Hence, the coefficients of g are algebraic over the field $\mathbb{F}_q$ as well (since these coefficients are symmetric polynomials in these roots with integer coefficients). On the other hand, these coefficients belong to F. But $F/\mathbb{F}_q$ is a purely transcendental field extension. Thus, every element of F that is algebraic over $\mathbb{F}_q$ must belong to $\mathbb{F}_q$ [1]. Thus, the coefficients of g must belong to $\mathbb{F}_q$ (since they are elements of F that are algebraic over $\mathbb{F}_q$). In other words, $g \in \mathbb{F}_q[t]$.

Since this polynomial $g \in \mathbb{F}_q[t]$ is non-constant, it must have a monic irreducible divisor in $\mathbb{F}_q[t]$. In other words, there exists a monic irreducible $\pi \in \mathbb{F}_q[t]$ such that $\pi \mid g$. We have $\pi \mid g \mid f$, thus $\deg \pi \leq \deg f$. Let $j = \deg \pi$. Then, $j \geq 1$ (since π is irreducible) and

$$j = \deg \pi \leq \deg f \leq n.$$

Hence, $j \in [1,n]$. Thus, $f \perp t^{q^j-1}-1$ (since we assumed that $f \perp t^{q^i-1}-1$ for all $i \in [1,n]$). Hence, every common divisor of f and $t^{q^j-1}-1$ in $F[t]$ must be constant.

From $\pi \mid g \mid t^h - 1$, we conclude that $t^h \equiv 1 \mod \pi$ in $F[t]$. If we had $\pi \mid t$ in $F[t]$, then we would have $t \equiv 0 \mod \pi$ in $F[t]$, which would entail $t^h \equiv 0^h = 0 \mod \pi$ and thus $0 \equiv t^h \equiv 1 \mod \pi$, which would lead to $\pi \mid 1$, which would be absurd (since $\deg \pi = j \geq 1$). Thus, we cannot have $\pi \mid t$ in $F[t]$. Thus, we cannot have $\pi \mid t$ in $\mathbb{F}_q[t]$ either. Hence, $\pi \nmid t$ in $\mathbb{F}_q[t]$.

Claim 10. $\pi \mid t^{q^j-1} - 1$.

Proof. This is a well-known fact about irreducible polynomials in $\mathbb{F}_q[t]$ distinct from t, but for the sake of completeness let us give a proof. For each $u \in \mathbb{F}_q[t]$, we let $\overline{u}$ denote the projection of u onto $\mathbb{F}_q[t]/(\pi)$.

We have $\pi \nmid t$ in $\mathbb{F}_q[t]$. In other words, $\overline{t} \neq 0$ in $\mathbb{F}_q[t]/(\pi)$. As π is irreducible, $\mathbb{F}_q[t]/(\pi)$ is a finite field of size q^j with $\deg \pi = j$. As a consequence, its group of units is a finite group of size $q^j - 1$. Thus, Lagrange's theorem shows that $u^{q^j-1} = 1$ for every nonzero element $u \in \mathbb{F}_q[t]/(\pi)$. Applying this to $u = \overline{t}$, we conclude that $\overline{t}^{q^j-1} = 1$ (since the element $\overline{t}$ of $\mathbb{F}_q[t]/(\pi)$ is nonzero). Hence, $\overline{t^{q^j-1}} = \overline{t}^{q^j-1} = 1 = \overline{1}$, so that $t^{q^j-1} \equiv 1 \mod \pi$ in $\mathbb{F}_q[t]$. In other words, $\pi \mid t^{q^j-1} - 1$. □

Combining $\pi \mid g \mid f$ with $\pi \mid t^{q^j-1} - 1$, we conclude that π is a common divisor of f and $t^{q^j-1} - 1$ in $F[t]$. Hence, π is constant (since every common divisor of f and $t^{q^j-1} - 1$ in $F[t]$ must be constant). This contradicts the irreducibility of π. This contradiction shows that our assumption was false. Hence, Lemma 9 is proven. □

The following is a known result which will be useful for proving Theorem 5.

