On the dynamical behaviour of linear higher-order cellular automata and its decidability

Alberto Dennunzio[a], Enrico Formenti[b], Luca Manzoni[a], Luciano Margara[c], Antonio E. Porreca[a,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]*Department of Computer Science and Engineering, University of Bologna, Cesena Campus, Via Sacchi 3, Cesena, Italy*
[d]*Aix Marseille Université, Université de Toulon, CNRS, LIS, Marseille, France*

Abstract

Higher-order cellular automata (HOCA) are a variant of cellular automata (CA) used in many applications (ranging, for instance, from the design of secret sharing schemes to data compression and image processing), and in which the global state of the system at time t depends not only on the state at time $t-1$, as in the original model, but also on the states at time $t-2, \ldots, t-n$, where n is the memory size of the HOCA. We provide decidable characterizations of two important dynamical properties, namely, sensitivity to the initial conditions and equicontinuity, for linear HOCA over the alphabet $\mathbb{Z}_m$. These characterizations have an impact in applications since the involved linear HOCA are usually required to exhibit a chaotic or stable behaviour. Moreover, they extend the ones shown in [28] for linear CA (LCA) over the alphabet $\mathbb{Z}_m^n$ in the case $n = 1$. We also show that linear HOCA of memory size n over $\mathbb{Z}_m$ form a class that is indistinguishable from a specific subclass of LCA over $\mathbb{Z}_m^n$. This enables to decide injectivity and surjectivity for linear HOCA of memory size n over $\mathbb{Z}_m$ using the decidable characterization provided in [2] and [25] for injectivity and surjectivity of LCA over $\mathbb{Z}_m^n$. Finally, we prove an equivalence between LCA over $\mathbb{Z}_m^n$ and an important class of non-uniform CA, another variant of CA used in many applications.

Keywords: cellular automata, higher-order cellular automata, linear cellular automata, sensitivity to the initial conditions, decidability, discrete dynamical systems

1. Introduction

Cellular automata (CA) are well-known formal models of natural computing which have been successfully applied in a wide number of fields to simulate complex phenomena involving local, uniform, and synchronous processing (for recent results and an up-to date bibliography on CA, see [30, 19, 10, 1, 9], while for other models of natural computing see for instance [15, 12, 20]). More formally, a CA is made of an infinite set of identical finite automata arranged over a regular cell grid (usually $\mathbb{Z}^d$ in dimension d) and all taking a state from a finite set S called the *set of states* or the *alphabet* of the CA. In this paper, we consider one-dimensional CA. A *configuration* is a snapshot of all states of the automata, i.e., a function $c : \mathbb{Z} \to S$. A *local rule* updates the state of each automaton on the basis of its current state and the ones of a finite set of neighboring automata. All automata are updated synchronously. In the one-dimensional settings, a CA over (the alphabet) S is a structure $\langle S, r, f \rangle$ where $r \in \mathbb{N}$ is the *radius* and $f : S^{2r+1} \to S$ is the local rule which updates, for each $i \in \mathbb{Z}$, the state of the automaton in the position i of the grid $\mathbb{Z}$ on the basis of states of the automata in the positions $i-r, \ldots, i+r$. A configuration is an element of $S^{\mathbb{Z}}$ and describes the (global) state of the CA. The feature of synchronous updating induces the

Email addresses: dennunzio@disco.unimib.it (Alberto Dennunzio), enrico.formenti@unice.fr (Enrico Formenti), luca.manzoni@disco.unimib.it (Luca Manzoni), luciano.margara@unibo.it (Luciano Margara), antonio.porreca@lis-lab.fr (Antonio E. Porreca)

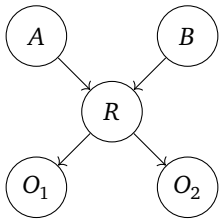
following *global rule* $F : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ defined as

$$\forall c \in S^{\mathbb{Z}}, \forall i \in \mathbb{Z}, \qquad F(c)_i = f(c_{i-r}, \dots c_{i+r}) \ .$$

As such, the global map F describes the change from any configuration c at any time $t \in \mathbb{N}$ to the configuration $F(c)$ at $t+1$ and summarises the main features of the CA model, namely, the fact that it is defined through a local rule which is applied uniformly and synchronously to all cells.

Because of a possible inadequacy, in some contexts, of every single one of the three defining features, variants of the original CA model started appearing, each one relaxing one among these three features. Asynchronous CA relax synchrony (see [23, 31, 13, 14, 11] for instance), non-uniform CA relax uniformity ([18, 16, 17]), while hormonal CA (for instance) relax locality [5]. However, from the mathematical point of view all those systems, as well as the original model, fall in the same class, namely, the class of autonomous discrete dynamical systems (DDS) and one could also precise *memoryless* systems. Indeed, the latter compute their next global state just on the basis of their current state, while the past ones play no active role. Allowing the original model to take into account past states leads to a further natural variant which can further extend the application range of the model itself.

As a motivating example, consider the following classical network routing problem. Assume to have two packet sources A and B which are connected to a common router R which in its turn is connected to two receiving hosts O_1 and O_2 as illustrated below.



If R receives a packet m_A from A but none from B, then it sends m_A to the output hosts O_1 and O_2; if both A and B send a packet, m_A and m_B, respectively, then m_B is enqueued and m_A is transmitted to O_1 and O_2. Of course, the more frequently simultaneous packets from A and B arrive at R, the longer the queue has to be in order to avoid packet loss. When a whole network is considered, this routing problem can be easily solved using a variant of CA in which the state of each node keeps track of the current state of the router and the past states which represent the received but not yet transmitted packets.

As to the possible variants of the original CA model, in [33], Toffoli introduced *higher-order CA* (HOCA), i.e., variants of CA in which the updating of the state of a cell also depends on the past states of the cell itself and its neighbours. In particular, he showed that any arbitrary reversible *linear* HOCA can be embedded in a reversible *linear CA* (LCA), where linear means that the local rule is linear. Essentially, the trick consisted in memorizing past states and recover them later on. Some years later, Le Bruyn and Van Den Bergh explained and generalized the Toffoli construction and proved that any linear HOCA having the ring $S = \mathbb{Z}_m$ as alphabet and memory size n can be simulated by a LCA over the alphabet $\mathbb{Z}_m^n$ (see the precise definition in Section 2) [2]. In this way, as we will see in Section 2, a practical way to decide injectivity (which is equivalent to reversibility in this setting) and surjectivity of HOCA can be easily derived by the characterization of the these properties for the corresponding LCA simulating them. Indeed, in [2] and [25], characterizations of injectivity and surjectivity of a LCA over $\mathbb{Z}_m^n$ are provided in terms of properties of the determinant of the matrix associated with it, where the determinant turns out to be another LCA (over $\mathbb{Z}_m$ and then a LCA simpler than that over $\mathbb{Z}_m^n$). Since the properties of LCA over $\mathbb{Z}_m$ (i.e., LCA over $\mathbb{Z}_m^n$ with $n = 1$) have been extensively studied and related decidable characterizations have been obtained [28, 3, 7, 4], one derives the algorithms to decide injectivity and surjectivity for LCA over $\mathbb{Z}_m^n$ and, then, as we will see in Section 2, also for HOCA over $\mathbb{Z}_m$ of memory size n, by means of the associated matrix.

Applications of HOCA (in particular the linear ones) cover a wide span of topics, ranging from the design of secret sharing schemes [8, 29] and encryption [6] to data compression and image processing [21]. Remark that, (linear) HOCA are often required to exhibit a chaotic or a strongly stable behavior (depending on the real-world situation) in order they can be used in applications, as for instance in those above mentioned.

The purpose of the present paper is to study, in the context of linear HOCA, sensitivity to the initial conditions and equicontinuity, where the former is the well-known basic component and essence of the chaotic behavior of a DDS, while the latter represents a strong form of stability. To do that, we put in evidence that any linear HOCA of memory size n over $\mathbb{Z}_m$ is not only simulated by, but also topologically conjugated to a LCA over $\mathbb{Z}_m^n$ defined by a matrix having a specific form. Thus, in order to decide injectivity and surjectivity for linear HOCA of memory size n over $\mathbb{Z}_m$, by means of that specific matrix one can use the decidable characterization provided in [2] and [25] for deciding the same properties for LCA over $\mathbb{Z}_m^n$. As main result, we prove that sensitivity to the initial conditions and equicontinuity are decidable properties for linear HOCA of memory size n over $\mathbb{Z}_m$(Theorem 14). In particular we provide a decidable characterization of those properties, in terms of the matrix associated with a linear HOCA. Remark that if $n = 1$, starting from our characterizations, one recovers exactly the well-known ones of sensitivity and equicontinuity for LCA over $\mathbb{Z}_m$. Moreover, HOCA over $\mathbb{Z}_m$ exhibit dynamical behaviours that are not captured by LCA over $\mathbb{Z}_m$.

The decidability result about sensitivity to the initial conditions has an impact in applications. Consider the secret sharing schemes designed by linear HOCA (see [8, 29], for instance). It is clear that the involved automata have to be reversible, i.e., injective, to make the decoding process of the secret possible. As above pointed out, in order to check reversibility or build reversible linear HOCA, one can use the decidable characterization provided in [2] and [25]. If, in addition, the involved linear HOCA is sensitive to the initial conditions (this can be checked by our algorithm), a possible knowledge of an even good approximation of the shares would hardly help an attacker to recover the secret. Indeed, the action of the HOCA global rule is able to amplify the error between any configuration belonging to the evolution starting from such an approximation and the configuration which, at the same time, belongs to the evolution starting from the correct initial condition (i.e., consisting of the correct shares) and falling to the secret. Also in the case of data encryption performed by linear HOCA (see [6]) reversibility of the system is not enough. Sensitivity to the initial conditions is necessary to secure the resulting method against basic differential attacks. Again, reversibility is required when linear HOCA are used for image compression. However, in the context of image filtering (most of time) it is also desirable that the filtering of images which differ by just few pixels produce similar results. Hence, the HOCA performing such a process should not be sensitive to the initial conditions. Therefore, our algorithm can be used in applications to build suitable linear HOCA with an improvement of the existing methods.

Finally, we prove an equivalence between LCA over $\mathbb{Z}_m^n$ and an important class of linear non-uniform cellular automata. This result gives strong motivations to further study LCA over $\mathbb{Z}_m^n$ in the next future. First of all, non-uniform cellular automata is indeed another variant of cellular automata which is used in many applications (in particular, the linear ones). For instance, as pointed out in [25], linear non-uniform cellular automata can be used as subband encoders for compressing signals and images [32]. Moreover, little is known for linear non-uniform cellular automata from the point of view of the dynamical behavior and its decidability.

2. Higher-Order CA and Linear CA

We begin by reviewing some general notions and introducing notations we will use throughout the paper.

