Decidable Characterizations of Dynamical Properties for Additive Cellular Automata over a Finite Abelian Group with Applications to Data Encryption

Decidable Characterizations of Dynamical Properties for Additive Cellular Automata over a Finite Abelian Group with Applications to Data Encryption

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

Additive cellular automata over a finite abelian group are a wide class of cellular automata (CA) that are able to exhibit the complex behaviors of general CA and are often exploited for designing applications in different practical contexts. We provide decidable characterizations for Additive CA of the following important properties defining complex behaviors of complex systems: injectivity, surjectivity, equicontinuity, sensitivity to the initial conditions, topological transitivity, and ergodicity. Since such properties describe the main features required by real systems, the decision algorithms from our decidability results are then important tools for designing proper applications based on Additive CA. Indeed, we describe how our results can be exploited in some emblematic applications of cryptosystems, a paradigmatic and nowadays crucial applicative domain in which Additive CA are extensively used. We deal with methods for data encryption and, namely, we propose some strong modifications to the existing schemes in order to increase their security level and make attacks much harder.

Keywords: Cellular Automata, Additive Cellular Automata, Decidability, Complex Systems, Data Encryption

1. Introduction

Cellular automata (CA) are widely known formal models that find application in several disciplines and their different subdomains (for recent results and an up-to date bibliography on CA see for instance [20, 1, 16, 9, 10, 14], while for simulations

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

of complex systems by CA see for instance [26, 4, 25, 22, 21]). This is essentially due to three reasons: the huge variety of distinct CA dynamical behaviors; the emergence of complex behaviors from simple local interactions; the ease of their implementation (even at a hardware level).

In practical applications one needs to know if the CA used for modelling a certain system exhibits some specific property. However, this can be a severe issue. Indeed, Jarkko Kari proved a strong result stating (roughly speaking) that all non-trivial dynamical behaviors are undecidable [28]. From this seminal result, a long sequence followed.

Luckily, the undecidability issue can be tackled by imposing some constraints on the model. In the specific case of this paper, the alphabet and the global updating map are constrained to be a finite abelian group and an additive function, respectively, giving rise to *Additive CA over a finite abelian group* (or, briefly, *Additive CA*). We stress that such requirements do not prevent Additive CA at all from being successfully used for practical purposes. On the contrary, since Additive CA are able to exhibit the complex behaviors of general CA, they are often exploited for designing many applications.

Decidable characterizations of the dynamical properties for Additive CA essentially exist only for the subclass of linear CA (LCA) over $(\mathbb{Z}/m\mathbb{Z})^n$, i.e., those with linear local rule defined by $n \times n$ matrices over $(\mathbb{Z}/m\mathbb{Z})$ (see [29, 3, 11] for results involving any $n \geq 1$, while see [33, 6, 23] for $n = 1$). The present paper provides decidable characterizations of injectivity, surjectivity, equicontinuity, sensitivity to the initial conditions, topological transitivity, and ergodicity for Additive CA over a finite abelian group. By means of an embedding of an Additive CA over a finite abelian group into a linear CA over a bigger alphabet (which is a commutative ring), the proof technique essentially consists in lifting each of the above mentioned properties from the linear CA to the additive one.

Let us emphasize the significance of our results in real-world scenarios. Since the properties under consideration often describe the main features required by real systems to ensure a good functioning for themselves, the decision algorithms derived from Theorems 18, 23, 24, 25, and Corollary 26 are then important tools for designing proper applications based on Additive CA. Indeed, applications involves systems that necessarily must exhibit one or more among the following features of complex systems: reversibility, reachability, stability, instability, stronger form of instability, ergodicity, *etc.*. The formal properties investigated in this paper just describe these features. Namely, injectivity and surjectivity make reference to reversibility, surjectivity alone is necessary to ensure any form of reachability, equicontinuity is just stability, sensitivity to the initial condition is the most recognized form of instability, topological chaos is a stronger form of instability defined by topological transitivity, denseness of periodic points, and sensitivity (see [24, 5]), while transitivity alone is a form of reachability, and the formal property of ergodicity just describes the ergodicity feature itself.

A paradigmatic and nowadays crucial applicative domain in which CA are extensively used is that of cryptosystems. We then illustrate how our decidability results can be exploited in some emblematic cryptographic applications such as block encryption and secret sharing schemes. In particular, since the choice of the local

rule plays an important role to get a method of high quality in several respects, the class of Additive CA is richer than LCA, injectivity and reversibility are equivalent for general CA, and, furthermore, chaos, topological transitivity and ergodicity coincide for Additive CA over a finite abelian group [12], we propose some strong modifications to the existing methods based on CA, namely, the use of Additive CA instead of the simpler LCA and the addition of the decision algorithms from Theorems 24 and 25 whenever reversibility and a transitivity/chaotic/ergodicity feature, respectively, is required by the system. Actually, cryptosystems always have to exhibit such features. Indeed, as to encryption systems, reversibility allows recovering the original data from the encrypted ones, while for general cryptosystems ergodicity and chaos ensure the confusion and diffusion conditions which in turn ensure an appropriate degree of security [2, 39].

Obviously, our results can be also exploited in all the scientific fields and all the applications where Additive CA are used.

The paper is structured as follows. Next section introduces all the necessary background and formal definitions. Section 3 recalls the known results about linear CA over $(\mathbb{Z}/m\mathbb{Z})^n$. Section 4 contains the new results, while Section 5 illustrates their impact in cryptographic applications. In the last section we draw our conclusions and provide some perspectives.

Acknowledgements

DG thanks the Mathematisches Forschungsinstitut Oberwolfach for its hospitality.

2. Background

Let S be a finite set. A configuration over S is a map from $\mathbb{Z}$ to S. We consider the following *space of configurations* $S^{\mathbb{Z}} = \{\boldsymbol{c} |\ \boldsymbol{c} : \mathbb{Z} \to S\}$. Each element $\boldsymbol{c} \in S^{\mathbb{Z}}$ can be visualized as an infinite one-dimensional cell lattice in which each cell $i \in \mathbb{Z}$ contains the element $\boldsymbol{c}_i \in S$. The space $S^{\mathbb{Z}}$ is endowed with the standard Tychonoff metric d.

Let $r \in \mathbb{N}$ and $\delta : S^{2r+1} \to S$ be any map. We say that δ is a *local rule* of *radius* r.

Definition 1 (Cellular Automaton). A *one-dimensional CA based on a radius r local rule δ* is a pair $(S^{\mathbb{Z}}, F)$, where $F : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ is the *global transition rule* defined as follows:

$$\forall \boldsymbol{c} \in S^{\mathbb{Z}},\ \forall i \in \mathbb{Z}, \quad F(\boldsymbol{c})_i = \delta\left(\boldsymbol{c}_{i-r}, \ldots, \boldsymbol{c}_{i+r}\right). \tag{1}$$

We stress that the local rule δ completely determines the global rule F of a CA. We also recall that any map $F : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ is the global transition rule of a CA if and only if F is (uniformly) continuous and $F \circ \sigma = \sigma \circ F$, where $\sigma : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ is the *shift map* defined as $\forall \boldsymbol{c} \in S^{\mathbb{Z}},\ \forall i \in \mathbb{Z},\ \sigma(\boldsymbol{c})_i = \boldsymbol{c}_{i+1}$. From now on, when no misunderstanding is possible, we identify a CA with its global rule. Moreover, whenever an ergodic property is considered for CA, μ is the well-known Haar measure over the collection $\mathcal{M}$ of measurable subsets of $S^{\mathbb{Z}}$, i.e., the one defined as the product measure induced by the uniform probability distribution over S.

For the definitions of the standard dynamical properties under consideration as *equicontinuity, sensitivity to the initial conditions, topological transitivity, ergodicity*, and all the other topological mixing and ergodic conditions, we address the reader for instance to [31, 11].

2.1. Additive and Linear Cellular Automata

Let us introduce the background of Additive CA. The alphabet S will be a finite abelian group G, with group operation $+$, neutral element 0, and inverse operation $-$. In this way, the configuration space $G^{\mathbb{Z}}$ turns out to be a finite abelian group, too, where the group operation of $G^{\mathbb{Z}}$ is the componentwise extension of $+$ to $G^{\mathbb{Z}}$. With an abuse of notation, we denote by the same symbols $+$, 0, and $-$ the group operation, the neutral element, and the inverse operation, respectively, both of G and $G^{\mathbb{Z}}$. Observe that $+$ and $-$ are continuous functions in the topology induced by the metric d. A configuration $\boldsymbol{c} \in G^{\mathbb{Z}}$ is said to be *finite* if the number of positions $i \in \mathbb{Z}$ with $\boldsymbol{c}_i \neq 0$ is finite.

