Information Sciences 657 (2024) 119942

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

An efficient algorithm deciding chaos for linear cellular automata over $(\mathbb{Z}/m\mathbb{Z})^n$ with applications to data encryption

Alberto Dennunzio [a,*], Enrico Formenti [b], Luciano Margara [c]

[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 dell'Università 50, Cesena, Italy

ARTICLE INFO

Keywords:
Cellular automata
Linear cellular automata
Chaos
Data encryption

ABSTRACT

We provide an efficient algorithm deciding chaos for linear cellular automata (LCA) over $(\mathbb{Z}/m\mathbb{Z})^n$, a large and important class of cellular automata (CA) which may exhibit many of the complex features typical of general CA and are used in many applications. The efficiency of our algorithm is mainly due to fact that it avoids the computation of the prime factor decomposition of m which is a well-known difficult task. Instead of factoring m we make use of a new and efficient generalized technique for computing the greatest common divisor (gcd) of polynomials with coefficients not belonging to a field, which in itself is an interesting result. We wish also to emphasize that the gcd computations required by our algorithm always involve polynomials of degree at most n.

We also illustrate the impact of our algorithm in real-world applications regarding the growing domain of cryptosystems, the latter being often based on LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ with $n > 1$. As a matter of facts, since cryptosystems have to satisfy the so-called confusion and diffusion properties (which are ensured if the involved LCA is chaotic) our algorithm turns out to be an important tool for building chaotic LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ and, hence, for improving the existing methods based on them.

1. Introduction

This paper is about one-dimensional *linear cellular automata (LCA)* over the alphabet $(\mathbb{Z}/m\mathbb{Z})^n$, i.e., one-dimensional *cellular automata (CA)* with local rule defined by $n \times n$ matrices with elements in $\mathbb{Z}/m\mathbb{Z}$. Despite their simplicity, they are able to exhibit the complex behaviours of general CA. Moreover, they are used in many applications in several scientific domains. We recall that LCA over the alphabet $(\mathbb{Z}/m\mathbb{Z})^n$ with $n = 1$ have been extensively studied. In that case, all the dynamical properties including chaos not only were proved to be decidable but also efficiently computable characterizations was provided for them [13,15].

Although LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ with $n > 1$ are used in many important applications such as data encryption, design of secret sharing schemes, data compression and image processing, there were few results regarding decidable characterizations of the dynamical properties for such LCA. Actually, the setting $n > 1$, which is more expressive and gives rise to much more complex dynamics than $n = 1$ (see, for instance [10]), is more difficult to deal with. The proof techniques from [13,15] used when $n = 1$ for obtaining decidable characterizations of dynamical and ergodic properties could no longer be exploited when $n > 1$ for achieving the same

* Corresponding author.
E-mail addresses: alberto.dennunzio@unimib.it (A. Dennunzio), enrico.formenti@univ-cotedazur.fr (E. Formenti), luciano.margara@unibo.it (L. Margara).

https://doi.org/10.1016/j.ins.2023.119942
Received 21 June 2023; Received in revised form 16 October 2023; Accepted 23 November 2023

Available online 28 November 2023

goal. Only injectivity and surjectivity had been characterized (in terms of decidable conditions on the matrix associated with the LCA [3,14]).

Anyway, in [7] we took an important step forward: we proved that important properties describing CA complex behaviours as chaos, ergodicity, topological transitivity, and topological mixing are decidable, beyond being equivalent, for one-dimensional LCA over $(\mathbb{Z}/m\mathbb{Z})^n$. However, the decision algorithm provided in [7] for one-dimensional LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$, where p is a known prime number and $k > 0$ is a known natural, turns out to have an exponential complexity and the scenario worsens when LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ for any natural $m > 1$ are considered. Indeed, the way of deciding chaos for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ exploits that algorithm once the prime factor decomposition of m is known, while no algorithm has been published yet that can factor any natural in polynomial time.

In this paper we provide an algorithm for deciding chaos for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ without the prime factor decomposition of m is known and without the algorithm decomposes m into prime factors (very recently, in [8], we provided an easy to check characterization of positive expansivity for additive cellular automata over a finite abelian group). First of all, we provide an efficient algorithm for deciding chaos for LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$ based on an idea which is completely different from that of the early algorithm in [7]. Indeed, unlike [7], the characteristic polynomial $\det(tI_n - M(X))$ of the matrix $M(X)$ associated with a LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$ is now considered as Laurent polynomial with coefficients from $(\mathbb{Z}/p^k\mathbb{Z})[t]$ (instead of a classic polynomial in the indeterminate t and, since LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$ are involved, with Laurent polynomials over $(\mathbb{Z}/p^k\mathbb{Z})$ as coefficients). The algorithm is based on the results proved in Theorems 6 and Lemma 7 as a consequence of which chaos turns out to be equivalent to a decidable condition on the degree of the gcd of those polynomial coefficients (elements from $(\mathbb{Z}/p^k\mathbb{Z})[t]$) when their coefficients (elements from $\mathbb{Z}/p^k\mathbb{Z}$) are taken modulo p. In this way, the exponential factor in the complexity of the decision procedure provided in [7] no longer appears.