A *discrete dynamical system* (DDS) is a pair $(\mathcal{X}, \mathcal{F})$ where $\mathcal{X}$ is a space equipped with a metric, i.e., a metric space, and $\mathcal{F}$ is a transformation on $\mathcal{X}$ which is continuous with respect to that metric. The *dynamical evolution* of a DDS $(\mathcal{X}, \mathcal{F})$ starting from the initial state $x^{(0)} \in \mathcal{X}$ is the sequence $\{x^{(t)}\}_{t\in\mathbb{N}} \subseteq \mathcal{X}$ where $x^{(t)} = \mathcal{F}^t(x^{(0)})$ for any $t \in \mathbb{N}$.

When $\mathcal{X} = S^{\mathbb{Z}}$ for some set finite S, $\mathcal{X}$ is usually equipped with the metric d defined as follows

$$\forall c, c' \in S^{\mathbb{Z}}, \quad d(c, c') = \frac{1}{2^n} \quad \text{where } n = \min\{i \geq 0 \,:\, c_i \neq c'_i \text{ or } c'_{-i} \neq c'_{-i}\} \ .$$

Recall that $S^{\mathbb{Z}}$ is a compact, totally disconnected and perfect topological space (i.e., $S^{\mathbb{Z}}$ is a Cantor space).

Any CA $\langle S, r, f \rangle$ defines the DDS $(S^{\mathbb{Z}}, F)$, where F is the CA global rule (which is continuous by Hedlund's Theorem [22]). From now on, for the sake of simplicity, we will sometimes identify a CA with its global rule F or with the DDS $(S^{\mathbb{Z}}, F)$.

Recall that two DDS $(\mathcal{X}, \mathcal{F})$ and $(\mathcal{X}', \mathcal{F}')$ are *topologically conjugated* if there exists a homeomorphism $\phi : \mathcal{X} \mapsto \mathcal{X}'$ such that $\mathcal{F}' \circ \phi = \phi \circ \mathcal{F}$, while the *product* of $(\mathcal{X}, \mathcal{F})$ and $(\mathcal{X}', \mathcal{F}')$ is the DDS $(\mathcal{X} \times \mathcal{X}', \mathcal{F} \times \mathcal{F}')$ where $\mathcal{F} \times \mathcal{F}'$ is

defined as $\forall (x,x') \in \mathcal{X} \times \mathcal{X}'$, $(\mathcal{F} \times \mathcal{F}')(x,x') = (\mathcal{F}(x), \mathcal{F}'(x'))$ and the space $\mathcal{X} \times \mathcal{X}'$ is as usual endowed with the infinite product metric, i.e., the metric defined by the infinite norm of the two-dimensional vector of the distances measured in X and X'.

Notation 2.1. *For all $i, j \in \mathbb{Z}$ with $i \leq j$, we write $[i,j] = \{i, i+1, \dots, j\}$ to denote the interval of integers between i and j. For any $n \in \mathbb{N}$ and any set Z the set of all $n \times n$ matrices with coefficients in Z and the set of Laurent polynomials with coefficients in Z will be noted by $Mat(n,Z)$ and $Z\left[X, X^{-1}\right]$, respectively. In the sequel, bold symbols are used to denote vectors, matrices, and configurations over a set of states consisting of vectors. Moreover, m will be an integer bigger than 1 and $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ the ring with the usual sum and product modulo m. For any $\boldsymbol{x} \in \mathbb{Z}^n$ (resp., any matrix $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}\left[X, X^{-1}\right]\right)$), we will denote by $[\boldsymbol{x}]_m \in \mathbb{Z}_m^n$ (resp., $[\boldsymbol{M}(X)]_m$), the vector (resp., the matrix) in which each component x^i of $\boldsymbol{x}$ (resp., every coefficient of each element of $\boldsymbol{M}(X)$) is taken modulo m. In the sequel, for the sake of clarity, we will often use the notation $[\,]_m$, even when the modulo is not strictly needed. Finally, for any matrix $\boldsymbol{M}(X) \in \mathbb{Z}_m\left[X, X^{-1}\right]$ and any $t \in \mathbb{N}$, the t-th power of $\boldsymbol{M}(X)$ will be noted more simply by $\boldsymbol{M}^t(X)$ instead of $(\boldsymbol{M}(X))^t$.*

Definition 1 (Higher-Order Cellular Automata). A *Higher-Order Cellular Automata (HOCA)* is a structure $\mathcal{H} = \langle k, S, r, h \rangle$ where $k \in \mathbb{N}$ with $k \geq 1$ is the *memory* size, S is the *alphabet*, $r \in \mathbb{N}$ is the *radius*, and $h : S^{(2r+1)k} \to S$ is the *local rule*. Any HOCA $\mathcal{H}$ induces the *global rule* $H : \left(S^{\mathbb{Z}}\right)^k \to \left(S^{\mathbb{Z}}\right)^k$ associating any vector $\boldsymbol{e} = (e^1, \dots, e^k) \in \left(S^{\mathbb{Z}}\right)^k$ of k configurations of $S^{\mathbb{Z}}$ with the vector $H(\boldsymbol{e}) \in \left(S^{\mathbb{Z}}\right)^k$ such that $H(\boldsymbol{e})^j = e^{j+1}$ for each $j \neq k$ and

$$\forall i \in \mathbb{Z}, \quad H(\boldsymbol{e})_i^k = h\begin{pmatrix} e^1_{[i-r,i+r]} \\ e^2_{[i-r,i+r]} \\ \vdots \\ e^k_{[i-r,i+r]} \end{pmatrix}$$

In this way, $\mathcal{H}$ defines the DDS $\left(\left(S^{\mathbb{Z}}\right)^k, H\right)$. As for CA, we sometimes identify a HOCA with its global rule or the DDS defined by it. Moreover, we will often refer to a HOCA over S to stress the alphabet over which the HOCA is defined.

Remark 2. It is easy to check that for any HOCA $\mathcal{H} = \langle k, S, r, h \rangle$ there exists a CA $\left\langle S^k, r, f \right\rangle$ which is topologically conjugated to $\mathcal{H}$.

The study of the dynamical behaviour of HOCA is still at its early stages; a few results are known for the class of *linear HOCA*, namely, those HOCA defined by a local rule h which is *linear*, i.e., S is $\mathbb{Z}_m$ and there exist coefficients $a_i^j \in \mathbb{Z}_m$ ($j = 1, \dots, k$ and $i = -r, \dots, r$) such that for any element

$$\boldsymbol{x} = \begin{pmatrix} x^1_{-r} & \dots & x^1_r \\ x^2_{-r} & \dots & x^2_r \\ \vdots & & \\ x^k_{-r} & \dots & x^k_r \end{pmatrix} \in \mathbb{Z}_m^{(2r+1)k}, \quad h(\boldsymbol{x}) = \left[\sum_{j=1}^{k}\sum_{i=-r}^{r} a_i^j x_i^j\right]_m .$$

It is easy to see that linear HOCA are additive, i.e.,

$$\forall \boldsymbol{c}, \boldsymbol{d} \in \left(\mathbb{Z}_m^{\mathbb{Z}}\right)^k, \quad H(\boldsymbol{c} + \boldsymbol{d}) = H(\boldsymbol{c}) + H(\boldsymbol{d})$$

where, with the usual abuse of notation, $+$ denotes the natural extension of the sum over $\mathbb{Z}_m$ to both $\mathbb{Z}_m^{\mathbb{Z}}$ and $\left(\mathbb{Z}_m^{\mathbb{Z}}\right)^k$.

In [2], a much more convenient representation is introduced for the case of linear HOCA (in dimension $d = 1$) by means of the following notion.

Definition 3 (Linear Cellular Automata). A *Linear Cellular Automaton* (LCA) over the alphabet $\mathbb{Z}_m^n$ is a CA $\mathcal{L} = \left\langle \mathbb{Z}_m^n, r, f \right\rangle$ where the local rule $f : (\mathbb{Z}_m^n)^{2r+1} \to \mathbb{Z}_m^n$ is defined by $2r+1$ matrices $\boldsymbol{M}_{-r}, \ldots, \boldsymbol{M}_0, \ldots, \boldsymbol{M}_r \in Mat(n, \mathbb{Z}_m)$ as follows: $f(\boldsymbol{x}_{-r}, \ldots, \boldsymbol{x}_0, \ldots, \boldsymbol{x}_r) = \left[\sum_{i=-r}^{r} \boldsymbol{M}_i \cdot \boldsymbol{x}_i\right]_m$, for any $(\boldsymbol{x}_{-r}, \ldots, \boldsymbol{x}_0, \ldots, \boldsymbol{x}_r) \in (\mathbb{Z}_m^n)^{2r+1}$.

Remark 4. LCA over $\mathbb{Z}_m^n$ have been strongly investigated in the case $n = 1$ and all the dynamical properties have been characterized in terms of the 1×1 matrices (i.e., coefficients) defining the local rule, in any dimension too [28, 3].

We recall that any linear HOCA $\mathcal{H}$ can be simulated by a suitable LCA, as shown in [2]. Precisely, given a linear HOCA $\mathcal{H} = \langle k, \mathbb{Z}_m, r, h \rangle$, where h is defined by the coefficients $a_i^j \in \mathbb{Z}_m$, the LCA simulating $\mathcal{H}$ is $\mathcal{L} = \left\langle \mathbb{Z}_m^k, r, f \right\rangle$ with f defined by following matrices

$$\boldsymbol{M}_0 = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ddots & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ a_0^1 & a_0^2 & a_0^3 & \ldots & a_0^{k-1} & a_0^k \end{bmatrix}, \tag{1}$$

and, for $i \in [-r, r]$ with $i \neq 0$,

$$\boldsymbol{M}_i = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 0 \\ a_i^1 & a_i^2 & a_i^3 & \ldots & a_i^{k-1} & a_i^k \end{bmatrix}. \tag{2}$$

Remark 5. We want to put in evidence that a stronger result actually holds (easy proof, important remark): any linear HOCA $\mathcal{H}$ is topologically conjugated to the LCA $\mathcal{L}$ defined by the matrices in (1) and (2). Clearly, the converse also holds: for any LCA defined by the matrices in (1) and (2) there exists a linear HOCA which is topologically conjugated to it. In other words, up to a homeomorphism the whole class of linear HOCA is identical to the subclass of LCA defined by the matrices above introduced. In the sequel, we will call $\mathcal{L}$ the *matrix presentation* of $\mathcal{H}$.