Definition 2 (Additive Cellular Automata). An *Additive CA* over a abelian finite group G is a CA $(G^{\mathbb{Z}}, F)$ where the global transition map $F : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$ is an endomorphism of $G^{\mathbb{Z}}$.

The *sum of two Additive CA* F_1 and F_2 over G is naturally defined as the map on $G^{\mathbb{Z}}$ denoted by $F_1 + F_2$ and such that

$$\forall \boldsymbol{c} \in G^{\mathbb{Z}}, \quad (F_1 + F_2)(\boldsymbol{c}) = F_1(\boldsymbol{c}) + F_2(\boldsymbol{c})$$

Clearly, $F_1 + F_2$ is an Additive CA over G.

We now recall the notion of linear CA, an important subclass of Additive CA. We stress that, whenever the term *linear* is involved, the alphabet S is $\mathbb{K}^n$, where $\mathbb{K} = \mathbb{Z}/m\mathbb{Z}$ for some positive integer m. Both $\mathbb{K}^n$ and $(\mathbb{K}^n)^{\mathbb{Z}}$ become $\mathbb{K}$-modules in the obvious (i.e., entrywise) way.

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 $A_{-r}, \ldots, A_0, \ldots, A_r \in \mathbb{K}^{n \times n}$ as follows:

$$\forall (x_{-r}, \ldots, x_0, \ldots, x_r) \in (\mathbb{K}^n)^{2r+1}, \quad \delta(x_{-r}, \ldots, x_0, \ldots, x_r) = \sum_{i=-r}^{r} A_i \cdot x_i \ .$$

Definition 3 (Linear Cellular Automata (LCA)). A *linear CA (LCA)* over $\mathbb{K}^n$ is a CA based on a linear local rule.

Let $\mathbb{K}^n[X, X^{-1}]$ and $\mathbb{K}^n[[X, X^{-1}]]$ denote the set of *Laurent polynomials* and the set of *Laurent series*, respectively, with coefficients in $\mathbb{K}^n$. A configuration $\boldsymbol{c} \in (\mathbb{K}^n)^{\mathbb{Z}}$ can be associated with the Laurent series

$$\boldsymbol{P}_{\boldsymbol{c}}(X) = \sum_{i \in \mathbb{Z}} \boldsymbol{c}_i X^i = \begin{bmatrix} c^1(X) \\ \vdots \\ c^n(X) \end{bmatrix} = \begin{bmatrix} \sum_{i \in \mathbb{Z}} c_i^1 X^i \\ \vdots \\ \sum_{i \in \mathbb{Z}} c_i^n X^i \end{bmatrix} \in \left(\mathbb{K}[[X, X^{-1}]]\right)^n \cong \mathbb{K}^n[[X, X^{-1}]] \ .$$

Then, if F is the global rule of a LCA defined by $A_{-r},\ldots,A_0,\ldots,A_r$, one finds

$$\boldsymbol{P}_{F(\boldsymbol{c})}(X) = A \cdot \boldsymbol{P}_{\boldsymbol{c}}(X)$$

where

$$A = \sum_{i=-r}^{r} A_i X^{-i} \in \mathbb{K}[X, X^{-1}]^{n\times n}$$

is the *the matrix associated with the LCA* F. In this way, for any integer $t > 0$ the matrix associated with F^t is A^t, and then $\boldsymbol{P}_{F^t(\boldsymbol{c})}(X) = A^t \cdot \boldsymbol{P}_{\boldsymbol{c}}(X)$.

3. Known Results about Additive and Linear CA

Let us start with with sensitivity and equicontinuity for LCA over $\mathbb{K}^n$. First of all, we remind that a dichotomy between sensitivity and equicontinuity holds for LCA. Moreover, these properties are characterized by the behavior of the powers of the matrix associated with a LCA.

Proposition 4 ([15]). *Let $\left((\mathbb{K}^n)^{\mathbb{Z}}, F\right)$ be a LCA over $\mathbb{K}^n$ and let A be the matrix associated with F. The following statements are equivalent:*

1. *F is sensitive to the initial conditions;*
2. *F is not equicontinuous;*
3. $\left|\{A^1, A^2, A^3, \ldots\}\right| = \infty$.

The decidability result concerning sensitivity and equicontinuity has been recently reached in [13] by means of a deep algebra result and the decidability of sensitivity and equicontinuity for the subclass of LCA over $\mathbb{K}^n$ with associated matrix in Frobenius normal form [15].

Theorem 5 ([13]). *Sensitivity and equicontinuity are decidable for LCA over $\mathbb{K}^n$.*

It is well-known that injectivity and surjectivity are decidable for general CA. As to LCA over $\mathbb{K}^n$, there was also provided a characterization of these properties in terms of the determinant of the matrix associated with a LCA (the decidability of such characterization follows from the fact that injectivity and surjectivity are decidable for LCA over $\mathbb{K}$, see [27]).

Theorem 6 ([3, 29]). *Injectivity and surjectivity are decidable for LCA over $\mathbb{K}^n$. In particular, a LCA F over $\mathbb{K}^n$ is injective (resp., surjective) if and only if the determinant of the matrix associated with F is the Laurent polynomial associated with an injective (resp., surjective) LCA over $\mathbb{K}$.*

The decidability of chaos, ergodicity, topologically transitivity, and other ergodic and mixing properties for LCA over $\mathbb{K}^n$ has been recently proved in [11]. Furthermore in [12], we showed the equivalence of all the mixing and ergodic properties for Additive CA over a finite abelian group. Summarizing, the following holds.

Theorem 7 ([11, 12]). *Let F be any Additive CA over a finite abelian group. The following statements are equivalent: (1) F is chaotic; (2) F is ergodic; (3) F is topologically transitive; (4) F is surjective and for every integer $t > 0$ it holds that $F^t - I$ is surjective (I is the identity map); (5) F is topologically mixing; (6) F is weak topologically transitive; (7) F is totally transitive; (8) F is weakly ergodic mixing; (9) F is ergodic mixing.*
Moreover, all the previously mentioned properties are decidable for LCA over $\mathbb{K}^n$. In particular, when $\mathbb{K} = \mathbb{Z}/p^k\mathbb{Z}$, given any LCA F over $\mathbb{K}^n$, all the previous statements are equivalent to the following condition:

$$\det(A \mod p) \neq 0 \quad \textit{and} \quad \det((A^{p^{kt}-1} - I_n) \mod p) \neq 0 \ \textit{for all for all } t \in \{1, \ldots, n\},$$

where A is the matrix associated with F, I_n is the $n \times n$ identity matrix, and the operator mod p *over a matrix means that all coefficients appearing inside that matrix are taken modulo p.*

4. From Linear to Additive CA

In this section we are going to prove that sensitivity, equicontinuity, topological transitivity, and all the properties equivalent to the latter are decidable also for Additive CA. For each of them we will reach the decidability result by extending the analogous one obtained for LCA to the wide class of Additive CA. In a similar way, we provide a decidable characterization of injectivity and surjectivity for Additive CA.

We recall that the local rule $\delta : G^{2r+1} \to G$ of an Additive CA of radius r over a finite abelian group G can be written as

$$\forall (x_{-r}, \ldots, x_r) \in G^{2r+1}, \qquad \delta(x_{-r}, \ldots, x_r) = \sum_{i=-r}^{r} \delta_i(x_i) \tag{2}$$

where the functions δ_i are endomorphisms of G.

The fundamental theorem of finite abelian groups states that every finite abelian group G is isomorphic to $\bigoplus_{i=1}^{h} \mathbb{Z}/k_i\mathbb{Z}$ where the numbers $k_1, \ldots, k_h$ are powers of (not necessarily distinct) primes and $\oplus$ is the direct sum operation. Hence, the global rule F of an Additive CA over G splits into the direct sum of a suitable number h' of Additive CA over subgroups $G_1, \ldots, G_{h'}$ with $h' \leq h$ and such that $\gcd(|G_i|, |G_j|) = 1$ for each pair of distinct $i, j \in \{1, \ldots, h'\}$. Each of them can be studied separately and then the investigation of the dynamical behavior of F can be carried out by combining together the results obtained for each component.

Let us illustrate the application of the fundamental theorem of finite abelian group to Additive CA by means of the following.