Lemma 11 ([22])**.** *Let $n \in \mathbb{N}$. Let K be any field. Let $N \in K^{n \times n}$ be a matrix. Let $f \in K[t]$ be any polynomial. Then, $\det(f(N)) \neq 0$ if and only if $\chi_N \perp f$.*

Proof of Theorem 5. Let h be a positive integer. Then, Lemma 11 (applied to $K = F$ and $f = t^h - 1$) shows that $\det\left(N^h - I_n\right) \neq 0$ if and only if $\chi_N \perp t^h - 1$. We thus have proven the equivalence

$$\left(\det\left(N^h - I_n\right) \neq 0\right) \iff \left(\chi_N \perp t^h - 1\right)$$

for each positive integer h. Hence, the statement **A.1** is equivalent to the statement **A.2**.

[1] Here we are using one of the basic properties of purely transcendental field extensions: If L/K is a purely transcendental field extension, then every element of L that is algebraic over K must belong to K. (Equivalently: If L/K is a purely transcendental field extension, then every element $x \in L \setminus K$ is transcendental over K.) This is proven in [3, § 7.1, Remark 10], for example.

On the other hand, $\chi_N \in F[t]$ is a polynomial with $\deg(\chi_N) = n$. Thus, Lemma 9 (applied to $f = \chi_N$) shows that if we have $\chi_N \perp t^{q^i-1}-1$ for all $i \in [1,n]$, then we have $\chi_N \perp t^h - 1$ for all positive integers h. In other words, the statement **A.3** implies the statement **A.2**. Conversely, the statement **A.2** implies the statement **A.3** (since each $q^i - 1$ with $i \in [1,n]$ is a positive integer). Combining these two sentences, we conclude that the statement **A.2** is equivalent to the statement **A.3**. Therefore, Theorem 5 is proven. □

Due to an interest in its own and a possible application to CA over a more general alphabet (as, for instance, an abelian group), we are going to extend Lemma 11 to arbitrary commutative rings and re-prove it in that generality. However, we first need to prove some additional lemmata.

Lemma 12. *Let $\mathbb{K}$ be any commutative ring. Let $f \in \mathbb{K}[t]$ be any polynomial. Let $\mathbb{L}$ be any commutative $\mathbb{K}$-algebra. Let u and v be two elements of $\mathbb{L}$. Then, $u - v \mid f(u) - f(v)$ in $\mathbb{L}$.*

Proof. This is well-known in the case when $\mathbb{K} = \mathbb{Z}$ and $\mathbb{L} = \mathbb{Z}$; but the same proof applies in the general case. Indeed, write the polynomial $f \in \mathbb{K}[t]$ in the form $f = \sum_{i=0}^{n} a_i t^i$ for some $n \in \mathbb{N}$ and some $a_0, a_1, \ldots, a_n \in \mathbb{K}$. Then, $f(u) = \sum_{i=0}^{n} a_i u^i$ and $f(v) = \sum_{i=0}^{n} a_i v^i$. Subtracting these two equalities from each other, we obtain

$$f(u) - f(v) = \sum_{i=1}^{n} a_i u^i - \sum_{i=1}^{n} a_i v^i = \sum_{i=1}^{n} a_i \underbrace{\left(u^i - v^i\right)}_{=(u-v)\sum_{k=0}^{i-1} u^k v^{i-1-k}}$$
$$= \sum_{i=1}^{n} a_i (u-v) \sum_{k=0}^{i-1} u^k v^{i-1-k} = (u-v) \sum_{i=1}^{n} a_i \sum_{k=0}^{i-1} u^k v^{i-1-k}.$$

The right hand side of this equality is clearly divisible by $u - v$. Thus, so is the left hand side. In other words, we have $u - v \mid f(u) - f(v)$ in $\mathbb{L}$. □

Note that commutativity of $\mathbb{L}$ is crucial in the proof of the previous lemma.