We are now going to show a stronger and useful new fact, namely, that the class of linear HOCA is nothing but the subclass of LCA represented by a formal power series which is a matrix in Frobenius normal form. Before proceeding, let us recall the *formal power series* (fps) which have been successfully used to study the dynamical behaviour of LCA in the case $n = 1$ [24, 28]. The idea of this formalism is that configurations and global rules are represented by suitable polynomials and the application of the global rule turns into multiplications of polynomials. In the more general case of LCA over $\mathbb{Z}_m^n$, a configuration $\boldsymbol{c} \in (\mathbb{Z}_m^n)^{\mathbb{Z}}$ can be associated with the fps

$$\boldsymbol{P}_{\boldsymbol{c}}(X) = \sum_{i \in \mathbb{Z}} \boldsymbol{c}_i X^i = \begin{bmatrix} c^1(X) \\ \vdots \\ c^n(X) \end{bmatrix} = \begin{bmatrix} \sum_{i \in \mathbb{Z}} c_i^1 X^i \\ \vdots \\ \sum_{i \in \mathbb{Z}} c_i^n X^i \end{bmatrix}$$

Then, if F is the global rule of a LCA defined by $\boldsymbol{M}_{-r}, \ldots, \boldsymbol{M}_0, \ldots, \boldsymbol{M}_r$, one finds

$$\boldsymbol{P}_{F(\boldsymbol{c})}(X) = [\boldsymbol{M}(X) \boldsymbol{P}_{\boldsymbol{c}}(X)]_m$$

where

$$\boldsymbol{M}(X) = \left[\sum_{i=-r}^{r} \boldsymbol{M}_i X^{-i}\right]_m$$

is the *finite fps*, or, *the matrix*, *associated with the LCA* F. In this way, for any integer $t > 0$ the fps associated with F^t is $\boldsymbol{M}(X)^t$, and then $\boldsymbol{P}_{F^t(\boldsymbol{c})}(X) = [\boldsymbol{M}(X)^t \boldsymbol{P}_{\boldsymbol{c}}(X)]_m$. Throughout this paper, $\boldsymbol{M}(X)^t$ will refer to $[\boldsymbol{M}(X)^t]_m$.

A matrix $\boldsymbol{M}(X) \in Mat\left(n, Z\left[X, X^{-1}\right]\right)$ is in *Frobenius normal form* if

$$\boldsymbol{M}(X) = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \ddots & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ \mathbb{m}_0(X) & \mathbb{m}_1(X) & \mathbb{m}_2(X) & \dots & \mathbb{m}_{n-2}(X) & \mathbb{m}_{n-1}(X) \end{bmatrix} \tag{3}$$

where each $\mathbb{m}_i(X) \in Z\left[X, X^{-1}\right]$

From now on, for a given matrix $\boldsymbol{M}(X) \in Mat\left(n, Z\left[X, X^{-1}\right]\right)$ in Frobenius normal form, $\mathbb{m}(X)$ will always make reference to its n-th row.

Definition 6 (Frobenius LCA). A LCA F over the alphabet $\mathbb{Z}_m^n$ is said to be a *Frobenius LCA* if the fps $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_m\left[X, X^{-1}\right]\right)$ associated with F is in Frobenius normal form.

It is immediate to see that a LCA is a Frobenius one iff it is defined by the matrices in (1) and (2), i.e., iff it is topologically conjugated to a linear HOCA. This fact together with Remark 5 and Definition 6, allow us to state the following

Proposition 7. *Up to a homeomorphism, the class of linear HOCA over* $\mathbb{Z}_m$ *of memory size* n *is nothing but the class of Frobenius LCA over* $\mathbb{Z}_m^n$.

At this point we want to stress that the action of a Frobenius LCA F, or, equivalently, a linear HOCA, over a configuration $\boldsymbol{c} \in (\mathbb{Z}_m^n)^{\mathbb{Z}}$ can be viewed as a bi-infinite array of *linear–feedback shift register*. Indeed, it holds that

$$\boldsymbol{P}_{F(\boldsymbol{c})}(X) = \boldsymbol{M}(X)\boldsymbol{P}_{\boldsymbol{c}}(X) = \begin{bmatrix} c^2(X) \\ \vdots \\ \sum_{i=1}^{n} \mathbb{m}_{i-1}(X) c^i(X) \end{bmatrix},$$

where the n–th component of the vector $\boldsymbol{P}_{F(\boldsymbol{c})}(X)$ is given by the sum of the results of the actions of n one-dimensional LCA over $\mathbb{Z}_m$ each of them applied on a different component of $\boldsymbol{P}_{\boldsymbol{c}}(X)$, or, in other words, on a different element of the memory of the linear HOCA which is topologically conjugated to F.

Remark 8. Actually, in literature a matrix is in Frobenius normal form if either it or its transpose has a form as in (3). Since any matrix in Frobenius normal form is conjugated to its transpose, any Frobenius LCA F is topologically conjugated to a LCA G such that the fps associated with G is the transpose of the fps associated with G. In other words, up to a homeomorphism, such LCA G, linear HOCA, and Frobenius LCA form the same class and, in particular, the action of G on any configuration $\boldsymbol{c} \in (\mathbb{Z}_m^n)^{\mathbb{Z}}$ is such that

$$\boldsymbol{P}_{G(\boldsymbol{c})}(X) = \boldsymbol{M}(X)^T \boldsymbol{P}_{\boldsymbol{c}}(X) = \begin{bmatrix} \mathbb{m}_0(X) c^n(X) \\ c^1(X) + \mathbb{m}_1(X) c^n(X) \\ \vdots \\ c^{n-1}(X) + \mathbb{m}_{n-1}(X) c^n(X) \end{bmatrix},$$

where $\boldsymbol{M}(X)^T$ is the transpose of the matrix $\boldsymbol{M}(X)$ associated to the LCA F which is topologically conjugated to G.

From now on, we will focus on Frobenius LCA, i.e., matrix presentations of linear HOCA. Indeed, they allow convenient algebraic manipulations that are very useful to study formal properties of linear HOCA. For example, in [2] and [25], the authors proved characterizations for injectivity and surjectivity for LCA in terms of the matrix $\boldsymbol{M}(X)$ associated to them and which turns out to be decidable by means of the characterization of injectivity and surjectivity for LCA over $\mathbb{Z}_m$ shown in [24].

Proposition 9 ([2, 25]). *Let $\left(\left(\mathbb{Z}_m^n\right)^{\mathbb{Z}}, F\right)$ be a LCA over $\mathbb{Z}_m^n$ and let $\boldsymbol{M}(X)$ be the matrix associated with F. Then, F is injective (resp., surjective) if and only if the determinant of $\boldsymbol{M}(X)$ is the fps associated with a injective (resp., surjective) LCA over $\mathbb{Z}_m$.*

We want to stress that, by Remark 5, Definition 6, and Proposition 7, one can use the characterizations from Proposition 9 for deciding injectivity and surjectivity of linear HOCA. Summarizing, the following result holds.

Proposition 10. *Injectivity and surjectivity are decidable properties for HOCA of memory size n over $\mathbb{Z}_m$.*

In this paper we are going to adopt a similar attitude, i.e., we are going to characterise the dynamical behaviour of linear HOCA by the properties of the matrices in their matrix presentation.

3. Dynamical properties and their decidability

In this paper we are particularly interested in the so-called *sensitivity to the initial conditions* and *equicontinuity*. As dynamical properties, they represent the main features of instable and stable DDS, respectively. The former is the well-known basic component and essence of the chaotic behavior of DDS, while the latter is a strong form of stability.

Let $(\mathcal{X}, \mathcal{F})$ be a DDS. The DDS $(\mathcal{X}, \mathcal{F})$ is *sensitive to the initial conditions* (or simply *sensitive*) if there exists $\varepsilon > 0$ such that for any $x \in \mathcal{X}$ and any $\delta > 0$ there is an element $y \in \mathcal{X}$ such that $d(y, x) < \delta$ and $d(\mathcal{F}^n(y), \mathcal{F}^n(x)) > \varepsilon$ for some $n \in \mathbb{N}$. Recall that, by Knudsen's Lemma [26], $(\mathcal{X}, \mathcal{F})$ is sensitive iff $(\mathcal{Y}, \mathcal{F})$ is sensitive where $\mathcal{Y}$ is any dense subset of $\mathcal{X}$ which is $\mathcal{F}$-invariant, i.e., $\mathcal{F}(\mathcal{Y}) \subseteq \mathcal{Y}$.

In the sequel, we will see that in the context of LCA an alternative way to study sensitivity is via equicontinuity points. An element $x \in \mathcal{X}$ is an *equicontinuity point* for $(\mathcal{X}, \mathcal{F})$ if $\forall \varepsilon > 0$ there exists $\delta > 0$ such that for all $y \in \mathcal{X}$, $d(x, y) < \delta$ implies that $d(\mathcal{F}^n(y), \mathcal{F}^n(x)) < \varepsilon$ for all $n \in \mathbb{N}$. The system $(\mathcal{X}, \mathcal{F})$ is said to be *equicontinuous* if $\forall \varepsilon > 0$ there exists $\delta > 0$ such that for all $x, y \in \mathcal{X}$, $d(x, y) < \delta$ implies that $\forall n \in \mathbb{N}$, $d(\mathcal{F}^n(x), \mathcal{F}^n(y)) < \varepsilon$. Recall that any CA $(S^{\mathbb{Z}}, F)$ is equicontinuous if and only if there exist two integers $q \in \mathbb{N}$ and $p > 0$ such that $F^q = F^{q+p}$ [27]. Moreover, for the subclass of LCA defined by $n = 1$ the following result holds:

Theorem 11 ([28]). *Let $(\mathbb{Z}_m^{\mathbb{Z}}, F)$ be a LCA where the local rule $f : (\mathbb{Z}_m)^{2r+1} \to \mathbb{Z}_m$ is defined by $2r + 1$ coefficients $m_{-r}, \ldots, m_0, \ldots, m_r \in \mathbb{Z}_m$. Denote by $\mathcal{P}$ the set of prime factors of m. The following statements are equivalent:*

1. *F is sensitive to the initial conditions;*
2. *F is not equicontinuous;*
3. *there exists a prime number $p \in \mathcal{P}$ which does not divide $\gcd(m_{-r}, \ldots, m_{-1}, m_1, \ldots, m_r)$.*

The dichotomy between sensitivity and equicontinuity still holds for general LCA.

Proposition 12. *Let $\left(\left(\mathbb{Z}_m^n\right)^{\mathbb{Z}}, F\right)$ be a LCA over $\mathbb{Z}_m^n$ and let $\boldsymbol{M}(X)$ 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. *$\left|\{\boldsymbol{M}^i(X), i \geq 1\}\right| = \infty$.*

Proof. It is clear that conditions 2. and 3. are equivalent. The equivalence between 1. and 2. is a consequence of linearity of F and Knudsen's Lemma applied on the subset of the finite configurations, i.e., those having a state different from the null vector only in a finite number of cells. □

An immediate consequence of Proposition 12 is that any characterization of sensitivity to the initial conditions in terms of the matrices defining LCA over $\mathbb{Z}_m^n$ would also provide a characterization of equicontinuity. In the sequel, we are going to show that such a characterization actually exists. First of all, we recall a result that helped in the investigation of dynamical properties in the case $n = 1$ and we now state it in a more general form for LCA over $\mathbb{Z}_m^n$ (immediate generalisation of the result in [3, 7]).