Example 8. Let F be an Additive CA over $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/49\mathbb{Z}$. Then, F splits into the direct sum of 3 Additive CA F_1, F_2, and F_3

over $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, and $\mathbb{Z}/49\mathbb{Z}$, respectively. Hence, F is topological transitive iff both F_1, F_2, and F_3 are topological transitive, while F is sensitive to initial conditions iff at least one Additive CA among F_1, F_2, and F_3 is sensitive to the initial conditions.

Three different situations can occur.

(S1) $G \cong \mathbb{Z}/p^k\mathbb{Z}$**.** The alphabet G turns out to be a cyclic group and Additive CA over $\mathbb{Z}/p^k\mathbb{Z}$ are just LCA over $\mathbb{Z}/p^k\mathbb{Z}$. Decidable characterizations of all the dynamical properties under consideration have been provided a few decades ago [33].

(S2) $G \cong (\mathbb{Z}/p^k\mathbb{Z})^n$ with $n > 1$**.** Again, Additive CA over G coincide with LCA over G, but $G = (\mathbb{Z}/p^k\mathbb{Z})^n$ is not a cyclic group and this makes the investigation of the dynamical properties much more difficult than the case $n = 1$. However, as recalled in Section 3, we recently succeeded in showing decidable characterizations of sensitivity, equicontinuity, transitivity, and ergodicity, while a characterization of injectivity and surjectivity had been already exhibited.

(S3) $G \cong \bigoplus_{i=1}^{n} \mathbb{Z}/p^{k_i}\mathbb{Z}$**.** In this situation ($\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}\times\mathbb{Z}/32\mathbb{Z}$ of Example 8), the group G is once more not cyclic and F turns out to be a subsystem of a suitable LCA. Therefore, the study of the dynamical behavior of F is even harder than in situation **(S2)**. We do not even know easy checkable characterizations of basic properties like surjectivity or injectivity so far. We will provide them in the sequel as we stated at the beginning of this section.

Assumption. Hence, without loss of generality, in the sequel we can assume that

$$G = \mathbb{Z}/p^{k_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{k_n}\mathbb{Z}$$

with $k_1 \geq k_2 \geq \ldots \geq k_n$ in order to reach our goal.

For any $i \in \{1, \ldots, n\}$ let us denote by $\boldsymbol{e}^{(i)} \in G^{\mathbb{Z}}$ the bi-infinite configuration such that $\boldsymbol{e}^{(i)}_0 = e_i$ and $\boldsymbol{e}^{(i)}_j = 0$ for every integer $j \neq 0$.

Definition 9. Let $(G^{\mathbb{Z}}, F)$ be an Additive CA over G. We say that $\boldsymbol{e}^{(i)} \in G^{\mathbb{Z}}$ *spreads under* F if for every $\ell \in \mathbb{N}$ there exists $k \in \mathbb{N}$ such that $F^k(\boldsymbol{e}^{(i)})_j \neq 0$ for some integer j with $|j| > \ell$.

Remark 10. Whenever we consider $\boldsymbol{P}_{\boldsymbol{e}^{(i)}}(X) \in G[[X, X^{-1}]]$, we will say that $\boldsymbol{P}_{\boldsymbol{e}^{(i)}}(X)$ spreads under F if for every $\ell \in \mathbb{N}$ there exists $k \in \mathbb{N}$ such that $\boldsymbol{P}_{F^k(\boldsymbol{e}^{(i)})}(X)$ has at least one component with a non null monomial of degree which is greater than ℓ in absolute value. Clearly, $\boldsymbol{P}_{\boldsymbol{e}^{(i)}}(X)$ spreads under F if and only if $\boldsymbol{e}^{(i)}$ spreads under F.

Let $\hat{G} = (\mathbb{Z}/p^{k_1}\mathbb{Z})^n$. Define the map $\psi : G \to \hat{G}$ as follows

$$\forall h \in G, \quad \forall i = 1, \ldots, n, \quad \psi(h)^i = h^i \, p^{k_1 - k_i} \ ,$$

where, for a sake of clarity, we stress that h^i denotes the i-th component of h, while $p^{k_1-k_i}$ is just the $(k_1 - k_i)$-th power of p.

Definition 11. We define the function $\Psi : G^{\mathbb{Z}} \to \hat{G}^{\mathbb{Z}}$ as the componentwise extension of ψ, i.e.,

$$\forall \boldsymbol{c} \in G^{\mathbb{Z}}, \quad \forall j \in \mathbb{Z}, \quad \Psi(\boldsymbol{c})_j = \psi(\boldsymbol{c}_j) \ .$$

It is easy to check that Ψ is continuous and injective. Since every configuration $\boldsymbol{c} \in G^{\mathbb{Z}}$ (or $\hat{G}^{\mathbb{Z}}$) is associated with the Laurent series $\boldsymbol{P}_{\boldsymbol{c}}(X) \in G[[X, X^{-1}]]$ (or $\hat{G}[[X, X^{-1}]]$), with an abuse of notation we will sometimes consider Ψ as map from $G[[X, X^{-1}]]$ to $\hat{G}[[X, X^{-1}]]$ with the obvious meaning.

For any Additive CA over G, we are now going to define a LCA over $(\mathbb{Z}/p^{k_1}\mathbb{Z})^n$ associated with it. With a further abuse of notation, in the sequel we will write p^{-m} with $m \in \mathbb{N}$ even if this quantity might not exist in $\mathbb{Z}/p^k\mathbb{Z}$. However, we will use it only when it multiplies $p^{m'}$ for some integer $m' > m$. In such a way $p^{m'-m}$ is well-defined in $\mathbb{Z}/p^k\mathbb{Z}$ and we will note it as product $p^{-m} \cdot p^{m'}$.

Definition 12. Let $(G^{\mathbb{Z}}, F)$ be any Additive CA and let $\delta : G^{2r+1} \to G$ be its local rule defined, according to (2), by $2r+1$ endomorphisms $\delta_{-r}, \ldots, \delta_r$ of G . For each $z \in \{-r, \ldots, r\}$, we define the matrix $A_z = (a_{i,j}^{(z)})_{1 \le i \le n,\, 1 \le j \le n} \in (\mathbb{Z}/p^{k_1}\mathbb{Z})^{n \times n}$ as

$$\forall i, j \in \{1, \ldots, n\}, \qquad a_{i,j}^{(z)} = p^{k_j - k_i} \cdot \delta_z(e_j)^i$$

The *LCA associated with the Additive CA* $(G^{\mathbb{Z}}, F)$ is $(\hat{G}^{\mathbb{Z}}, L)$, where L is defined by $A_{-r}, \ldots, A_r$ or, equivalently, by $A = \sum_{z=-r}^{r} A_z X^{-z} \in \mathbb{Z}/p^{k_1}\mathbb{Z}\left[X, X^{-1}\right]^{n \times n}$.

Remark 13. Since every δ_z is an endomorphism of G, by construction A turns out to be well-defined.

Remark 14. The following diagram commutes

$$\begin{array}{ccc} G^{\mathbb{Z}} & \xrightarrow{F} & G^{\mathbb{Z}} \\ {\scriptstyle\Psi}\downarrow & & \downarrow{\scriptstyle\Psi} \\ \hat{G}^{\mathbb{Z}} & \xrightarrow[L]{} & \hat{G}^{\mathbb{Z}} \end{array},$$

i.e., $L \circ \Psi = \Psi \circ F$. Therefore we say that $(\hat{G}^{\mathbb{Z}}, L)$ is the LCA associated with $(G^{\mathbb{Z}}, F)$ *via the embedding* Ψ. Let us stress that we can not state that $(G^{\mathbb{Z}}, F)$ is topologically conjugated (i.e., homeomorphic) to $(\hat{G}^{\mathbb{Z}}, L)$. Indeed, $(G^{\mathbb{Z}}, F)$ is a subsystem of $(\hat{G}^{\mathbb{Z}}, L)$ and the subsystem condition alone is not enough in general to lift dynamical properties from a one system to the other one. Despite this obstacle, in the sequel we will succeed in doing such a lifting.

4.1. Sensitivity and Equicontinuity for Additive Cellular Automata

Let us start with the decidability of sensitivity and equicontinuity.