Lemma 13. *Let $n \in \mathbb{N}$. Let $\mathbb{L}$ be any commutative ring. Let $A \in \mathbb{L}^{n \times n}$ be any $n \times n$-matrix. Let $\lambda \in \mathbb{L}$. Then,*

$$\det(\lambda I_n + A) \equiv \det A \bmod \lambda\mathbb{L}.$$

Proof. This can be proven using the explicit formula for $\det(\lambda I_n + A)$ in terms of principal minors of A, or using the fact that the characteristic polynomial of A has constant term $(-1)^n \det A$. Here is another argument: For each $u \in \mathbb{L}$, we let $\overline{u}$ be the projection of u onto the quotient ring $\mathbb{L}/\lambda\mathbb{L}$; furthermore, for each matrix $B \in \mathbb{L}^{n \times n}$, we let $\overline{B} \in (\mathbb{L}/\lambda\mathbb{L})^{n \times n}$ be the result of projecting each entry of the matrix B onto the quotient ring $\mathbb{L}/\lambda\mathbb{L}$. Then, $\lambda \in \lambda\mathbb{L}$ and thus $\overline{\lambda} = 0$. Hence, $\overline{\lambda I_n + A} = \underbrace{\overline{\lambda I_n}}_{\substack{=0 \\ (\text{since } \overline{\lambda}=0)}} + \overline{A} = \overline{A}$. But the determinant of a matrix is a polynomial in the entries of the matrix, and thus is respected by the canonical projection $\mathbb{L} \to \mathbb{L}/\lambda\mathbb{L}$; hence,

$$\det\left(\overline{\lambda I_n + A}\right) = \overline{\det(\lambda I_n + A)} \qquad \text{and} \qquad \det\overline{A} = \overline{\det A}.$$

The left hand sides of these two equalities are equal (since $\overline{\lambda I_n + A} = \overline{A}$). Thus, the right hand sides are equal as well. In other words, $\overline{\det(\lambda I_n + A)} = \overline{\det A}$. In other words, $\det(\lambda I_n + A) \equiv \det A \bmod \lambda\mathbb{L}$. This proves Lemma 13. □

Lemma 14. *Let $n \in \mathbb{N}$. Let $\mathbb{K}$ be any commutative ring. Let $f \in \mathbb{K}[t]$ be any polynomial. Let $N \in \mathbb{K}^{n \times n}$ be any $n \times n$-matrix. Then, there exist two polynomials $a, b \in \mathbb{K}[t]$ such that*

$$\det(f(N)) = fa + \chi_N b \qquad \text{in } \mathbb{K}[t].$$

(Note that the left hand side of this equality is a constant polynomial, since $f(N) \in \mathbb{K}^{n \times n}$.)

Proof. Consider N as a matrix over the polynomial ring $\mathbb{K}[t]$ (via the standard embedding $\mathbb{K}^{n\times n} \to (\mathbb{K}[t])^{n\times n}$). The $\mathbb{K}$-subalgebra $(\mathbb{K}[t])[N]$ of $(\mathbb{K}[t])^{n\times n}$ is commutative (since it is generated by the single element N over the commutative ring $\mathbb{K}[t]$).

Hence, Lemma 12 (applied to $\mathbb{L} = (\mathbb{K}[t])[N]$ and $u = tI_n$ and $v = N$) shows that $tI_n - N \mid f(tI_n) - f(N)$ in $(\mathbb{K}[t])[N]$. In other words, there exists $U \in (\mathbb{K}[t])[N]$ such that

$$f(tI_n) - f(N) = (tI_n - N) \cdot U. \tag{1}$$

Consider this U. Taking determinants on both sides of the Equality (1), we find

$$\det(f(tI_n) - f(N)) = \det((tI_n - N) \cdot U) = \underbrace{\det(tI_n - N)}_{=\chi_N \text{ (by the definition of } \chi_N)} \cdot \det U$$
$$= \chi_N \cdot \det U.$$