Let $\left((\mathbb{Z}_m^n)^{\mathbb{Z}}, F\right)$ be a LCA and let q be any factor of m. We will denote by $[F]_q$ the map $[F]_q : (\mathbb{Z}_q^n)^{\mathbb{Z}} \to (\mathbb{Z}_q^n)^{\mathbb{Z}}$ defined as $[F]_q(\boldsymbol{c}) = [F(\boldsymbol{c})]_q$, for any $\boldsymbol{c} \in (\mathbb{Z}_q^n)^{\mathbb{Z}}$.

Lemma 13 ([3, 7]). *Consider any LCA $\left((\mathbb{Z}_m^n)^{\mathbb{Z}}, F\right)$ with $m = pq$ and $\gcd(p,q) = 1$. It holds that the given LCA is topologically conjugated to $\left((\mathbb{Z}_p^n)^{\mathbb{Z}} \times (\mathbb{Z}_q^n)^{\mathbb{Z}}, [F]_p \times [F]_q\right)$.*

As a consequence of Lemma 13, if $m = p_1^{k_1} \cdots p_l^{k_l}$ is the prime factor decomposition of m, any LCA over $\mathbb{Z}_m^n$ is topologically conjugated to the product of LCAs over $\mathbb{Z}_{p_i^{k_i}}^n$. Since sensitivity is preserved under topological conjugacy for DDS over a compact space and the product of two DDS is sensitive if and only if at least one of them is sensitive, we will study sensitivity for Frobenius LCA over $\mathbb{Z}_{p^k}^n$. We will show a decidable characterization of sensitivity to the initial conditions for Frobenius LCA over $\mathbb{Z}_{p^k}^n$ (Theorem 31). Such a decidable characterization together with the previous remarks about the decomposition of m, the topological conjugacy involving any LCA over $\mathbb{Z}_m^n$ and the product of LCAs over $\mathbb{Z}_{p_i^{k_i}}^n$, and how sensitivity behaves with respect to a topological conjugacy and the product of DDS, immediately lead to state the main result of the paper.

Theorem 14. *Sensitivity and Equicontinuity are decidable for Frobenius LCA over $\mathbb{Z}_m^n$, or, equivalently, for linear HOCA over $\mathbb{Z}_m$ of memory size n.*

4. Sensitivity of Frobenius LCA over $\mathbb{Z}_{p^k}^n$

In order to study sensitivity of Frobenius LCA over $\mathbb{Z}_{p^k}^n$, we introduce two concepts about Laurent polynomials.

Definition 15 (deg^+ and deg^-). Given any polynomial $\mathbb{p}(X) \in \mathbb{Z}_{p^k}\left[X, X^{-1}\right]$, 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).

Example 16. Consider the Laurent polynomial $\mathbb{p}(X) = 4X^{-4} + 3X^{-3} + 3 + 7X^2 + 6X^5$ with coefficients in $\mathbb{Z}_8$. Then, $deg^+[\mathbb{p}(X)] = 2$ and $deg^-[\mathbb{p}(X)] = -3$.

Definition 17 (Sensitive polynomial). A polynomial $\mathbb{p}(X) \in \mathbb{Z}_{p^k}\left[X, X^{-1}\right]$ is *sensitive* if either $deg^+[\mathbb{p}(X)] > 0$ or $deg^-[\mathbb{p}(X)] < 0$. As a consequence, a Laurent polynomial $\mathbb{p}(X)$ is not sensitive iff $deg^+[\mathbb{p}(X)] = deg^-[\mathbb{p}(X)] = 0$.

Trivially, it is decidable to decide whether a Laurent polynomial is sensitive.

Remark 18. Consider a matrix $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form. By the Cayley-Hamilton Theorem, one obtains

$$\boldsymbol{M}^n(X) = \mathbb{m}_{n-1}(X)\boldsymbol{M}^{n-1}(X) + \cdots + \mathbb{m}_1(X)\boldsymbol{M}^1(X) + \mathbb{m}_0(X)I \ . \tag{4}$$

We now introduce two further matrices that will allow us to access the information hidden inside $\boldsymbol{M}(X)$.

Definition 19 ($\boldsymbol{U}(X)$, $\boldsymbol{L}(X)$, d^+, and d^-). For any matrix $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form the matrices $\boldsymbol{U}(X), \boldsymbol{L}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ associated with $\boldsymbol{M}(X)$ are the matrices in Frobenius normal

where each component $\mathbb{u}_i(X)$ and $\mathbb{l}_i(X)$ (with $i = 0, \ldots, n-1$) of the n-th row $\mathbb{u}(X)$ and $\mathbb{l}(X)$ of $\boldsymbol{U}(X)$ and $\boldsymbol{L}(X)$, respectively, is defined as follows:

$$\mathbb{u}_i(X) = \begin{cases} \text{monomial of degree } deg^+[\mathbb{m}_i(X)] \text{ inside } \mathbb{m}_i(X) & \text{if } d_i^+ = d^+ \\ 0 & \text{otherwise} \end{cases}$$
$$\mathbb{l}_i(X) = \begin{cases} \text{monomial of degree } deg^-[\mathbb{m}_i(X)] \text{ inside } \mathbb{m}_i(X) & \text{if } d_i^- = d^- \\ 0 & \text{otherwise} \end{cases},$$

where $d_i^+ = \frac{deg^+[\mathbb{m}_i(X)]}{n-i}$, $d_i^- = \frac{deg^-[\mathbb{m}_i(X)]}{n-i}$, $d^+ = \max\{d_i^+\}$, and $d^- = \min\{d_i^-\}$.

Example 20. Consider the following matrix $\boldsymbol{M}(X) \in Mat\left(4, \mathbb{Z}_{49}[X, X^{-1}]\right)$ in Frobenius normal form

$$\boldsymbol{M}(X) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ X^{-2} + 1 + X + 2X^8 + 14X^{123} & 3X^{-3} + 3 + X^2 & 21X^{-70} + 4X^{-1} + 3X^4 & 7X^{-35} + X^{-1} + 3 \end{bmatrix}$$

We get $d_0^+ = 2$, $d_1^+ = \frac{2}{3}$, $d_2^+ = 2$, $d_3^+ = 0$ and $d_0^- = -\frac{1}{2}$, $d_1^- = -1$, $d_2^- = -\frac{1}{2}$, $d_3^- = -1$. Since $d^+ = 2$ and $d^- = -1$, it holds that $\mathbb{u}_0(X) = 2X^8$, $\mathbb{u}_1(X) = 0$, $\mathbb{u}_2(X) = 3X^4$, $\mathbb{u}_3(X) = 0$ and $\mathbb{l}_0(X) = 0$, $\mathbb{l}_1(X) = 3X^{-3}$, $\mathbb{l}_2(X) = 0$, $\mathbb{l}_3(X) = X^{-1}$. Therefore,

$$\boldsymbol{U}(X) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2X^8 & 0 & 3X^4 & 0 \end{bmatrix}$$

and

$$\boldsymbol{L}(X) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 3X^{-3} & 0 & X^{-1} \end{bmatrix}$$

Definition 21 ($\widehat{\boldsymbol{M}}(X)$ and $\overline{\boldsymbol{M}}(X)$). For any Laurent polynomial $\mathbb{p}(X) \in \mathbb{Z}_{p^k}\left[X, X^{-1}\right]$, $\widehat{\mathbb{p}}(X)$ and $\overline{\mathbb{p}}(X)$ are defined as the Laurent polynomial obtained from $\mathbb{p}(X)$ by removing all the monomials having coefficients that are multiple of p and $\overline{\mathbb{p}}(X) = \mathbb{p}(X) - \widehat{\mathbb{p}}(X)$, respectively. These definitions extend component-wise to vectors. For any matrix $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form, $\widehat{\boldsymbol{M}}(X)$ and $\overline{\boldsymbol{M}}(X)$ are defined as the matrix obtained from $\boldsymbol{M}(X)$ by replacing its n-th row $\mathbb{m}(X)$ with $\widehat{\mathbb{m}}(X)$ and $\overline{\boldsymbol{M}}(X) = \boldsymbol{M}(X) - \widehat{\boldsymbol{M}}(X)$, respectively.

It is clear that any matrix $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form can be written as $\boldsymbol{M}(X) = \widehat{\boldsymbol{M}}(X) + p\overline{\boldsymbol{M}'}(X)$, for some $\boldsymbol{M}'(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$.

Definition 22 (Graph $G_{\boldsymbol{M}}$). Let $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ be any matrix in Frobenius normal form. The graph $G_{\boldsymbol{M}} = \langle V_{\boldsymbol{M}}, E_{\boldsymbol{M}} \rangle$ associated with $\boldsymbol{M}(X)$ is such that $V_{\boldsymbol{M}} = \{1, \ldots, n\}$ and $E_{\boldsymbol{M}} = \{(h,k) \in V_{\boldsymbol{M}}^2 | \boldsymbol{M}(X)_k^h \neq 0\}$. Moreover, each edge $(h,k) \in E_{\boldsymbol{M}}$ is labelled with $\boldsymbol{M}(X)_k^h$.

Clearly, for any matrix $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form, any natural $t > 0$, and any pair (h,k) of entries, the element $\boldsymbol{M}^t(X)_k^h$ is the sum of the weights of all paths of length t starting from h and ending to k, where the weight of a path is the product of the labels of its edges.

Example 23. Consider any matrix $\boldsymbol{M}(X) \in Mat\left(4, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form. The graph $G_{\boldsymbol{M}}$ associated with $\boldsymbol{M}(X)$ is represented in Figure 1. It will help to compute $\boldsymbol{M}^t(X)_k^h$. Indeed, $\boldsymbol{M}^t(X)_k^h$ is the sum of

the labels of all paths of length t from vertex k to h (labels along edges of the same path multiply). For example for $(h,k)=(4,4)$ one finds

$$\begin{aligned}
\boldsymbol{M}^1(X)_4^4 &= \mathbb{m}_3(X)\\
\boldsymbol{M}^2(X)_4^4 &= (\mathbb{m}_3(X))^2 + \mathbb{m}_2(X)\\
\boldsymbol{M}^3(X)_4^4 &= \mathbb{m}_1(X) + 2\mathbb{m}_2(X)\mathbb{m}_3(X) + (\mathbb{m}_3(X))^3
\end{aligned}$$

and so on.