Lemma 15. *Let $(G^{\mathbb{Z}}, F)$ be any Additive CA. If for some $i \in \{1, \ldots, n\}$ the configuration $\boldsymbol{e}^{(i)} \in G^{\mathbb{Z}}$ spreads under F then $(G^{\mathbb{Z}}, F)$ is sensitive to the initial conditions.*

Proof. We prove that F is sensitive with constant $\varepsilon = 1$. Let $\boldsymbol{e}^{(i)} \in G^{\mathbb{Z}}$ be the configuration spreading under F. Choose arbitrarily an integer $\ell \in \mathbb{N}$ and a configuration $\boldsymbol{c} \in G^{\mathbb{Z}}$. Let $t \in \mathbb{N}$ and $j \notin \{-\ell, \dots, \ell\}$ be the integers such that $F^t(\boldsymbol{e}^{(i)})_j \neq 0$. Consider the configuration $\boldsymbol{c}' = \boldsymbol{c} + \sigma^j(\boldsymbol{e}^{(i)})$. Clearly, it holds that $d(\boldsymbol{c}, \boldsymbol{c}') < 2^{-\ell}$ and $F^t(\boldsymbol{c}') = F^t(\boldsymbol{c}) + F^t(\sigma^j(\boldsymbol{e}^{(i)})) = F^t(\boldsymbol{c}) + \sigma^j(F^t(\boldsymbol{e}^{(i)}))$. So, we get $d(F^t(\boldsymbol{c}'), F^t(\boldsymbol{c})) = 1$ and this concludes the proof. □

In order to prove the decidability of sensitivity, we need to deal with the following notions about Laurent polynomials.

Definition 16. Given any polynomial $\mathbb{p}(X) \in \mathbb{Z}/p^{k_1}\mathbb{Z}\left[X, X^{-1}\right]$, the *positive* (resp., *negative*) *degree of* $\mathbb{p}(X)$, denoted by $deg^+[\mathbb{p}(X)]$ (resp., $deg^-[\mathbb{p}(X)]$) is the maximum (resp., minimum) degree among those of the monomials having both positive (resp., negative) degree and coefficient which is not multiple of p. If there is no monomial satisfying both the required conditions, then $deg^+[\mathbb{p}(X)] = 0$ (resp., $deg^-[\mathbb{p}(X)]$=0).

Lemma 17. *Let $(\hat{G}^{\mathbb{Z}}, L)$ be a LCA and let $A \in \mathbb{Z}/p^{k_1}\mathbb{Z}\left[X, X^{-1}\right]^{n\times n}$ be the matrix associated with L. If $(\hat{G}^{\mathbb{Z}}, L)$ is sensitive then for every integer $m \geq 1$ there exists an integer $k \geq 1$ such that at least one entry of A^k has either positive or negative degree with absolute value which is greater than m.*

Proof. We can write $A = B + p \cdot C$ for some $B, C \in \mathbb{Z}/p^{k_1}\mathbb{Z}\left[X, X^{-1}\right]^{n\times n}$, where the monomials of all entries of B have coefficient which is not multiple of p. Assume that there exists a bound $b \geq 1$ such that for every $k \geq 1$ all entries of A^k have degree less than b in absolute value. Therefore, it holds that $\left|\{A^k, k \geq 1\}\right| < \infty$ and so, by Proposition 4, $(\hat{G}^{\mathbb{Z}}, L)$ is not sensitive. □

We are now able to prove the following important result.

Theorem 18. *Let $(G^{\mathbb{Z}}, F)$ be any Additive CA over G and let $(\hat{G}^{\mathbb{Z}}, L)$ be the LCA associated with F via the embedding Ψ. Then, the CA $(G^{\mathbb{Z}}, F)$ is sensitive to the initial conditions if and only if $(\hat{G}^{\mathbb{Z}}, L)$ is. Moreover, the CA $(G^{\mathbb{Z}}, F)$ is equicontinuous if and only if $(\hat{G}^{\mathbb{Z}}, L)$ is.*

Proof. Let us start with the equivalence between sensitivity of $(G^{\mathbb{Z}}, F)$ and sensitivity of $(\hat{G}^{\mathbb{Z}}, L)$.
$\Longrightarrow$: Assume that $(\hat{G}^{\mathbb{Z}}, L)$ is not sensitive. Then, by Proposition 4, there exist two integers $k \in \mathbb{N}$ and $m > 0$ such that $L^{k+m} = L^k$. Therefore, we get $\Psi \circ F^{k+m} = L^{k+m} \circ \Psi = L^k \circ \Psi = \Psi \circ F^k$. Since Ψ is injective, it holds that $F^{k+m} = F^k$ and so $(G^{\mathbb{Z}}, F)$ is not sensitive.
$\Longleftarrow$: Assume that $(\hat{G}^{\mathbb{Z}}, L)$ is sensitive and for any natural k let $A^k = (a^{(k)}_{i,j})_{1\leq i\leq n, 1\leq j\leq n}$ be the k-th power of $A \in \mathbb{Z}/p^{k_1}\mathbb{Z}\left[X, X^{-1}\right]^{n\times n}$, where A is the matrix associated with $(\hat{G}^{\mathbb{Z}}, L)$. We are going to show that at least one configuration among $\boldsymbol{e}^{(1)}, \dots, \boldsymbol{e}^{(n)}$ spreads under F. Choose arbitrarily $\ell \in \mathbb{N}$. By Lemma 17, there exist an integer $m \geq 1$ and one entry (i, j) such that either $deg^-[a^{(m)}_{i,j}] < -\ell$ or $deg^+[a^{(m)}_{i,j}] > \ell$. Without loss of generality suppose that $deg^+[a^{(m)}_{i,j}] > \ell$. The i–th component of

$\boldsymbol{P}_{F^m(\boldsymbol{e}^{(j)})}(X)$ is the well defined polynomial $p^{k_i-k_1}\cdot p^{k_1-k_j}\cdot a_{i,j}^{(m)}$. Since $deg^+[a_{i,j}^{(m)}]>\ell$, we can state that $\boldsymbol{e}^{(j)}$ spreads under F. By Lemma 15, it follows that $(G^{\mathbb{Z}},F)$ is sensitive.

As to the equicontinuity equivalence, the above first implication also proves that if $(\hat{G}^{\mathbb{Z}},L)$ is equicontinuous (i.e., by Proposition 4, it is not sensitive) then $F^{k+m}=F^k$, i.e., by [30], $(G^{\mathbb{Z}},F)$ is equicontinuous. Conversely, if $(G^{\mathbb{Z}},F)$ is equicontinuous then it trivially follows that it is not sensitive, i.e., by the above second implication, $(\hat{G}^{\mathbb{Z}},L)$ is not sensitive, i.e., by Proposition 4, $(\hat{G}^{\mathbb{Z}},L)$ is equicontinuous. □

As immediate consequence of Theorem 18 we can state that the dichotomy between sensitivity and equicontinuity also holds for Additive CA.

Corollary 19. *Any Additive CA over a finite abelian group is sensitive to the initial conditions if and only if it is not equicontinuous.*

The following decidability result follows from Theorem 18 and the decidability of sensitivity for LCA.

Corollary 20. *Equicontinuity and sensitivity to the initial conditions are decidable for Additive CA over a finite abelian group.*

Proof. Use Theorem 5 and 18. □

4.2. Surjectivity and Injectivity for Additive Cellular Automata

We now study injectivity and surjectivity for Additive CA.

Lemma 21. *Let $(\hat{G}^{\mathbb{Z}},L)$ be any LCA over $\hat{G}$. If there exists a configuration $\boldsymbol{b}\in\hat{G}^{\mathbb{Z}}$ with $\boldsymbol{b}\neq 0$ and $L(\boldsymbol{b})=0$, then there exists a configuration $\boldsymbol{b}'\in\Psi(G^{\mathbb{Z}})$ such that $\boldsymbol{b}'\neq 0$ and $L(\boldsymbol{b}')=0$. In particular, if $\boldsymbol{b}$ is finite then $\boldsymbol{b}'$ is finite too.*

Proof. Let $\boldsymbol{b}\in\hat{G}^{\mathbb{Z}}$ any configuration with $\boldsymbol{b}\neq 0$ and $L(\boldsymbol{b})=0$. Set $\boldsymbol{b}^{(1)}=p\cdot\boldsymbol{b}$. If $\boldsymbol{b}^{(1)}=0$ then for every $i\in\mathbb{Z}$ each component of $\boldsymbol{b}_i$ has p^{k_1-1} as factor. So, $\boldsymbol{b}\in\Psi(G^{\mathbb{Z}})$ and $\boldsymbol{b}'=\boldsymbol{b}$ is just one possible configuration the thesis requires to exhibit. Otherwise, by repeating the same argument, set $\boldsymbol{b}^{(2)}=p\cdot\boldsymbol{b}^{(1)}$. If $\boldsymbol{b}^{(2)}=0$ then, for every $i\in\mathbb{Z}$, each component of $\boldsymbol{b}_i^{(1)}$ has p^{k_1-1} as factor and so $\boldsymbol{b}^{(1)}\in\Psi(G^{\mathbb{Z}})$. Since $L(\boldsymbol{b}^{(1)})=0$, a configuration we are looking for is $\boldsymbol{b}'=\boldsymbol{b}^{(1)}$. After k_1-1 iterations, i.e., once we get $\boldsymbol{b}^{(k_1-1)}=p\cdot\boldsymbol{b}^{(k-2)}$ (with $\boldsymbol{b}^{(k-2)}\neq 0$), if $\boldsymbol{b}^{(k_1-1)}=0$ holds we conclude that $\boldsymbol{b}'=\boldsymbol{b}^{(k_1-2)}$ by using the same argument of the previous steps. Otherwise, by definition, for every $i\in\mathbb{Z}$ each component of $\boldsymbol{b}_i^{(k_1-1)}$ itself certainly contains p^{k_1-1} as factor. Therefore, $\boldsymbol{b}^{(k_1-1)}\in\Psi(G^{\mathbb{Z}})$. Moreover, $L(\boldsymbol{b}^{(k_1-1)})=0$. Hence, we can set $\boldsymbol{b}'=\boldsymbol{b}^{(k_1-1)}$ and this concludes the proof. □

The following lemma will be useful for studying both surjectivity and other properties.