Then, we exhibit an efficient algorithm for deciding chaos for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ that is based on Theorems 13 and where, by efficiency, we mean that the prime factor decomposition of m is bypassed, while the latter is required in [7]. The procedure has as input the coefficients (elements from $(\mathbb{Z}/m\mathbb{Z})[t]$) of the Laurent polynomial by which the characteristic polynomial of the matrix associated with a given LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ can be rewritten and it aims at testing a condition equivalent to chaos which is essentially the same than the one for LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$, but now, since $(\mathbb{Z}/m\mathbb{Z})$ is not in general a field, an "unconventional gcd" is involved and hence the situation is more complicated. As a matter of fact, the procedure exploits an unconventional use of the Euclidean algorithm for the computation of the gcd of two polynomials from $(\mathbb{Z}/m\mathbb{Z})[t]$, where, by unconventional use, we means that the Euclidean algorithm is used although $\mathbb{Z}/m\mathbb{Z}$ is not a field. Namely, its run proceeds until it encounters a division of two polynomials that can not be performed because the leading coefficient of the divisor is not coprime with m. If such a situation happens, we say that a "crash" occurs and, as a consequence, m is decomposed as a product $m_1 \cdot m_2$ (or as power $m_1^{s_1}$) where m_1 and m_2 are coprime. In this way, a given LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ is decomposed into the product of two LCA too, one over $(\mathbb{Z}/m_1\mathbb{Z})^n$ and the other over $(\mathbb{Z}/m_2\mathbb{Z})^n$ (or, a single LCA over $(\mathbb{Z}/m_1\mathbb{Z})^n$ is determined), and, once the procedure recursively decides chaos for each of the two components (or, for the single LCA over $(\mathbb{Z}/m_1\mathbb{Z})^n$), it is able to decide chaos for the given LCA over $(\mathbb{Z}/m\mathbb{Z})^n$. Otherwise, i.e., if no crash occurs - and this situation defines the basis case of the recursion - the procedure computes an "unconventional gcd" of polynomials from $(\mathbb{Z}/m\mathbb{Z})[t]$ and it decides chaos on the basis of its degree. We stress that the decidable characterisation of chaos for LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ provided in Theorem 6 and ensuring together with Lemma 7 the correctness of the algorithm for LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$ will be essential for proving the correctness of the one for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$.

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

The paper is organized as follows. In Section 2 all the notations and basic definitions used in the paper are introduced. Section 3 recalls the known results and the existing algorithm deciding chaos for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$, while in Sections 4 and 5 we illustrate the efficient algorithms deciding chaos for LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$ and over $(\mathbb{Z}/m\mathbb{Z})^n$, respectively, along with the results regarding their correctness. Since the proof of the correctness of the algorithm for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ is very long, we located it in Section 6. Section 7 illustrates the impact of our results in real-world applications. Finally, the last section contains our conclusions.

2. Basic notions

Throughout this paper $\mathbb{N} = \{0, 1, \dots\}$ is the set of natural numbers.

Let $\mathbb{K}$ be any commutative ring and let $A \in \mathbb{K}^{n\times n}$ be an $n \times n$-matrix over $\mathbb{K}$. We denote by χ_A the characteristic polynomial $\det\left(tI_n - A\right) \in \mathbb{K}[t]$ of A, where I_n always stands for the $n \times n$ identity matrix (over whatever ring we are considering). Furthermore, $\mathbb{K}[X, X^{-1}]$ denotes the set of Laurent polynomials with coefficients in $\mathbb{K}$. In particular, whenever $\mathbb{K} = \mathbb{Z}/m\mathbb{Z}$ for some natural $m > 1$, we will write $\mathbb{L}_m$ instead of $\mathbb{Z}/m\mathbb{Z}[X, X^{-1}]$.

Let $\mathbb{K} = \mathbb{Z}/m\mathbb{Z}$ for some natural $m > 1$ and let q be a natural with $1 < q < m$. If P is any polynomial from $\mathbb{K}[t]$ (resp., a Laurent polynomial from $\mathbb{L}_m$) (resp., a matrix from $(\mathbb{L}_m)^{n\times n}$), $P \bmod q$ denotes the polynomial (resp., the Laurent polynomial) (resp., the matrix) obtained by P by taking all its coefficients modulo q.

In the sequel, for every pair of elements a, b of any commutative ring $\mathbb{K}$, we will write $b \mid a$ to denote that b divides a, i.e., there exists an element c from that ring such that $a = b \cdot c$. As usual, if $\mathbb{K}$ is also an Euclidean domain, gcd stands for greatest common divisor.

Let Q be a finite set (also called *alphabet*). A *CA configuration* (or, briefly, a *configuration*) is any function from $\mathbb{Z}$ to Q. Given a configuration $c \in Q^{\mathbb{Z}}$ and any integer $i \in \mathbb{Z}$, the value of c in position i is denoted by c_i. The set $Q^{\mathbb{Z}}$, called *configuration space*, is as usual equipped with the standard Tychonoff distance d. Whenever the term *linear* is involved the alphabet Q is $\mathbb{K}^n$, where $\mathbb{K} = \mathbb{Z}/m\mathbb{Z}$ for some natural $m > 1$. Clearly, in that case both $\mathbb{K}^n$ and $(\mathbb{K}^n)^{\mathbb{Z}}$ become $\mathbb{K}$-modules in the obvious (i.e., entrywise) way.