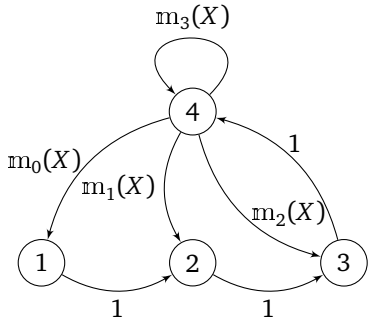


Figure 1: Graph $G_{\boldsymbol{M}}$ associated with $\boldsymbol{M}(X)$ from Example 23.

Lemma 24. *Let $p>1$ be a prime number and $a,b\geq 0$, $k>0$ be integers such that $1\leq a<p^k$ and $\gcd(a,p)=1$. Then,*

$$[a+pb]_{p^k}\neq 0 \tag{5}$$

Proof. For the sake of argument, assume that $[a+pb]_{p^k}=0$. Thus, $a+pb=cp^k$ for some $c\geq 0$ and then $a=cp^k-pb=p(cp^{k-1}-b)$, that contradicts $\gcd(a,p)=1$. □

Lemma 25. *Let $p>1$ be a prime number and h,k be two positive integers. Let $l_1,\ldots,l_h$ and $\alpha_1,\ldots,\alpha_h$ be positive integers such that $l_1<l_2<\cdots<l_h$ and for each $i=1,\ldots,h$ both $1\leq\alpha_i<p^k$ and $\gcd(\alpha_i,p)=1$ hold. Consider the sequence $b:\mathbb{Z}\to\mathbb{Z}_{p^k}$ defined for any $l\in\mathbb{Z}$ as*

$$\begin{aligned}
b_l &= \left[\alpha_1 b_{l-l_1}+\cdots+\alpha_h b_{l-l_h}\right]_{p^k} \quad \text{if } l>0\\
b_0 &= 1\\
b_l &= 0 \quad \text{if } l<0
\end{aligned} \tag{6}$$

Then, it holds that $[b_l]_p\neq 0$ for infinitely many $l\in\mathbb{N}$.

Proof. Set $dz=\left|\{l\in\mathbb{N}:[b_l]_p\neq 0\}\right|$. For the sake of argument, assume that dz is finite. Then, there exists $h_0\in\mathbb{N}$ such that $\left[b_{h_0}\right]_p\neq 0$ and $[b_l]_p=0$ for all $l>h_0$. Thus, there exist non negative integers $s_0,s_1,\ldots,s_{h-1}$ such that $b_{l_h+h_0}=ps_0$ and $b_{l_h+h_0-l_i}=ps_i$ for each $i=1,\ldots,h-1$. Equation (6) can be rewritten with $l=l_h+h_0$ as

$$b_{l_h+h_0}=\left[\alpha_1 b_{l_h+h_0-l_1}+\cdots+\alpha_{h-1}b_{l_h+h_0-l_{h-1}}+\alpha_h b_{h_0}\right]_{p^k}\ ,$$

which gives

$$ps_0=\left[\alpha_1 ps_1+\cdots+\alpha_{h-1}ps_{h-1}+\alpha_h b_{h_0}\right]_{p^k}\ .$$

Thus, there must exist an integer $s \geq 0$ such that

$$p\sum_{i=1}^{h-1}\alpha_i s_i + \alpha_h b_{h_0} = sp^k + ps_0 \ ,$$

or, equivalently,

$$\alpha_h b_{h_0} = p\left(sp^{k-1} + s_0 - \sum_{i=1}^{h-1}\alpha_i s_i\right) \ ,$$

with $ps_0 < p^k$. If $sp^{k-1} + s_0 - \sum_{i=1}^{h-1}\alpha_i s_i = 0$, we get $\alpha_h b_{h_0} = 0$ that contradicts either the assumption $\left[b_{h_0}\right]_p \neq 0$ or the hypothesis $1 \leq \alpha_h < p^k$. Otherwise, p must divide either α_h or b_{h_0}. However, that is impossible since $\gcd(\alpha_h, p) = 1$ and $\gcd(b_{h_0}, p) = 1$. □

For any matrix $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form, we are now going to study the behavior of $\boldsymbol{U}^t(X)$ and $\boldsymbol{L}^t(X)$, and, in particular, of their elements $\boldsymbol{U}^t(X)_n^n$ and $\boldsymbol{L}^t(X)_n^n$. These will turn out to be crucial in order to establish the sensitivity of the LCA defined by $\boldsymbol{M}(X)$. To make our arguments clearer we prefer to start with an example.

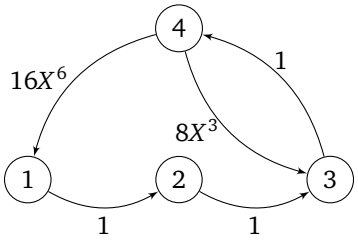
Example 26. Consider the following matrix $\boldsymbol{M}(X) \in Mat\left(4, \mathbb{Z}_{49}[X, X^{-1}]\right)$ in Frobenius normal form

$$\boldsymbol{M}(X) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ X^{-2}+1+X+16X^6 & 13X^{-3}+3+X^2 & 34X^{-1}+8X^3 & X^{-1}+31 \end{bmatrix}$$

One finds $d^+ = 3/2$ and then

$$\boldsymbol{U}(X) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 16X^6 & 0 & 8X^3 & 0 \end{bmatrix}$$

The graph G_U is represented in Figure 2, along with the values $\boldsymbol{U}^t(X)_4^4$ and td^+, for $t = 1, \ldots, 8$.



	$\boldsymbol{U}^t(X)_4^4$	td^+
$t=1$	0	3/2
$t=2$	$8X^3$	3
$t=3$	0	9/2
$t=4$	$31X^6$	6
$t=5$	0	15/2
$t=6$	$33X^9$	9
$t=7$	0	21/2
$t=8$	$25X^{12}$	12

Figure 2: The graph G_U (on the left), and the values $\boldsymbol{U}^t(X)_4^4$ and td^+, for $t = 1, \ldots, 8$ (on the right) from Example 26.

Notation 4.1. *For a sake of simplicity, for any given matrix $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form, from now on we will denote by $\mathbb{u}^{(t)}(X)$ and $\mathbb{l}^{(t)}(X)$ the elements $(\boldsymbol{U}^t(X))_n^n$ and $\boldsymbol{L}^t(X)_n^n$, respectively.*

Lemma 27. *Let $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ be a matrix such that $\boldsymbol{M}(X) = \widehat{\boldsymbol{N}}(X)$ for some matrix $\boldsymbol{N}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form. For any natural $t > 0$, $\mathbb{u}^{(t)}(X)$ (resp., $\mathbb{l}^{(t)}(X)$) is either null or a monomial of degree td^+ (resp., td^-).*

Proof. We show that the statement is true for $\mathfrak{u}^{(t)}(X)$ (the proof concerning $\mathbb{I}^{(t)}(X)$ is identical by replacing d^+, $\boldsymbol{U}(X)$ and related elements with d^-, $\boldsymbol{L}(X)$ and related elements). For each $i \in V_U$, let γ_i be the simple cycle of G_U from n to n and passing through the edge (n,i). Clearly, γ_i is the path $n \to i \to i+1 \ldots \to n-1 \to n$ (with γ_n the self-loop $n \to n$) of length $n-i+1$ and its weight is the monomial $\mathfrak{u}_{i-1}(X)$ of degree $(n-i+1)d^+$. We know that $\mathfrak{u}^{(t)}(X)$ is the sum of the weights of all cycles of length t starting from n and ending to n in G_U if at least one of such cycles exists, 0, otherwise. In the former case, each of these cycles can be decomposed in a certain number $s \geq 1$ of simple cycles $\gamma^1_{j_1}, \ldots, \gamma^s_{j_s}$ of lengths giving sum t, i.e., such that $\sum_{i=1}^{s}(n-j_i+1) = t$. Therefore, $(\boldsymbol{U}^t(X))^n_n$ is a monomial of degree $\sum_{i=1}^{s}(n-j_i+1)d^+ = td^+$. □

Lemma 28. *Let $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ be any matrix in Frobenius normal form. For every integer $t \geq 1$ both the following recurrences hold*

$$\mathfrak{u}^{(t)}(X) = \mathfrak{u}_{n-1}(X)\mathfrak{u}^{(t-1)}(X) + \cdots + \mathfrak{u}_1(X)\mathfrak{u}^{(t-n+1)}(X) + \mathfrak{u}_0(X)\mathfrak{u}^{(t-n)}(X) \quad (7)$$

$$\mathbb{I}^{(t)}(X) = \mathbb{I}_{n-1}(X)\mathbb{I}^{(t-1)}(X) + \cdots + \mathbb{I}_1(X)\mathbb{I}^{(t-n+1)}(X) + \mathbb{I}_0(X)\mathbb{I}^{(t-n)}(X) \quad (8)$$

with the related initial conditions

$$\mathfrak{u}^{(0)}(X) = 1, \quad \mathbb{I}^{(0)}(X) = 1 \quad (9)$$

$$\mathfrak{u}^{(l)}(X) = 0, \quad \mathbb{I}^{(l)}(X) = 0 \quad \text{for } l < 0. \quad (10)$$

Proof. We show the recurrence involving $\mathfrak{u}^{(t)}(X)$ (the proof for $\mathbb{I}^{(t)}(X)$ is identical by replacing $\boldsymbol{U}(X)$ and its elements with $\boldsymbol{L}(X)$ and its elements). Since $\boldsymbol{U}(X)$ is in Frobenius normal form too, by (4), Recurrence (7) holds for every $t \geq n$. It is clear that $\mathfrak{u}^{(0)}(X) = 1$. Furthermore, by the structure of the graph G_U and the meaning of $\boldsymbol{U}(X)^n_n$, Equation (7) is true under the initial conditions (9) and (10) for each $t = 1, \ldots, n-1$. □

Lemma 29. *Let $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ be a matrix such that $\boldsymbol{M}(X) = \widehat{\boldsymbol{N}}(X)$ for some matrix $\boldsymbol{N}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form. Let $\upsilon(t)$ (resp., $\lambda(t)$) be the coefficient of $\mathfrak{u}^{(t)}(X)$ (resp., $\mathbb{I}^{(t)}(X)$). It holds that $\gcd[\upsilon(t), p] = 1$ (resp., $\gcd[\lambda(t), p] = 1$), for infinitely many $t \in \mathbb{N}$.*
In particular, if the value d^+ (resp., d^-) associated with $\boldsymbol{M}(X)$ is non null, then for infinitely many $t \in \mathbb{N}$ both $\left[\mathfrak{u}^{(t)}(X)\right]_{p^k} \neq 0$ and $deg(\left[\mathfrak{u}^{(t)}(X)\right]_{p^k}) \neq 0$ (resp., $\left[\mathbb{I}^{(t)}(X)\right]_{p^k} \neq 0$ and $deg(\left[\mathbb{I}^{(t)}(X)\right]_{p^k}) \neq 0$) hold. In other terms, if $d^+ > 0$ (resp., $d^- < 0$) then $|\{\mathfrak{u}^{(t)}(X), t \geq 1\}| = \infty$ (resp., $|\{\mathbb{I}^t(X), t \geq 1\}| = \infty$).