Lemma 22. *Let $(G^{\mathbb{Z}},F)$ and $(\hat{G}^{\mathbb{Z}},L)$ be any Additive CA over G and any LCA over $\hat{G}$, respectively, such that $L\circ\Psi=\Psi\circ F$. Then, the CA $(G^{\mathbb{Z}},F)$ is surjective if and only if $(\hat{G}^{\mathbb{Z}},L)$ is.*

Proof. $\Longleftarrow$: Assume that F is not surjective. Then, by the Garden of Eden theorem [35, 36], F is not injective on the finite configurations, i.e., there exist two distinct and finite configurations $\boldsymbol{c}', \boldsymbol{c}'' \in G^{\mathbb{Z}}$ with $F(\boldsymbol{c}') = F(\boldsymbol{c}'')$. Therefore, the element $\boldsymbol{c} = \boldsymbol{c}' - \boldsymbol{c}'' \in G^{\mathbb{Z}}$ is a finite configuration such that $\boldsymbol{c} \neq 0$ and $F(\boldsymbol{c}) = 0$. So, we get both $\Psi(\boldsymbol{c}) \neq 0$ and $L(\Psi(\boldsymbol{c})) = \Psi(F(\boldsymbol{c})) = 0$. Since $\Psi(\boldsymbol{c}) \neq 0$, it follows that L is not surjective.
$\Longrightarrow$: Assume that L is not surjective. Then it is not injective on the finite configurations. Thus, there exist a finite configuration $\boldsymbol{b} \neq 0$ with $L(\boldsymbol{b}) = 0$. By Lemma 21, there exists a finite configuration $\boldsymbol{b}' \in \Psi(G^{\mathbb{Z}})$ such that $\boldsymbol{b}' \neq 0$ and $L(\boldsymbol{b}') = 0$. Let $\boldsymbol{c} \in G^{\mathbb{Z}}$ be the finite configuration such that $\Psi(\boldsymbol{c}) = \boldsymbol{b}'$. Clearly, it holds that $\boldsymbol{c} \neq 0$. We get $\Psi(F(\boldsymbol{c})) = L(\Psi(\boldsymbol{c})) = 0$. Since Ψ is injective, it follows that $F(\boldsymbol{c}) = 0$. Therefore, we conclude that F is not surjective. □

Next two theorems state that surjectivity and injectivity behave as sensitivity when looking at an Additive CA over G and the associated LCA via the embedding Ψ.

Theorem 23. *Let $(G^{\mathbb{Z}}, F)$ be any Additive CA over G and let $(\hat{G}^{\mathbb{Z}}, L)$ be the LCA associated with it via the embedding Ψ. Then, the CA $(G^{\mathbb{Z}}, F)$ is surjective if and only if $(\hat{G}^{\mathbb{Z}}, L)$ is.*

Proof. Use Lemma 22. □

Theorem 24. *Let $(G^{\mathbb{Z}}, F)$ be any Additive CA and let $(\hat{G}^{\mathbb{Z}}, L)$ be the LCA associated with it via the embedding Ψ. Then, the CA $(G^{\mathbb{Z}}, F)$ is injective if and only if $(\hat{G}^{\mathbb{Z}}, L)$ is.*

Proof. $\Longleftarrow$: Assume that F is not injective. Then, there exist two distinct configurations $\boldsymbol{c}, \boldsymbol{c}' \in G^{\mathbb{Z}}$ with $F(\boldsymbol{c}) = F(\boldsymbol{c}')$. We get $L(\Psi(\boldsymbol{c})) = \Psi(F(\boldsymbol{c})) = \Psi(F(\boldsymbol{c}')) = L(\Psi(\boldsymbol{c}'))$ and, since Ψ is injective, it follows that L is not injective.
$\Longrightarrow$: Assume that L is not injective. Then, there exists a configuration $\boldsymbol{b} \in \hat{G}^{\mathbb{Z}}$ such that $\boldsymbol{b} \neq 0$ and $L(\boldsymbol{b}) = 0$. By Lemma 21, there exists a configuration $\boldsymbol{b}' \in \Psi(G^{\mathbb{Z}})$ such that $\boldsymbol{b}' \neq 0$ and $L(\boldsymbol{b}') = 0$. Let $\boldsymbol{c} \in G^{\mathbb{Z}}$ be the configuration such that $\Psi(\boldsymbol{c}) = \boldsymbol{b}'$. Clearly, it holds that $\boldsymbol{c} \neq 0$. We get $\Psi(F(\boldsymbol{c})) = L(\Psi(\boldsymbol{c})) = 0$. Since Ψ is injective, it follows that $F(\boldsymbol{c}) = 0$. Since $F(0) = 0$, we conclude that F is not injective. □

4.3. Topological transitivity and ergodicity

We start by proving that the embedding Ψ also preserves topological transitivity between an Additive CA over G and the associated LCA.

Theorem 25. *Let $(G^{\mathbb{Z}}, F)$ be any Additive CA over G and let $(\hat{G}^{\mathbb{Z}}, L)$ be the LCA associated with it via the embedding Ψ. Then, the CA $(G^{\mathbb{Z}}, F)$ is topologically transitive if and only if $(\hat{G}^{\mathbb{Z}}, L)$ is.*

Proof. Since $\Psi \circ F = L \circ \Psi$, for every $k \in \mathbb{N}$ it holds that $\Psi \circ (F^k - I) = \Psi \circ F^k - \Psi = L^k \circ \Psi - \Psi = (L^k - I) \circ \Psi$. By Lemma 22 , $F^k - I$ is surjective iff $L^k - I$ is. Theorem 23 and 7 conclude the proof. □

As a final result, we get the decidability of many mixing and ergodic properties for Additive CA over any finite abelian group, including chaos, ergodicity, and topological transitivity.

Corollary 26. *All the following properties are decidable for Additive CA over any finite abelian group: (1) chaos; (2) ergodicity; (3) topological transitivity; (4) topological mixing; (5) weak topological transitivity; (6) total transitivity; (7) weak ergodic mixing; (8) ergodic mixing.*

Proof. It is an immediate consequence of Theorem 7 and 25. □

5. Applications

The above decidability results find application in several computer science domains. We are going to deal with some cryptographic applications that are nowadays of crucial importance and, in particular, illustrate how our results can be exploited for improving the existing methods already based on CA (especially LCA).

Before proceeding, we want to stress the class of Additive CA over a finite abelian group is richer than LCA. Indeed, for a same alphabet cardinality and the same radius, the former includes also rules over a finite abelian group G that, according to situation **(S3)** from Section 4, has some set $\bigoplus_{i=1}^{n} \mathbb{Z}/p^{k_i}\mathbb{Z}$ as subgroup or it agrees with such a set.

Block Encryption Several schemes exist that are based on linear higher-order CA over $\mathbb{Z}/m\mathbb{Z}$ (see for instance [7], where the size of the alphabet and the memory used are $m = 2$ and $n = 2$, respectively), i.e., those specific, and in a sense simpler, LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ with associated matrix in Frobenius normal form.

Since the choice of the local rule plays a relevant role to get a method of high quality in several respects and the class of Additive CA is richer than LCA, we propose the following significant modifications to the existing schemes.