In view of $f(tI_n) = f(t) \cdot I_n$, this rewrites as

$$\det(f(t) \cdot I_n - f(N)) = \chi_N \cdot \det U.$$

Hence,

$$\begin{aligned}
\chi_N \cdot \det U &= \det\underbrace{(f(t) \cdot I_n - f(N))}_{=f(t)\cdot I_n + (-f(N))} = \det(f(t) \cdot I_n + (-f(N))) \\
&\equiv \det(-f(N)) \qquad \text{(by Lemma 13, applied to } \mathbb{L} = \mathbb{K}[t],\ \lambda = f(t) \text{ and } A = -f(N)) \\
&= (-1)^n \det(f(N)) \bmod f(t)\,\mathbb{K}[t].
\end{aligned}$$

Multiplying this congruence by $(-1)^n$, we obtain

$$(-1)^n \chi_N \cdot \det U \equiv \underbrace{(-1)^n (-1)^n}_{=1} \det(f(N)) = \det(f(N)) \bmod f(t)\,\mathbb{K}[t].$$

In other words, $(-1)^n \chi_N \cdot \det U - \det(f(N)) \in f(t)\,\mathbb{K}[t]$. In other words, there exists a polynomial $c \in \mathbb{K}[t]$ such that

$$(-1)^n \chi_N \cdot \det U - \det(f(N)) = f(t)\,c. \tag{2}$$

Consider this c. Solving the Equality (2) for $\det(f(N))$, we find

$$\det(f(N)) = (-1)^n \chi_N \cdot \det U - \underbrace{f(t)}_{=f} c = (-1)^n \chi_N \cdot \det U - fc$$
$$= f \cdot (-c) + \chi_N \cdot (-1)^n \det U.$$

Hence, there exist two polynomials $a, b \in \mathbb{K}[t]$ such that $\det(f(N)) = fa + \chi_N b$ in $\mathbb{K}[t]$ (namely, $a = -c$ and $b = (-1)^n \det U$). This proves Lemma 14. □

We can now generalize Lemma 11 to arbitrary rings.

Lemma 15. *Let $n \in \mathbb{N}$. Let $\mathbb{K}$ be any commutative ring. Let $N \in \mathbb{K}^{n\times n}$ be a matrix. Let $f \in \mathbb{K}[t]$ be any polynomial. Then, $\det(f(N)) \in \mathbb{K}$ is invertible if and only if there exist polynomials $a, b \in \mathbb{K}[t]$ such that $fa + \chi_N b = 1$.*

Proof. $\Longrightarrow$: Assume that $\det(f(N)) \in \mathbb{K}$ is invertible. Thus, there exists $c \in \mathbb{K}$ such that $\det(f(N)) \cdot c = 1$. Lemma 14 ensures that there exist two polynomials $a, b \in \mathbb{K}[t]$ such that $\det(f(N)) = fa + \chi_N b$ in $\mathbb{K}[t]$. Consider these a and b, and denote them by a_0 and b_0. Thus, a_0 and b_0 are two polynomials in $\mathbb{K}[t]$ such that $\det(f(N)) = fa_0 + \chi_N b_0$. Now, comparing $\det(f(N)) \cdot c = 1$ with

$$\underbrace{\det(f(N))}_{=fa_0+\chi_N b_0} \cdot c = (fa_0 + \chi_N b_0) \cdot c = fa_0 c + \chi_N b_0 c,$$

we obtain $f\,a_0c + \chi_N\,b_0c = 1$. Thus, there exist polynomials $a, b \in \mathbb{K}[t]$ such that $f\,a + \chi_N\,b = 1$ (namely, $a = a_0c$ and $b = b_0c$). This proves the "$\Longrightarrow$" direction.