Proof. We show the statements concerning $\upsilon(t)$, $\boldsymbol{U}(X)$, $\mathfrak{u}^{(t)}(X)$, and d^+. Replace X by 1 in the matrix $\boldsymbol{U}(X)$. Now, the coefficient $\upsilon(t)$ is just the element of position (n,n) in the t-th power of the obtained matrix $\boldsymbol{U}(1)$. Over $\boldsymbol{U}(1)$, the thesis of Lemma 28 is still valid replacing $\mathfrak{u}^{(t)}(X)$ by $\upsilon(t)$. Thus, for every $t \in \mathbb{N}$

$$\upsilon(t) = \mathfrak{u}_{n-1}(1)\upsilon(t-1) + \cdots + \mathfrak{u}_1(1)\upsilon(t-n+1) + \mathfrak{u}_0(1)\upsilon(t-n)$$

with initial conditions

$$\upsilon(0) = 1$$
$$\upsilon(l) = 0 \quad \text{for } l < 0,$$

where each $\mathfrak{u}_i(1)$ is the coefficient of the monomial $\mathfrak{u}_i(X)$ inside $\boldsymbol{U}(X)$. Thus, it follows that

$$[\upsilon(t)]_{p^k} = [\mathfrak{u}_{n-1}(1)\upsilon(t-1) + \cdots + \mathfrak{u}_1(1)\upsilon(t-n+1) + \mathfrak{u}_0(1)\upsilon(t-n)]_{p^k}$$

By Lemma 25 we obtain that $\gcd[\upsilon(t), p] = 1$ (and so $[\upsilon(t)]_{p^k} \neq 0$, too) for infinitely many $t \in \mathbb{N}$. In particular, if the value d^+ associated with $\boldsymbol{M}(X)$ is non null, then, by the structure of G_U and Lemma 27, both $\left[\mathfrak{u}^{(t)}(X)\right]_{p^k} \neq 0$ and $deg(\left[\mathfrak{u}^{(t)}(X)\right]_{p^k}) \neq 0$ hold for infinitely many $t \in \mathbb{N}$, too. Therefore, $|\{\mathfrak{u}^{(t)}(X), t \geq 1\}| = \infty$. The same proof runs for the statements involving $\lambda(t)$, $\boldsymbol{L}(X)$, $\mathfrak{u}^{(t)}(X)$, and d^- provided that these replace $\upsilon(t)$, $\boldsymbol{U}(X)$, $\mathfrak{u}^{(t)}(X)$, and d^+, respectively. □

The following Lemma puts in relation the behavior of $\mathbb{u}^{(t)}(X)$ or $\mathbb{l}^{(t)}(X)$ with that of $\widehat{\boldsymbol{M}}^t(X)_n^n$, for any matrix $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form.

Lemma 30. *Let $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ be a matrix in Frobenius normal form. If either $|\{\mathbb{u}^{(t)}(X), t \geq 1\}| = \infty$ or $|\{\mathbb{l}^{(t)}(X), t \geq 1\}| = \infty$ then $|\{\widehat{\boldsymbol{M}}^t(X)_n^n, t \geq 1\}| = \infty$.*

Proof. Assume that $|\{\mathbb{u}^{(t)}(X), t \geq 1\}| = \infty$. Since G_U is a subgraph of $G_{\widehat{\boldsymbol{M}}}$ (with different labels), for each integer t from Lemma 29 applied to $\widehat{\boldsymbol{M}}(X)$, the cycles of length t in $G_{\widehat{\boldsymbol{M}}}$ with weight containing a monomial of degree td^+ are exactly the cycles of length t in G_U. Therefore, it follows that $|\{\widehat{\boldsymbol{M}}^t(X)_n^n, t \geq 1\}| = \infty$. The same argument on G_L and involving d^- allows to prove the thesis if $|\{\mathbb{l}^{(t)}(X), t \geq 1\}| = \infty$.

We are now able to present and prove the main result of this section. It shows a decidable characterization of sensitivity for Frobenius LCA over $\mathbb{Z}_{p^k}^n$.

Theorem 31. *Let $\left((\mathbb{Z}_{p^k}^n)^{\mathbb{Z}}, F\right)$ be any Frobenius LCA over $\mathbb{Z}_{p^k}^n$ and let $(\mathbb{m}_0(X), \ldots, \mathbb{m}_{n-1})$ be the n-th row of the matrix $\boldsymbol{M}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form associated with F. Then, F is sensitive to the initial conditions if and only if $\mathbb{m}_i(X)$ is sensitive for some $i \in [0, n-1]$.*

Proof. Let us prove the two implications separately.
Assume that all $\mathbb{m}_i(X)$ are not sensitive. Then, $\widehat{\boldsymbol{M}}(X) \in Mat\left(n, \mathbb{Z}_{p^k}\right)$, i.e., it does not contain the formal variable X, and $\boldsymbol{M}(X) = \widehat{\boldsymbol{M}}(X) + p\boldsymbol{M}'(X)$, for some $\boldsymbol{M}'(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ in Frobenius normal form. Therefore, for any integer $t > 0$, $\boldsymbol{M}^t(X)$ is the sum of terms, each of them consisting of a product in which p^j appears as factor, for some natural j depending on t and on the specific term which p^j belongs to. Since every element of $\boldsymbol{M}^t(X)$ is taken modulo p^k, for any natural $t > 0$ it holds that in each term of such a sum p^j appears with $j \in [0, k-1]$ (we stress that j may depend on t and on the specific term of the sum, but it is always bounded by k). Therefore, $|\{\boldsymbol{M}^i(X) : i > 0\}| < \infty$ and so, by Proposition 12, F is not sensitive to the initial conditions.

Conversely, suppose that $\mathbb{m}_i(X)$ is sensitive for some $i \in [0, n-1]$ and $d^+ > 0$ (the case $d^- < 0$ is identical). By Definition 21, for any natural $t > 0$ there exists a matrix $\boldsymbol{M}'(X) \in Mat\left(n, \mathbb{Z}_{p^k}\left[X, X^{-1}\right]\right)$ such that $\boldsymbol{M}^t(X) = \widehat{\boldsymbol{M}}^t(X) + p\boldsymbol{M}'(X)$. By a combination of Lemmata 29 and 30, we get $|\{\widehat{\boldsymbol{M}}^t(X)_n^n, t \geq 1\}| = \infty$ and so, by Lemma 24, $|\{\boldsymbol{M}^t(X)_n^n, t \geq 1\}| = \infty$ too. Therefore, it follows that $|\{\boldsymbol{M}^t(X), t \geq 1\}| = \infty$ and, by Proposition 12, we conclude that F is sensitive to the initial conditions. □

Example 32. Consider the matrix in Frobenius normal $\boldsymbol{M}(X) \in Mat\left(4, \mathbb{Z}_{49}[X, X^{-1}]\right)$ from Example 26. Let F be the Frobenius LCA over $\mathbb{Z}_{49}^4$ such that $\boldsymbol{M}(X)$ is just the matrix associated to it. It is easy to check that F is sensitive since there exists at least one sensitive $\mathbb{m}_i(X)$ (in particular, all $\mathbb{m}_i(X)$ are sensitive).

Theorem 31 also allows to show that HOCA over $\mathbb{Z}_m$ exhibit dynamical behaviours that are not captured by the well known LCA over $\mathbb{Z}_m$.

Example 33. Consider the HOCA $\mathcal{H}$ of size memory 2 over $\mathbb{Z}_4$ such that its matrix presentation $\mathcal{L}$ is a LCA over $\mathbb{Z}_4^2$ having local rule defined by

$$\boldsymbol{M}_{-1} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad \boldsymbol{M}_0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad \boldsymbol{M}_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

The matrix in Frobenius normal formal associated with $\mathcal{L}$ is then

$$\boldsymbol{M}(X) = \begin{bmatrix} 0 & 0 \\ 0 & X \end{bmatrix} .$$

By Theorem 31, $\mathcal{L}$, and so $\mathcal{H}$, is sensitive to initial conditions since $deg^+[\mathbb{m}_1(X)] = 1 > 0$. However, by Proposition 9, $\mathcal{H}$ is not surjective since the determinant of $M(X) = 0$ does not define a surjective LCA over $\mathbb{Z}_4$. Remark that such a HOCA behaviour, i.e., one in which the system is sensitive but non surjective, can not be captured by LCA over $\mathbb{Z}_4$. Indeed, every sensitive CA over $\mathbb{Z}_{p^k}$, with p prime and $k > 0$, is also surjective (see [28, Theorem 3.1] and [24, Theorem 1]).

5. Application to real-world scenarios

This section illustrates the impact of our previous results in real-world scenarios. We stress that the presented applications are based on reversible linear HOCA. However, as we will explain in the sequel, reversibility is not enough and such HOCA need to be also sensitive to the initial conditions. Indeed, a reversible but not sensitive system is necessarily periodic. In that case, either the security level or the easy hardware implementation are compromised. Therefore, in order to the secure the involved methods, these can be equipped with the algorithm provided by our Theorem 31 for checking sensitivity.

Secret sharing scheme. In [8], Martín del Rey, Pereira Mateus, and Rodríguez Sánchez proposed a (k,n)-threshold secret sharing scheme involving n participants and based on linear HOCA of memory k over the alphabet $\mathbb{Z}_2$, each of them built starting from k LCA over $\mathbb{Z}_2$. Precisely, according to our definitions, any linear HOCA used in that proposed method is a structure $\langle k, \mathbb{Z}_2, r, h\rangle$ where the local rule $h\colon \mathbb{Z}_2^{(2r+1)k} \to \mathbb{Z}_2$ is defined as follows

$$\forall \boldsymbol{x} = \begin{pmatrix} x_{-r}^1 & \dots & x_r^1 \\ x_{-r}^2 & \dots & x_r^2 \\ \vdots & & \\ x_{-r}^k & \dots & x_r^k \end{pmatrix} \in \mathbb{Z}_2^{(2r+1)k}, \quad h(\boldsymbol{x}) = \left[\sum_{j=1}^{k} f^{(j)}(x_{i-r}^j, \dots, x_{i+r}^j) \right]_m ,$$

on the basis of the local rules $f^{(1)}, \dots, f^{(k)}$ of k linear LCA of radius r over $\mathbb{Z}_2$ such that each $f^{(j)}$ is expressed by a linear combination determined by coefficients $a_i^j \in \mathbb{Z}_2$ $(i = -r, \dots, r)$ with the constraint (over $f^{(1)}$) that $a_i^1 = 1$, if $i = 0$, while $a_i^1 = 0$, otherwise.