First of all, the linear local rule is replaced with one giving rise to an Additive CA F over the abelian group $\mathbb{Z}/256\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (instead of a LCA over $(\mathbb{Z}/2\mathbb{Z})^2$ with associated matrix in Frobenius normal form) in order that, once the radius and the alphabet are fixed, the variety of local rules to be chosen, and then the security of the cryptosystem, strongly increases. According to Definition 12, the LCA L over $(\mathbb{Z}/256\mathbb{Z})^2$ associated with the Additive CA F is also built.

Furthermore, by virtue of Theorems 24 and 25, algorithms from Theorems 6 and 7 checking reversibility, ergodicity, and chaos for LCA are included in the encryption schemes in order that a good rule is chosen, i.e., one defining an Additive CA which is at the same time reversible, ergodic, and chaotic. Indeed, besides reversibility which allows recovering the exact original plaintext from the cyphertext, block encryption systems have to satisfy the so-called *confusion* and *diffusion* properties [2]. Being just the dynamical counterparts of confusion and diffusion for the dynamical system on which the cryptosystem is based, ergodicity and chaos ensure that these required cryptographic properties hold.

The setup phase of the scheme consists of the following steps:

$SetupBE-1$. A first part of bits of the plaintext to be cyphered are collected in bytes, each of them represented as element of $\mathbb{Z}/256\mathbb{Z}$, and put in the first component c^1 while the remaining ones, just as they are, are put in the second component c^2 with elements in $\mathbb{Z}/2\mathbb{Z}$, respectively, of the initial configuration

$$\boldsymbol{c} = \begin{pmatrix} c^1 \\ c^2 \end{pmatrix}$$

of an Additive CA F to be built over the abelian group $G = \mathbb{Z}/256\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$SetupBE-2a$. Then, an Additive CA $(G^{\mathbb{Z}}, F)$ over G with radius 1 local rule $\delta : G^3 \to G$ is built as follows. A pseudo random number generator provides the values of the functions δ_{-1}, δ_0, and δ_1 from (2) over the generators of the group G, i.e., the values $\alpha_{i,j}^{(z)}$ for $z = -1, 0, 1$, and $i, j = 1, 2$ such that

$$\delta_{-1}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\alpha_{1,1}^{(-1)}\\ \alpha_{2,1}^{(-1)}\end{pmatrix} \quad , \quad \delta_{-1}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha_{1,2}^{(-1)}\\ \alpha_{2,2}^{(-1)}\end{pmatrix} \quad ,$$

$$\delta_{0}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\alpha_{1,1}^{(0)}\\ \alpha_{2,1}^{(0)}\end{pmatrix} \quad , \quad \delta_{0}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha_{1,2}^{(0)}\\ \alpha_{2,2}^{(0)}\end{pmatrix} \quad ,$$

$$\delta_{1}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\alpha_{1,1}^{(1)}\\ \alpha_{2,1}^{(1)}\end{pmatrix} \quad , \quad \delta_{1}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha_{1,2}^{(1)}\\ \alpha_{2,2}^{(1)}\end{pmatrix} \quad ,$$

where, for any z and j as above, $\alpha_{1,j}^{(z)} \in \mathbb{Z}/256\mathbb{Z}, \alpha_{2,j}^{(z)} \in \mathbb{Z}/2\mathbb{Z}$, and, in addition, the constraints $\alpha_{1,2}^{(-1)}, \alpha_{1,2}^{(0)}, \alpha_{1,2}^{(1)} \in \{0, 128\}$ must necessarily hold in order that δ_{-1}, δ_0, and δ_1 are endomorphisms of G. In this way, according to Definition 12, the LCA $(\hat{G}^{\mathbb{Z}}, L)$ over $\hat{G} = (\mathbb{Z}/256\mathbb{Z})^2$ associated with $(G^{\mathbb{Z}}, F)$ is defined by the matrices $A_{-1}, A_0, A_1 \in (\mathbb{Z}/256\mathbb{Z})^{2\times 2}$, where

$$A_{-1} = \begin{bmatrix} \alpha_{1,1}^{(-1)} & 2^{-7}\alpha_{1,2}^{(-1)} \\ 2^7\alpha_{2,1}^{(-1)} & \alpha_{2,2}^{(-1)} \end{bmatrix} ,$$
$$A_0 = \begin{bmatrix} \alpha_{1,1}^{(0)} & 2^{-7}\alpha_{1,2}^{(0)} \\ 2^7\alpha_{2,1}^{(0)} & \alpha_{2,2}^{(0)} \end{bmatrix} ,$$
$$A_1 = \begin{bmatrix} \alpha_{1,1}^{(1)} & 2^{-7}\alpha_{1,2}^{(1)} \\ 2^7\alpha_{2,1}^{(1)} & \alpha_{2,2}^{(1)} \end{bmatrix} ,$$

or, equivalently, by the matrix $A = \sum_{z=-1}^{1} A_z X^{-z} \in \mathbb{Z}/256\mathbb{Z}\left[X, X^{-1}\right]^{2\times 2}$,

i.e.,

$$A = \begin{bmatrix} \alpha_{1,1}^{(1)} X^{-1} + \alpha_{1,1}^{(0)} + \alpha_{1,1}^{(-1)} X^{1} & 2^{-7}\alpha_{1,2}^{(1)} X^{-1} + 2^{-7}\alpha_{1,2}^{(0)} + 2^{-7}\alpha_{1,2}^{(-1)} X^{1} \\ 2^{7}\alpha_{2,1}^{(1)} X^{-1} + 2^{7}\alpha_{2,1}^{(0)} + 2^{7}\alpha_{2,1}^{(-1)} X^{1} & \alpha_{2,2}^{(1)} X^{-1} + \alpha_{2,2}^{(0)} + \alpha_{2,2}^{(-1)} X^{1} \end{bmatrix} .$$

Thus, the coefficients of the characteristic polynomial of A are (up to sign)

$$\det A = d_{1,1}X^{-2} + (d_{1,0} + d_{0,1})X^{-1} + (d_{1,-1} + d_{0,0} + d_{-1,1}) + (d_{0,-1} + d_{-1,0})X^{1} + d_{-1,-1}X^{2}$$

and

$$\mathrm{tr}(A) = \mathrm{tr}(A_1)X^{-1} + \mathrm{tr}(A_0) + \mathrm{tr}(A_{-1})X^{1} \ ,$$

where $d_{u,v} = \det\left(\delta_u \begin{pmatrix} 1 \\ 0 \end{pmatrix} \delta_v \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$, for $u, v = -1, 0, 1$.

At this point, an Additive CA F over the abelian group $\mathbb{Z}/256\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the LCA L over $(\mathbb{Z}/256\mathbb{Z})^2$ associated with F have been built.

$SetupBE-2b$. Algorithms from Theorems 6 and 7 run on L, i.e., on the coefficients $\mathrm{tr}(A)$ and $\det(A)$ of the characteristic polynomial of A, to establish whether, by virtue of Theorems 24 and 25, F is at the same time reversible, chaotic, and ergodic.

Steps $SetupBE-2a$ and $SetupBE-2b$ are repeated until an Additive CA with the required properties is outputted.

The encryption phase simply consists in computing, for some $\ell > 2$, the next ℓ elements of the dynamical evolution of F starting from $\boldsymbol{c}$. The cyphertext is just $F^{\ell}(\boldsymbol{c})$.

We stress that about $1/7$ turns out to be the fraction of the injective, i.e., reversible, Additive CA over a total of 2^{33} possible distinct ones that can be outputted by step $SetupBE-2a$ at varying all the possible 12-tuples of values $\alpha_{i,j}^{(z)}$. The scenario resulting from these numbers represents a huge improvement with respect to the corresponding one involving linear higher-order CA over $\mathbb{Z}/2\mathbb{Z}$ (as for instance in [7]) and where these numbers are very small. In particular, one reversible Additive CA can be detected from a large set of reversible Additive ones during step $SetupBE-2b$. Hence, our modification to the scheme consisting of the introduction and the use, as above illustrated, of Additive CA for encrypting a plaintext increases the security level of the scheme itself. Furthermore, according to step $SetupBE-2b$, the addition of the algorithms ensuring confusion and diffusion, made it possible by Theorems 24 and 25, makes attacks much harder.

Secret Sharing Schemes. Secret sharing schemes are those methods that define how a secret can be shared among different participants. Regarding the existing methods based on CA, the secret is inserted in an initial configuration of a reversible linear higher-order CA F over $\mathbb{Z}/2\mathbb{Z}$ of memory n (that can be seen as a LCA over $(\mathbb{Z}/2\mathbb{Z})^n$ with associated matrix in Frobenius normal

form) and, after a certain number of iterations of F starting from the initial configuration, the n-th components inside the last l configurations obtained are the shares (see for instance [34, 8]). Each share is distributed by a trusted authority among the l participants in such a way that only suitable subsets of them can recover the secret. This is done putting together the shares and calculating back the initial configuration by means of the inverse of the CA.