$\Longleftarrow$: Assume that there exist polynomials $a, b \in \mathbb{K}[t]$ such that $f\,a + \chi_N\,b = 1$. Consider these a and b. The Cayley–Hamilton theorem yields $\chi_N(N) = 0$. But evaluating both sides of the equality $f\,a + \chi_N\,b = 1$ at N, we obtain

$$f(N)\,a(N) + \chi_N(N)\,b(N) = I_n.$$

Hence,

$$I_n = f(N)\,a(N) + \underbrace{\chi_N(N)}_{=0}\,b(N) = f(N)\,a(N).$$

Taking determinants on both sides of this equality, we find

$$\det(I_n) = \det(f(N)\,a(N)) = \det(f(N)) \cdot \det(a(N)).$$

Thus,

$$\det(f(N)) \cdot \det(a(N)) = \det(I_n) = 1.$$

Hence, $\det(f(N)) \in \mathbb{K}$ is invertible (and its inverse is $\det(a(N))$). This proves the "$\Longleftarrow$" direction. □

4. Applications

In this section we illustrate how our results can improve applications. Considering the rapid growing of cryptographic techniques and the fact that LCA are often involved in designing these latter, we will deal with two representative applications in the domain of cryptosystems, namely, a secret sharing scheme and a data encryption method. Such applications are based on reversible (i.e., equivalently, injective) one-dimensional LCA over $\mathbb{K}^n$ with $\mathbb{K} = \mathbb{Z}/m\mathbb{Z}$ for some natural $m > 1$. Although reversibility is an essential requirement allowing the authorized parts to recover the cyphered/secreted data, it is largely not enough in order to ensure the security level expected in real scenarios. Indeed, it is well-known that good cryptosystems have to satisfy the so-called *confusion* and *diffusion* properties (along with some variants of them). Ergodicity and chaotic behavior are just the dynamical counterparts of the required cryptographic properties [2] and then they have to be exhibited by the dynamical system on which the cryptosystem is based. Actually, Corollary 7 and Algorithm 1 allow one to establish whether one-dimensional LCA exhibit such behaviors. Therefore, they are important tools to be used in the above mentioned applications for building one-dimensional LCA with the required properties and, then, for improving the existing methods which are based on such LCA.

In [9], authors propose a (n, l)-threshold secret sharing scheme involving l participants and based on linear higher-order CA of memory n over the alphabet $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$. Such automata are nothing but one-dimensional linear CA over $\mathbb{K}^n$ (with associated matrix presenting a specific structure, namely, a Frobenius normal form) and this makes it possible to analyse the scheme by exploiting the results concerning LCA.

As discussed at the beginning of this section, the one-dimensional LCA Δ on which the method is based has to be both ergodic and chaotic in order to ensure the cryptographic properties of confusion and diffusion. By Corollary 7 ergodicity and chaos are equivalent. Therefore, it is essential that Algorithm 1 deciding ergodicity is inserted in the scheme just before step 4. of the setup phase from [9] with the additional requirement that steps 1. to 3., which by using a pseudo-random number generator produce the LCA Δ, have to be repeated whenever they provide a non ergodic LCA.

As a specific application, let us consider the (3,4)-threshold scheme for texts of 64 bits proposed in [9]. The involved LCA Δ, which is one of the possible LCA provided by the method, has local rule with radius $r = 1$ and matrix $M(X)$ in Frobenius normal form and with characteristic polynomial

$$\chi_{M(X)}(t) = t^3 + (-X^{-1} - 1 - X)t^2 + (-X^{-1} - X)t - 1\ .$$

Clearly, it holds that $\det M(X) = 1$ and so, by [24, Proposition 3], it follows that Δ is reversible, that is, as already pointed out, a necessary but non sufficient requirement. Now, since $\chi_{M(X)}(t)$ is coprime with $t^{2^i-1} - 1$ for all $i \in [1, 3]$, Algorithm 1 outputs that Δ is ergodic.