The method consists of three phases, namely, the setup, the sharing and the recovery one. The setup phase is comprised of the following steps:

1. By means of a pseudorandom number generator, the mutually trusted party (MTP) provides a natural r, i.e., the radius of the HOCA to be built, and $k-1$ integers $\omega_2, \dots, \omega_k$ with $0 \le \omega_j \le 2^{2r+1} - 1$, for $j = 2, \dots, k$. Each ω_j defines the coefficients $a_i^j \in \mathbb{Z}_2$ $(i = -r, \dots, r)$ of the local rule $f^{(j)}$ in such a way that $\omega_j = \sum_{i=-r}^{r} a_i^j 2^{i+r}$, i.e., the $(2r+1)$-tuple of the coefficients is just the binary representation of ω_j. Therefore, a HOCA $\mathcal{H} = \langle k, \mathbb{Z}_2, r, h\rangle$ is individuated, where h is defined on the basis of the local rules $f^{(1)}, \dots, f^{(k)}$, as above illustrated.
2. The vector representing the secret is put into the first component c^1 of the initial configuration $\boldsymbol{c}$ of $\mathcal{H}$.
3. By means of a cryptographic secure random number generator, the MTP provides the remaining $k-1$ components $c^2, \dots, c^k$ of the initial configuration $\boldsymbol{c}$.

The sharing phase is made up of the following steps:

1. Let H be the global rule of $\mathcal{H}$. On the basis of a pseudorandom integer $\ell \ge k$, the MTP computes the first $\ell + n$ elements of the dynamical evolution of $\mathcal{H}$ starting from the initial configuration $\boldsymbol{c}$:

$$\boldsymbol{c} = \begin{pmatrix} c^1 \\ \vdots \\ c^k \end{pmatrix} \to H(\boldsymbol{c}) \to H^2(\boldsymbol{c}) \to \cdots \to H^\ell(\boldsymbol{c}) \to \cdots \to H^{\ell+n-1}(\boldsymbol{c}) \ , \tag{11}$$

   where n is the number of participants.
2. The shares distributed to the n participants are the k-th components of the last n elements computed, i.e., $H^\ell(\boldsymbol{c})^k, \dots, H^{\ell+n-1}(\boldsymbol{c})^k$.

The recovery phase just consists in taking any consecutive k of the n shares and using the inverse of H to compute back the initial configuration $\boldsymbol{c}$ from which the secret c^1 can be extracted. Clearly, this is possible if $\mathcal{H}$ is reversible. The way the local rule h has been designed, namely, the constraint over $f^{(1)}$, assures this requirement.

We now want to highlight some important implications of our study over that method. First of all, reversibility can be also checked via Proposition 9 by means of the matrix $\boldsymbol{M}(X) \in Mat\left(k, \mathbb{Z}_2[X, X^{-1}]\right)$ in Frobenius normal form associated with the matrix presentation of $\mathcal{H}$, i.e., the Frobenius LCA $\mathcal{L}$ over $\mathbb{Z}_2^k$ which is topologically conjugated to $\mathcal{H}$. Indeed, under the above mentioned constraint, the matrices from (1) and (2) defining $\mathcal{L}$ and $\boldsymbol{M}(X)$ are such that the element $\mathbb{m}_0(X) = \sum_{i=-r}^{r} a_i^1 X^{-i}$ inside $\boldsymbol{M}(X)$ becomes

$$\mathbb{m}_0(X) = 1$$

Since the determinant of $\boldsymbol{M}(X)$ is just $\mathbb{m}_0(X)$, by Proposition 9, $\mathcal{H}$ is reversible. This remark leads us to consider that the constraint over $f^{(1)}$ can be replaced by the (random) choice of a one among $2r+1$ expressions to be used for $f^{(1)}$, each of them determined by a (random) value $s \in [-r, r]$ defining its coefficients: $a_i^1 = 1$, if $i = s$, and $a_i^1 = 0$, otherwise. Indeed, with such a choice, it holds that

$$\mathbb{m}_0(X) = X^{-s} \ ,$$

and then reversibility of the resulting HOCA is preserved. We want to stress that any expression different from the $2r+1$ possible ones gives rise to a non reversible HOCA. Moreover, the number of the expressions to be used for $f^{(1)}$ increases for schemes over an alphabet $\mathbb{Z}_m$ with $m > 2$. The introduction of such a choice in the scheme makes attacks much harder.

However, reversibility is not enough for designing such a method. Sensitivity to the initial conditions is a necessary property to secure the scheme against basic differential attacks. Indeed, if $\mathcal{H}$ is not sensitive then, by Proposition 12, it is equicontinuous. Thus, by a well-known result on reversible and equicontinuous CA, the HOCA global rule H is periodic, i.e., there exists a natural $t > 0$ such that $H^t(\boldsymbol{c}) = \boldsymbol{c}$ for any configuration $\boldsymbol{c}$ of $\mathcal{H}$. In that case, a possible knowledge of an even good approximation of k shares would leads by iterations of H to a good approximation of the secret. In other terms, if on the contrary $\mathcal{H}$ were sensitive, an even good approximation of the shares would hardly help an attacker to recover the secret. In the recovery phase of the method, the action of H^{-1} (which is sensitive too) is able to amplify the error between any configuration belonging to the evolution starting from such an approximation and the configuration which, at the same time, belongs to the evolution starting from the correct initial condition (i.e., consisting of the correct shares) and falling to the secret.

Sensitivity to the initial conditions can be checked using Theorem 31 and, in order to increase the level of security, it is important that the algorithm provided by Theorem 31 is inserted in the scheme just before the step 2. with the additional requirement that the step 1. is repeated if the HOCA individuated in the step itself is not sensitive.

As an illustrative case, consider the (3,4)-threshold secret sharing scheme for texts of 64 bits dealt with in [8]. According to our notation, the matrix presentation $\mathcal{L}$ of the HOCA $\mathcal{H}$ built by the method is an LCA with local rule defined by the matrices

$$\boldsymbol{M}_{-1} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \qquad \boldsymbol{M}_0 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \qquad \boldsymbol{M}_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

The matrix in Frobenius normal form associated with $\mathcal{L}$ is then

$$\boldsymbol{M}(X) = \sum_{i=-1}^{1} \boldsymbol{M}_i X^i = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & X^{-1}+X & X^{-1}+1+X \end{bmatrix}$$

Since the determinant of $M(X)$ is the polynomial $\mathbb{m}_0(X) = 1$, by Proposition 9, $\mathcal{H}$ is reversible. Moreover, by Theorem 31, it is sensitive to the initial conditions. Indeed, there exists at least a sensitive polynomial inside $\mathbb{m}(X)$, namely, for instance, the polynomial $\mathbb{m}_1(X) = X^{-1} + X$ (which is sensitive since $deg^+[\mathbb{m}_1(X)] = 1 > 0$). Remark that if all ω_j provided by the MPT define coefficients a_i^j with $a_{-1}^j = a_1^j = 0$ and $a_0^j = 0$, then $\mathcal{H}$ is not sensitive. When this happens, the scheme is vulnerable. Luckily, the undesirable situation is avoided by the insertion of the algorithm provided by Theorem 31 in the scheme.

Data encryption. In [6], Chai, Cao, and Zhou proposed a block cypher scheme based on linear HOCA with memory $k = 2$ over $\mathbb{Z}_2$.

The scheme basically consists in taking a plain text and put the first and second half bits in the first and second component, respectively, of the HOCA initial configuration $\boldsymbol{c} = \begin{pmatrix} c^1 \\ c^2 \end{pmatrix}$. Then, the authors propose to compute the next ℓ elements (with $\ell > 2$) of the dynamical evolution of $\mathcal{H}$ starting from $\boldsymbol{c}$, where $\mathcal{H}$ is a HOCA of radius 1 built on the basis of a LCA $\langle \mathbb{Z}_2, 1, f \rangle$. Precisely, the local rule $h : \mathbb{Z}_2^6 \to \mathbb{Z}_2$ of $\mathcal{H}$ is defined as follows

$$\forall \boldsymbol{x} = \begin{pmatrix} x_{-1}^1 & x_0^1 & x_1^1 \\ x_{-1}^2 & x_0^2 & x_1^2 \end{pmatrix} \in \mathbb{Z}_2^6, \quad h(\boldsymbol{x}) = \left[\sum_{j=1}^{2} \sum_{i=-1}^{1} a_i^j x_i^j \right]_2 .$$

where $a_{-1}^1 = a_1^1 = 0$, $a_0^1 = 1$, and a_i^2 are the coefficients of the local rule f of the LCA to be chosen. The ciphered text is nothing but the content of $H^\ell(\boldsymbol{c})$. According to Equations (1) and (2), the local rule of the matrix presentation $\mathcal{L}$ of $\mathcal{H}$ is defined by the following matrices

$$\boldsymbol{M}_{-1} = \begin{bmatrix} 0 & 0 \\ 0 & a_{-1}^2 \end{bmatrix} \qquad \boldsymbol{M}_0 = \begin{bmatrix} 0 & 1 \\ 1 & a_0^2 \end{bmatrix} \qquad \boldsymbol{M}_1 = \begin{bmatrix} 0 & 0 \\ 0 & a_1^2 \end{bmatrix}$$

Therefore, the matrix in Frobenius normal form associated with $\mathcal{L}$ is

$$\boldsymbol{M}(X) = \sum_{i=-1}^{1} \boldsymbol{M}_i X^i = \begin{bmatrix} 0 & 1 \\ 1 & a_{-1}^2 X^{-1} + a_0^2 + a_1^2 X \end{bmatrix}$$

Since the determinant of $M(X)$ is just the polynomial $\mathbb{m}_0(X) = 1$, by Proposition 9, $\mathcal{H}$ is reversible, that is an important requirement to be satisfied for the functioning of the cypher scheme. As for the secret sharing schemes previously illustrated, the way reversibility is checked suggests that coefficients a_{-1}^1, a_0^1, a_1^1 could be determined by a (random) value $s \in [-1, 1]$ defining them, instead of being fixed. Indeed, the reversibility of the resulting HOCA would be preserved and this modification increases the security level of the scheme. Clearly, the same still holds when LCA $\langle \mathbb{Z}_m, r, f \rangle$ (with $r > 1$ and $m > 2$) are considered for building the HOCA $\mathcal{H}$.