The use of Additive CA improves the schemes. Indeed, the same points about both the choice of the local rule and the properties of the global behavior discussed for block encryption apply here. Therefore, we propose the following modifications to the standard secret sharing schemes based on CA.

An Additive CA F over the abelian group $G = \mathbb{Z}/256\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \ldots \times \mathbb{Z}/2\mathbb{Z}$, where $\mathbb{Z}/2\mathbb{Z}$ appears $n-1$ times, is used instead of a LCA over $(\mathbb{Z}/2\mathbb{Z})^n$ with associated matrix in Frobenius normal form. In this way, once the radius is fixed, the number of local rules to be chosen hugely increases. The local rule of F is defined by the values of every δ_i from (2) over the generators of the group G. Such values can be chosen by a further modification of the standard scheme in order that, by virtue of Theorems 24 and 25, a reversible, chaotic, and ergodic Additive CA is defined. Then, they are suitably distributed by the trusted authority to the participants together with the shares.

Remark 27. The fact that the values of the generators are also distributed to the participants is a novelty and hence it represents a further difference with respect to the existing schemes. Moreover, in the method we propose, unlike the standard scheme, each share contains a piece of (blended besides disjoint) information from each, instead of one, element among n out of the last l configurations obtained by means of iterations of F starting from the initial configuration in which the secret has been inserted. As a matter of fact, now the CA used in the scheme is no longer strongly limited to be an LCA with associated matrix in Frobenius normal form.

Let us detail the modified scheme involving l participants, i.e., with (n, l)-threshold, by starting with the setup phase which is comprised of the following two steps.

$SetupSS-1$. The bits of the secret are collected in bytes, each of them represented as element of $\mathbb{Z}/256\mathbb{Z}$, and put in the first component c^1 of the initial configuration

$$\boldsymbol{c} = \begin{pmatrix} c^1 \\ \vdots \\ c^n \end{pmatrix}$$

of an Additive CA F to be built over the abelian group $G = \mathbb{Z}/256\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \ldots \times \mathbb{Z}/2\mathbb{Z}$. The remaining components $c^2, \ldots, c^n$ are provided by the mutually trusted party (MTP) by means of a pseudo random number generator.

$SetupSS-2a$. An Additive CA $(G^{\mathbb{Z}}, F)$ over G with local rule $\delta : G^{2r+1} \to G$ of radius r is built by the MTP which provides a natural number $r > 0$, i.e., the radius of F, and the values of the functions $\delta_{-r}, \ldots, \delta_0, \ldots \delta_r$ from Equation (2) over the generators of the group G, i.e., the values

$$\alpha_{i,j}^{(z)} = \delta_z(e_j)^i \quad \text{for } z = -r, \ldots, r, \text{ and } i, j = 1, \ldots, n, \tag{3}$$

where, for each z and j, $\alpha_{1,j}^{(z)} \in \mathbb{Z}/256\mathbb{Z}$, $\alpha_{i,j}^{(z)} \in \mathbb{Z}/2\mathbb{Z}$ for $i = 2, \ldots, n$, and, in addition, for each z and $j = 2, \ldots, n$, the constraint $\alpha_{1,j}^{(z)} \in \{0, 128\}$ must necessarily hold in order that δ_z is an endomorphism of G. In this way, according to Definition 12, the LCA $(\hat{G}^{\mathbb{Z}}, L)$ over $\hat{G} = (\mathbb{Z}/256\mathbb{Z})^n$ associated with $(G^{\mathbb{Z}}, F)$ is defined by the matrices $A_{-r}, \ldots A_r \in (\mathbb{Z}/256\mathbb{Z})^{n \times n}$, where for each z, i, and j, the (i, j)-entry of A_z is

$$a_{i,j}^{(z)} = \begin{cases} 2^{-7}\alpha_{i,j}^{(z)} & \text{if } i = 1,\ j > 1, \\ 2^{7}\alpha_{i,j}^{(z)} & \text{if } j = 1,\ i > 1, \\ \alpha_{i,j}^{(z)} & \text{otherwise} \ , \end{cases}$$

or, equivalently, by $A = \sum_{z=-r}^{r} A_z X^{-z} \in \mathbb{Z}/256\mathbb{Z}\left[X, X^{-1}\right]^{n \times n}$.

$SetupSS-2b$. By virtue of Theorems 24 and 25, the algorithms for establishing whether F is at the same time reversible, chaotic, and ergodic are run on A.

Steps $SetupSS-2a$ and $SetupSS-2b$ are repeated until an Additive CA with the required properties is outputed.

The sharing phase is carried out by the MTP which computes, for some $\ell \geq n$, the next $\ell + l - 1$ elements

$$F(\boldsymbol{c}), F^2(\boldsymbol{c}), \ldots, F^{\ell}(\boldsymbol{c}), \ldots, F^{\ell+l-1}(\boldsymbol{c})$$

of the dynamical evolution of F starting from $\boldsymbol{c}$. For each $h = 1, \ldots, l$, the share that the MTP distributes to the h-th participant is the vector

$$\begin{pmatrix} F^{\ell+h-1}(\boldsymbol{c})^1 \\ F^{\ell+h-2}(\boldsymbol{c})^2 \\ \vdots \\ F^{\ell+h-n}(\boldsymbol{c})^n \end{pmatrix}$$

together with the values of the $2r+1$ endomorphisms over the h'-th generator $e_{h'}$ of G

$$\delta_{-r}(e_{h'}), \ldots, \delta_r(e_{h'}) \ ,$$

where $h' = (h-1) \bmod n + 1$. In this way, any set of n consecutive participants $h, h+1, \ldots, h+n-1$ are able to rebuild the element $F^{\ell+h-1}(\boldsymbol{c})$ together with the local rule δ and compute back the initial configuration $\boldsymbol{c}$ from which the secret c^1 can be extracted.

Let us describe now the impact of our modifications to the standard scheme over a significant case, namely, the secret sharing scheme with $(3,4)$-threshold for texts of 64 bits used in [8]. Such a scheme is based on a LCA over $(\mathbb{Z}/2\mathbb{Z})^n$ with associated matrix in Frobenius normal form and fixed radius $r=1$.

The CA we propose to use is then an Additive CA over the abelian group $G = \mathbb{Z}/256\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ defined by the 27 values $\alpha_{i,j}^{(z)}$ $(z=-1,0,1,\ i,j=1,2,3)$ that the MTP provides according to Equation (3). In this way, the LCA L over $(\mathbb{Z}/256)^3$ associated with F is defined by the matrix $A\in\mathbb{Z}/256\mathbb{Z}\left[X,X^{-1}\right]^{3\times 3}$ where for each i,j the (i,j)-entry of A is

$$a_{i,j}=\begin{cases}2^{-7}\alpha_{i,j}^{(1)}X^{-1}+2^{-7}\alpha_{i,j}^{(0)}+2^{-7}\alpha_{i,j}^{(-1)}X^{1} & \text{if } i=1,\ j>1,\\ 2^{7}\alpha_{i,j}^{(1)}X^{-1}+2^{7}\alpha_{i,j}^{(0)}+2^{7}\alpha_{i,j}^{(-1)}X^{1} & \text{if } j=1,\ i>1,\\ \alpha_{i,j}^{(1)}X^{-1}+\alpha_{i,j}^{(0)}+\alpha_{i,j}^{(-1)}X^{1} & \text{otherwise }.\end{cases}$$

Thus, we get that

$$\begin{aligned}\det A = {} & d_{1,1,1}X^{-3}+(d_{1,1,0}+d_{1,0,1}+d_{0,1,1})X^{-2}+\\ & +(d_{1,1,-1}+d_{1,0,0}+d_{1,-1,1}+d_{0,1,0}+d_{0,0,1}+d_{-1,1,1})X^{-1}+\\ & +(d_{1,-1,0}+d_{1,0,-1}+d_{0,1,-1}+d_{0,0,0}+d_{0,-1,1}+d_{-1,1,0}+d_{-1,0,1})X^{0}+\\ & +(d_{1,-1,-1}+d_{0,0,-1}+d_{0,-1,0}+d_{-1,1,-1}+d_{-1,0,0}+d_{-1,-1,1})X^{1}+\\ & +(d_{0,-1,-1}+d_{-1,0,-1}+d_{-1,-1,0})X^{2}+d_{-1,-1,-1}X^{3}\ ,\end{aligned}$$

where $d_{u,v,w}=\det\left(\delta_u\begin{pmatrix}1\\0\\0\end{pmatrix}\delta_v\begin{pmatrix}0\\1\\0\end{pmatrix}\delta_w\begin{pmatrix}0\\0\\1\end{pmatrix}\right)$, for $u,v,w=-1,0,1$.