Assume now that steps 1. to 3. generate a LCA Δ such that $\chi_{M(X)}(t) = t^3 - 1$ (this situation may actually happen). Then, Algorithm 1 outputs that Δ is not ergodic. By Theorem 1, the LCA is not even chaotic. Hence, the confusion and diffusion properties are not satisfied and the scheme turns out to be vulnerable. This situation can be avoided by adding Algorithm 1 at the end of step 3..

A block cypher scheme based on a linear higher-order CA of memory $n = 2$ over $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, i.e., a LCA $((\mathbb{K}^2)^{\mathbb{Z}}, \Delta)$, was proposed in [8]. The local rule of Δ has radius $r = 1$ and the matrix $M(X)$ associated with Δ has characteristic polynomial

$$\chi_{M(X)}(t) = t^2 + (-\alpha_{-1}^2 X^{-1} - \alpha_0^2 - \alpha_1^2 X)t - 1$$

where α_i^2s are coefficients to be suitably set up. According to the experimental observations by the authors, the following three choices $a_{-1}^2 = a_1^2 = 1$ and $a_0^2 = 0$, $a_0^2 = a_1^2 = 1$ and $a_{-1}^2 = 0$, and $a_{-1}^2 = a_0^2 = a_1^2 = 1$ allow good performances of the encryption scheme. Indeed, by running Algorithm 1 in these three situations, one finds that all the corresponding LCA are ergodic and chaotic. This is a formal explanation of such observations about the proposed encryption scheme. Therefore, also the cypher scheme can be equipped by Algorithm 1 to avoid bad choices and so in such a way that attacks are much harder.

5. Conclusions

We have proved that ergodicity, chaos, topological transitivity, and topological mixing, are decidable for one-dimensional LCA over $(\mathbb{Z}/m\mathbb{Z})^n$. Providing decision algorithms for other interesting dynamical properties such as equicontinuity, sensitivity to the initial conditions, expansivity, and strong transitivity for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ is the first step for further researches in this domain.

Another interesting research direction consists in extending the decidability results for all the above mentioned properties from one-dimensional LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ to the more general class of one-dimensional additive CA over any finite abelian group. This would allow to build more robust methods based on such CA in several applications.

[1] Luigi Acerbi, Alberto Dennunzio, and Enrico Formenti. Conservation of some dynamical properties for operations on cellular automata. *Theoretical Computer Science*, 410(38-40):3685–3693, 2009.

[2] Gonzalo Álvarez and Shujun Li. Some basic cryptographic requirements for chaos-based cryptosystems. *I. J. Bifurcation and Chaos*, 16(8):2129–2151, 2006.

[3] Siegfried Bosch. *Algebra*. Birkhäuser Advanced Texts Basler Lehrbücher. Birkhäuser Basel, 2018.

[4] Lieven Le Bruyn and Michel Van den Bergh. Algebraic properties of linear cellular automata. *Linear algebra and its applications*, 157:217–234, 1991.

[5] Gianpiero Cattaneo, Alberto Dennunzio, and Fabio Farina. A full cellular automaton to simulate predator-prey systems. In Samira El Yacoubi, Bastien Chopard, and Stefania Bandini, editors, *Cellular Automata, 7th International Conference on Cellular Automata, for Research and Industry, ACRI 2006, Perpignan, France, September 20-23, 2006, Proceedings*, volume 4173 of *Lecture Notes in Computer Science*, pages 446–451. Springer, 2006.

[6] Gianpiero Cattaneo, Alberto Dennunzio, and Luciano Margara. Solution of some conjectures about topological properties of linear cellular automata. *Theoretical Computer Science*, 325(2):249–271, 2004.

[7] Gianpiero Cattaneo, Enrico Formenti, Giovanni Manzini, and Luciano Margara. Ergodicity, transitivity, and regularity for linear cellular automata over $\mathbb{Z}_m$. *Theoretical Computer Science*, 233(1-2):147–164, 2000.