In order to analyse their method, the authors experimentally study the avalanche effect of one bit change in the plain text *w.r.t.* the ciphered text. Sensitivity to the initial conditions is a necessary condition in order that $\mathcal{H}$ exhibits such an effect. Thus, also the cypher scheme can be equipped by the algorithm provided by Theorem 31 in order to make attacks much harder. The application of such an algorithm over the method is that sensitivity is exhibited if and only if either $deg^+[\mathbb{m}_1(X)] = deg^+[a_{-1}^2 X^{-1} + a_0^2 + a_1^2 X] = a_1^2 > 0$ or $deg^-[\mathbb{m}_1(X)] = deg^-[a_{-1}^2 X^{-1} + a_0^2 + a_1^2 X] = a_{-1}^2 > 0$. Therefore, the only possible candidates for LCA to be chosen for building sensitive $\mathcal{H}$ are those with Wolfram number 90, 102 and 150, as experimentally observed by the authors.

6. Perspectives

In this paper we have studied equicontinuity and sensitivity to the initial conditions for linear HOCA over $\mathbb{Z}_m$ of memory size n, providing decidable characterizations for these properties. Such characterizations extend the ones shown in [28] for linear cellular automata (LCA) over $\mathbb{Z}_m^n$ in the case $n = 1$ and, as illustrated in Introduction and Section 5, have an impact in many applications, for instance those concerning the design of secret sharing schemes [8], data encryption [6], and data compression and image processing [21], where linear HOCA are involved and a chaotic or strongly stable behaviour is required.

We also showed that linear HOCA over $\mathbb{Z}_m$ of memory size n form a class that is indistinguishable from a subclass of LCA (namely, the subclass of Frobenius LCA) over $\mathbb{Z}_m^n$. This enables to decide injectivity and surjectivity for linear HOCA over $\mathbb{Z}_m$ of memory size n by means of the decidable characterizations of injectivity and surjectivity provided in [2] and [25] for LCA over $\mathbb{Z}_m^n$. A natural and pretty interesting research direction consists of investigating other chaotic properties as transitivity and expansivity for linear HOCA. Possible characterizations of the latter properties

would be useful in cryptographic applications since they would allow to design schemes that make attacks even more difficult. Furthermore, all the mentioned dynamical properties, including sensitivity and equicontinuity, could be studied for the whole class of LCA over $\mathbb{Z}_m^n$ (more difficult task). Besides leading to a generalization of the shown results, such investigations would indeed help to understand also the behavior of other models used in applications, as for instance linear *non-uniform cellular automata* over $\mathbb{Z}_m$. Let us explain precisely the meaning of such a sentence.

First of all, recall that a *non-uniform cellular automaton* (ν-CA) over the alphabet S is a structure $\langle S, \{f_j, r_j\}_{j\in\mathbb{Z}}\rangle$ defined by a family of local rules $f_j : S^{2r_j+1} \to S$, each of them of its own radius r_j. Similarly to CA, the global rule of a ν-CA is the map $F_\nu : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ defined as

$$\forall c \in S^{\mathbb{Z}}, \quad \forall i \in \mathbb{Z}, \qquad F_\nu(c)_i = f_i(c_{i-r}, \dots c_{i+r}) \ ,$$

and, so, $(S^{\mathbb{Z}}, F_\nu)$ is the DDS associated with a given ν-CA. A ν-CA over the alphabet $S = \mathbb{Z}_m$ is linear if all its local rules are linear. We are going to focus our attention on an interesting class of (linear) ν-CA, namely, the (linear) periodic ones. A *periodic ν-CA ($\pi\nu$-CA)* is a ν-CA satisfying the following condition: there exists an integer $n > 0$ (called the structural period) such that $f_j = f_{j \bmod n}$ for any $j \in \mathbb{Z}$. It is clear that a $\pi\nu$-CA of structural period n is defined by the local rules $f_0, \dots, f_{n-1}$, which, without loss of generality, can be all assumed to have a same radius r. The following result holds.

Proposition 34. *Every linear $\pi\nu$-CA over $\mathbb{Z}_m$ of structural period n is topologically conjugated to a LCA over $\mathbb{Z}_m^n$, and vice versa. In other terms, up to a homeomorphism, the class of linear $\pi\nu$-CA over $\mathbb{Z}_m$ of structural period n is nothing but the class of LCA over $\mathbb{Z}_m^n$.*

Proof. Consider any linear $\pi\nu$-CA of structural period n, radius r, and local rules $f_0, \dots, f_{n-1}$, where, for each $j = 0, \dots, n-1$, the rule f_j is defined on the basis of coefficients $a_{j,i} \in \mathbb{Z}_m$ $(i = -r, \dots, r)$ as follows

$$\forall (x_{-r}, \dots, x_r) \in \mathbb{Z}_m^{2r+1}, \quad f_j(x_{-r}, \dots, x_r) = \left[\sum_{i=-r}^{r} a_{j,i} x_i \right]_m \ .$$

Set $s = -\lceil r/n \rceil$ and let $\left((\mathbb{Z}_m^n)^{\mathbb{Z}}, F\right)$ be the LCA over $\mathbb{Z}_m^n$ such that its local rule is defined by the matrices $\boldsymbol{M}_{-s}, \dots, \boldsymbol{M}_0, \dots, \boldsymbol{M}_s \in Mat(n, \mathbb{Z}_m)$, where, for each $\ell \in [-s, s]$,

$$\boldsymbol{M}_\ell = \begin{pmatrix} a_{0,\ell n} & a_{0,\ell n+1} & \cdots & a_{0,\ell n+n-1} \\ a_{1,\ell n-1} & a_{1,\ell n} & \cdots & a_{1,\ell n+n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,\ell n-n+1} & a_{n-1,\ell n-n+2} & \cdots & a_{n-1,\ell n} \end{pmatrix} \ ,$$

with $a_{j,i} = 0$ whenever $i \notin [-r, r]$. One gets that $\varphi \circ F_\nu = F \circ \varphi$, where $\varphi : \mathbb{Z}_m^{\mathbb{Z}} \to \left(\mathbb{Z}_m^n\right)^{\mathbb{Z}}$ is the homeomorphism associating any configuration $c \in \mathbb{Z}_m^{\mathbb{Z}}$ with the element $\varphi(c) \in \left(\mathbb{Z}_m^n\right)^{\mathbb{Z}}$ such that for any $i \in \mathbb{Z}$ and for each $j = 0, \dots, n-1$, the $(j+1)$–th component of the vector $\psi(c)_i \in \mathbb{Z}_m^n$ is $\psi(c)_i^{j+1} = c_{in+j}$. Then, the linear $\pi\nu$-CA F_ν is topologically conjugated to the LCA F. Similarly, one proves that every LCA over $\mathbb{Z}_m^\pi$ is topologically conjugated to a linear $\pi\nu$-CA over $\mathbb{Z}_m$ of structural period π. □

Remark that very little is known for linear ν-CA, therefore Proposition 34 further motivates the study of LCA over $\mathbb{Z}_m^n$ since it makes a deep connection between LCA and $\pi\nu$-CA and this last class of CA is used in many applications. For instance, they may be used as subband encoders for compressing signals [25] and images [32].

Acknowledgements. E. Formenti acknowledges the partial support from the project PACA APEX FRI. A. Dennunzio, L. Manzoni, and A. E. Porreca were partially supported by Fondo d'Ateneo (FA) "Sistemi Complessi e Incerti: teoria ed applicazioni" (2016) and "Complessità computazionale e applicazioni crittografiche di modelli di calcolo bioispirati" (2015) of Università degli Studi di Milano–Bicocca.

References

[1] Luigi Acerbi, Alberto Dennunzio, and Enrico Formenti. Shifting and lifting of cellular automata. In S. Barry Cooper, Benedikt Löwe, and Andrea Sorbi, editors, *Computation and Logic in the Real World, Third Conference on Computability in Europe, CiE 2007, Siena, Italy, June 18-23, 2007, Proceedings*, volume 4497 of *Lecture Notes in Computer Science*, pages 1–10. Springer, 2007.

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

[3] 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.

[4] 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.

[5] Julien Cervelle and Grégory Lafitte. On shift-invariant maximal filters and hormonal cellular automata. In *LICS: Logic in Computer Science*, pages 1–10, Reykjavik, Iceland, June 2017.

[6] 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.

[7] Michele d'Amico, Giovanni Manzini, and Luciano Margara. On computing the entropy of cellular automata. *Theoretical Computer Science*, 290(3):1629–1646, 2003.

[8] A. Martín del Rey, J. Pereira Mateus, and G. 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, and Luca Manzoni. Computing issues of asynchronous CA. *Fundamenta Informaticae*, 120(2):165–180, 2012.

[12] Alberto Dennunzio, Enrico Formenti, and Luca Manzoni. Reaction systems and extremal combinatorics properties. *Theoretical Computer Science*, 598:138–149, 2015.

[13] Alberto Dennunzio, Enrico Formenti, Luca Manzoni, and Giancarlo Mauri. m-asynchronous cellular automata: from fairness to quasi-fairness. *Natural Computing*, 12(4):561–572, 2013.

[14] 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.

[15] Alberto Dennunzio, Enrico Formenti, Luca Manzoni, and Antonio E. Porreca. Ancestors, descendants, and gardens of eden in reaction systems. *Theoretical Computer Science*, 608:16–26, 2015.

[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] Alberto Dennunzio, Pierre Guillon, and Benoît Masson. Stable dynamics of sand automata. In Giorgio Ausiello, Juhani Karhumäki, Giancarlo Mauri, and C.-H. 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.

[21] Jing Gu and Dianxun Shuai. The faster higher-order cellular automaton for hyper-parallel undistorted data compression. *Journal of Computer Science and Technology*, 15(2):126, Mar 2000.

[22] Gustav Arnold Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Mathematical Systems Theory*, 3:320–375, 1969.

[23] T.E. Ingerson and R.L. Buvel. Structure in asynchronous cellular automata. *Physica D: Nonlinear Phenomena*, 10(1):59 – 68, 1984.

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

[25] Jarkko Kari. Linear cellular automata with multiple state variables. In H. reichel and Sophie Tison, editors, *STACS 2000*, volume 1770 of *LNCS*, pages 110–121. Springer-Verlag, 2000.

[26] C. Knudsen. Chaos without nonperiodicity. *American Mathematical Monthly*, 101:563–565, 1994.

[27] P. Kůrka. Languages, equicontinuity and attractors in cellular automata. *Ergodic Theory & Dynamical Systems*, 17:417–433, 1997.

[28] 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.

[29] 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.

[30] Luca Mariot, Alberto Leporati, Alberto Dennunzio, and Enrico Formenti. Computing the periods of preimages in surjective cellular automata. *Natural Computing*, 16(3):367–381, 2017.

[31] Birgitt Schönfisch and André de Roos. Synchronous and asynchronous updating in cellular automata. *Biosystems*, 51(3):123 – 143, 1999.

[32] Jerome M. Shapiro. Embedded image coding using zerotrees of wavelet coefficients. *IEEE Trans. Signal Processing*, 41(12):3445–3462, 1993.

[33] Tommaso Toffoli. Computation and construction universality. *Journal of Computer and Systems Sciences*, 15:213–231, 1977.