By considering all the possible 27-tuple of values $\alpha_{i,j}^{(z)}$, it follows that step $SetupSS-2a$ provides one Additive CA over a total of 2^{48} possible distinct ones. We estimated that among them just under 6% are reversible. We got this outcome by repeatedly running the algorithm from Theorem 24 on $\det(A)$ at varying A among a sample of all the matrices that can be defined in step $SetupSS-2a$. As in the case of data encryption, our modifications to the standard scheme give rise to a scenario that, on the basis of these numbers and the addition of the algorithms ensuring confusion and diffusion, represents a significant improvement with respect to the corresponding one where linear higher-order CA over $\mathbb{Z}/2\mathbb{Z}$ are used.

6. Conclusions and perspectives

In this paper we have provided many decidability and characterization results about the dynamical behavior of Additive CA over finite abelian groups. Moreover, we have described how our results can be exploited in some emblematic applications of cryptosystems such as block encryption and secret sharing schemes. Indeed, we have proposed significant modifications to the existing methods, i.e., the use of

Additive CA instead of the simpler LCA and the addition of the decision algorithms from Theorems 24 and 25. In this way, the security of the resulting cryptosystems strongly increases.

The are several research directions that are worth investigating from both theoretical and applicative points of view.

First of all, one might ask what results and characterizations are still true when considering non abelian groups. Furthermore, it would be very interesting to find out characterization or decidability results about positive expansivity and strong transitivity. Since these are stronger conditions of chaos for Additive CA, they could be required by the cryptographic methods in order these latter improve even more from the security point of view. Finally, an important research direction consists in generalizing our results to higher dimensions. Besides having a theoretical value, they will be certainly useful in many applications as for instance the encryption or compression of images and other multidimensional data [34, 32].

Going back to the results of the present paper, further possible investigations concern how they can be exploited to improve the existing pseudo random number generators (PRNG). Indeed, the most recent PNRG based on cellular models involve linear non-uniform (or hybrid) CA over $\mathbb{Z}/m\mathbb{Z}$ (see for instance [37, 38]). These are variants of CA where cells use different local rules (see [17, 18, 19] for an introduction and recent results on non-uniform CA). The random numbers are got by the dynamical evolution of one fixed cell. Since linear non-uniform CA over $\mathbb{Z}/m\mathbb{Z}$ used in applications are homeomorphic to LCA over $(\mathbb{Z}/m\mathbb{Z})^n$, we can state that the functioning of such PNRG depends on the dynamical behavior of these latter. In particular, the studies on the existing methods show that the choice of the (local and then global) transition rules is crucial in order to reach a high quality pseudorandomness and an appropriate period length. As already pointed out, the class of Additive CA over a finite abelian group is richer than LCA. Therefore, that is a more suitable container of which one can draw rules up for further improving the existing methods. Moreover, since a chaotic behavior is required to the dynamical systems on which PNRG are based and chaos agrees with topological transitivity for Additive CA, the algorithm deciding topological transitivity is an important tool to be added in applications for providing, by virtue of Theorem 25, PNRG based on chaotic Additive CA.

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

[4] 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.

[5] Gianpiero Cattaneo, Alberto Dennunzio, and Luciano Margara. Chaotic subshifts and related languages applications to one-dimensional cellular automata. *Fundamenta Informaticae*, 52(1-3):39–80, 2002.

[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] 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.

[8] 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.

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

[10] 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.

[11] 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.

[12] 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.

[13] Alberto Dennunzio, Enrico Formenti, Darij Grinberg, and Luciano Margara. An efficiently computable characterization of stability and instability for linear cellular automata. *To appear*, 2021.

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

[15] Alberto Dennunzio, Enrico Formenti, Luca Manzoni, Luciano Margara, and Antonio E. Porreca. On the dynamical behaviour of linear higher-order cellular automata and its decidability. *Information Sciences*, 486:73–87, 2019.

[16] Alberto Dennunzio, Enrico Formenti, Luca Manzoni, Giancarlo Mauri, and Antonio E. Porreca. Computational complexity of finite asynchronous cellular automata. *Theoretical Computer Science*, 664:131–143, 2017.

[17] Alberto Dennunzio, Enrico Formenti, and Julien Provillard. Non-uniform cellular automata: Classes, dynamics, and decidability. *Information and Computation*, 215:32 – 46, 2012.

[18] Alberto Dennunzio, Enrico Formenti, and Julien Provillard. Local rule distributions, language complexity and non-uniform cellular automata. *Theoretical Computer Science*, 504:38–51, 2013.

[19] Alberto Dennunzio, Enrico Formenti, and Julien Provillard. Three research directions in non-uniform cellular automata. *Theoretical Computer Science*, 559:73 – 90, 2014.

[20] 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.

[21] Alberto Dennunzio, Pierre Guillon, and Benoît Masson. Stable dynamics of sand automata. In Giorgio Ausiello, Juhani Karhumäki, Giancarlo Mauri, and Chih-Hao Luke Ong, editors, *Fifth IFIP International Conference On Theoretical Computer Science - TCS 2008, IFIP 20th World Computer Congress, TC 1, Foundations of Computer Science, September 7-10, 2008, Milano, Italy*, volume 273 of *IFIP*, pages 157–169. Springer, 2008.

[22] Alberto Dennunzio, Pierre Guillon, and Benoît Masson. Sand automata as cellular automata. *Theoretical Computer Science*, 410(38-40):3962–3974, 2009.

[23] 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.

[24] Robert Luke Devaney. *An Introduction to Chaotic Dynamical Systems*. Addison-Wesley advanced book program. Addison-Wesley, 1989.

[25] Fabio Farina, Gianpiero Cattaneo, and Alberto Dennunzio. Grid and HPC dynamic load balancing with lattice boltzmann models. In Robert Meersman and Zahir Tari, editors, *On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, OTM Confederated International Conferences, CoopIS, DOA, GADA, and ODBASE 2006, Montpellier, France, October 29 - November 3, 2006. Proceedings, Part II*, volume 4276 of *Lecture Notes in Computer Science*, pages 1152–1162. Springer, 2006.

[26] Fabio Farina and Alberto Dennunzio. A predator-prey cellular automaton with parasitic interactions and environmental effects. *Fundamenta Informaticae*, 83(4):337–353, 2008.

[27] Masanobu Ito, Nobuyasu Osato, and Masakazu Nasu. Linear cellular automata over $\mathbb{Z}_m$. *Journal of Computer and Systems Sciences*, 27:125–140, 1983.

[28] Jarkko Kari. Rice's theorem for the limit sets of cellular automata. *Theoretical Computer Science*, 127(2):229–254, 1994.

[29] 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.

[30] Petr Kůrka. Languages, equicontinuity and attractors in cellular automata. *Ergodic Theory and Dynamical Systems*, 17(2):417–433, 1997.

[31] Petr Kůrka. *Topological and Symbolic Dynamics*. Volume 11 of Cours Spécialisés. Société Mathématique de France, 2004.

[32] Olu Lafe. Data compression and encryption using cellular automata transforms. *Engineering Applications of Artificial Intelligence*, 10(6):581 – 591, 1997.

[33] 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.

[34] Gonzalo Álvarez Marañón, Luis Hernández Encinas, and Ángel Martín del Rey. A multisecret sharing scheme for color images based on cellular automata. *Information Sciences*, 178(22):4382–4395, 2008.

[35] Edward Forrest Moore. Machine models of self-reproduction. *Proceedings of Symposia in Applied Mathematics*, 14:13–33, 1962.

[36] John Myhill. The converse to Moore's garden-of-eden theorem. *Proceedings of the American Mathematical Society*, 14:685–686, 1963.

[37] Sukumar Nandi, B. K. Kar, and Parimal Pal Chaudhuri. Theory and applications of cellular automata in cryptography. *IEEE Trans. Computers*, 43(12):1346–1357, 1994.

[38] C. Fraile Rubio, Luis Hernández Encinas, S. Hoya White, Ángel Martín del Rey, and Gerardo Rodríguez Sánchez. The use of linear hybrid cellular automata as pseudo random bit generators in cryptography. *Neural Parallel & Scientific Comp.*, 12(2):175–192, 2004.

[39] Claude E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28(4):656–715, 1949.