[8] Zhenchuan Chai, Zhenfu Cao, and Yuan Zhou. Encryption based on reversible second-order cellular automata. In Guihai Chen, Yi Pan, Minyi Guo, and Jian Lu, editors, *Parallel and Distributed Processing and Applications - ISPA 2005 Workshops*, pages 350–358, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[9] Angel Martín del Rey, Joaquim Pereira Mateus, and Gerardo Rodríguez Sánchez. A secret sharing scheme based on cellular automata. *Applied Mathematics and Computation*, 170(2):1356 – 1364, 2005.

[10] Alberto Dennunzio. From one-dimensional to two-dimensional cellular automata. *Fundamenta Informaticae*, 115(1):87–105, 2012.

[11] Alberto Dennunzio, Pietro di Lena, Enrico Formenti, and Luciano Margara. On the directional dynamics of additive cellular automata. *Theoretical Computer Science*, 410(47-49):4823–4833, 2009.

[12] Alberto Dennunzio, Pietro Di Lena, Enrico Formenti, and Luciano Margara. Periodic orbits and dynamical complexity in cellular automata. *Fundamenta Informaticae*, 126(2-3):183–199, 2013.

[13] Alberto Dennunzio, Enrico Formenti, Darij Grinberg, and Luciano Margara. Additive cellular automata over finite abelian groups: Topological and measure theoretic properties. In Peter Rossmanith, Pinar Heggernes, and Joost-Pieter Katoen, editors, *44th International Symposium on Mathematical Foundations of Computer Science, MFCS 2019, August 26-30, 2019, Aachen, Germany*, volume 138 of *LIPIcs*, pages 68:1–68:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[14] Alberto Dennunzio, Enrico Formenti, Darij Grinberg, and Luciano Margara. Dynamical behavior of additive cellular automata over finite abelian groups. *Theoretical Computer Science*, 2020.

[15] Alberto Dennunzio, Enrico Formenti, and Luca Manzoni. Computing issues of asynchronous CA. *Fundamenta Informaticae*, 120(2):165–180, 2012.

[16] Alberto Dennunzio, Enrico Formenti, and Julien Provillard. Non-uniform cellular automata: Classes, dynamics, and decidability. *Information and Computation*, 215:32 – 46, 2012.
[17] Alberto Dennunzio, Enrico Formenti, and Julien Provillard. Local rule distributions, language complexity and non-uniform cellular automata. *Theoretical Computer Science*, 504:38–51, 2013.
[18] Alberto Dennunzio, Enrico Formenti, and Julien Provillard. Three research directions in non-uniform cellular automata. *Theoretical Computer Science*, 559:73 – 90, 2014.
[19] Alberto Dennunzio, Enrico Formenti, and Michael Weiss. Multidimensional cellular automata: closing property, quasi-expansivity, and (un)decidability issues. *Theoretical Computer Science*, 516:40–59, 2014.
[20] Robert Luke Devaney. *An Introduction to Chaotic Dynamical Systems*. Addison-Wesley advanced book program. Addison-Wesley, 1989.
[21] Fabio Farina and Alberto Dennunzio. A predator-prey cellular automaton with parasitic interactions and environmental effects. *Fundamenta Informaticae*, 83(4):337–353, 2008.
[22] Paul A. Fuhrmann. *A Polynomial Approach to Linear Algebra*. Universitext. Springer, 2012. Second Edition.
[23] Masanobu Ito, Nobuyasu Osato, and Masakazu Nasu. Linear cellular automata over $\mathbb{Z}_m$. *Journal of Computer and Systems Sciences*, 27:125–140, 1983.
[24] Jarkko Kari. Linear cellular automata with multiple state variables. In Horst Reichel and Sophie Tison, editors, *STACS 2000*, volume 1770 of *LNCS*, pages 110–121. Springer-Verlag, 2000.
[25] 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.
[26] Mazi Shirvani and Thomas D. Rogers. Ergodic endomorphisms of compact abelian groups. *Communications in Mathematical Physics*, 118:401–410, 1988.
[27] Peter Walters. *An introduction to ergodic theory*, volume 79 of *Grauate text in mathematics*. Springer-Verlag, 1982.