A *one-dimensional CA* (or, briefly, a *CA*) over Q is a pair $(Q^{\mathbb{Z}}, \mathcal{F})$, where $\mathcal{F} : Q^{\mathbb{Z}} \to Q^{\mathbb{Z}}$ is the uniformly continuous transformation (called *global rule*) defined as $\forall c \in Q^{\mathbb{Z}}, \forall i \in \mathbb{Z}, \mathcal{F}(c)_i = f(c_{i-r}, \dots, c_{i+r})$,for some fixed natural number $r \in \mathbb{N}$ (called *radius*) and some fixed function $f : Q^{2r+1} \to Q$ (called *local rule* of radius r). *Elementary CA (ECA)* are those CA defined by elementary local rules, i.e., the ones where $Q = \{0, 1\}$ and $r = 1$. According to [16], each elementary rule, or ECA, is associated with a natural number from the set $\{0, \dots, 255\}$. In the sequel, when no misunderstanding is possible, we will sometimes identify any CA with its global rule.

We recall that a CA $(Q^{\mathbb{Z}}, \mathcal{F})$ is *topologically transitive* if for any pair of nonempty open subset $U, V \subseteq Q^{\mathbb{Z}}$ there exists a natural $h > 0$ such that $\mathcal{F}^h(U) \cap V \neq \emptyset$, while it has *dense periodic orbits* if the set of its periodic points is dense in $Q^{\mathbb{Z}}$, where a periodic point for $\mathcal{F}$ is any configuration $c \in Q^{\mathbb{Z}}$ such that $\mathcal{F}^h(c) = c$ for some natural $h > 0$. Surjectivity of the global rule is a necessary condition for both topological transitivity and denseness of periodic orbits. A CA is said to be *chaotic* if it is topologically transitive and, at the same time, it has dense periodic orbits. We also recall that a CA $(Q^{\mathbb{Z}}, \mathcal{F})$ is *ergodic* with respect to the normalized Haar measure $\mu : \mathcal{M} \to [0, 1]$ if for every set $E \in \mathcal{M}$ it holds that $\left(E = \mathcal{F}^{-1}(E)\right) \Rightarrow (\mu(E) = 0 \text{ or } \mu(E) = 1)$, where $\mathcal{M}$ is the usual collection of measurable sets of $Q^{\mathbb{Z}}$.

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

A local rule $f : (\mathbb{K}^n)^{2r+1} \to \mathbb{K}^n$ of radius r is said to be *linear* if it is defined by $2r + 1$ matrices $A_{-r}, \dots, A_r \in \mathbb{K}^{n \times n}$ as follows: $\forall (x_{-r}, \dots, x_r) \in (\mathbb{K}^n)^{2r+1}, f(x_{-r}, \dots, x_r) = \sum_{i=-r}^{r} A_i \cdot x_i$. A one-dimensional *linear CA (LCA)* over $\mathbb{K}^n$ is a CA $\mathcal{F}$ based on a linear local rule. The Laurent polynomial (or matrix)

$$M(X) = \sum_{i=-r}^{r} A_i X^{-i} \in \mathbb{K}^{n \times n}[X, X^{-1}] \cong (\mathbb{L}_m)^{n \times n}$$

is said to be the *matrix associated with* $\mathcal{F}$.

We recall that the dynamical behaviour of LCA over $\mathbb{K}^n$ when $n = 1$ has been successfully investigated by means of $M(X)$ (see [13,15]). In that case, all the dynamical and ergodic properties, including those we will deal with in this paper, have been characterized and, in particular, they turn out to be decidable. For this reason, in the sequel we will deal with naturals $n > 1$ as far as new results are concerned.

3. Known results and the existing algorithm deciding chaos for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$

We start to recall some useful results. The first one concerns surjectivity.

Theorem 1 *([13,14,3]). Let $\mathcal{F}$ be a LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ with associated matrix $M(X) \in (\mathbb{L}_m)^{n \times n}$, where $n > 0$. The following facts hold:*

(i) if $n = 1$ then $\mathcal{F}$ is surjective if and only if the gcd *among m and the 1×1 matrices defining its local rule is equal to 1;*
(ii) if $n > 1$ then $\mathcal{F}$ is surjective if and only if $\det(M(X))$ *is the 1×1 matrix associated with a surjective LCA over $\mathbb{Z}/m\mathbb{Z}$.*

Remark 2. Whenever $m = p^k$ for some prime p and some natural $k > 0$, for every matrix $M(X) \in (\mathbb{L}_m)^{n \times n}$ it holds that $\det(M(X))$ is the matrix associated with a surjective LCA over $\mathbb{Z}/m\mathbb{Z}$ if and only if $p \nmid \det(M(X))$, i.e., if and only if $\det(M(X) \bmod p) \neq 0$.

The following result is an immediate consequence of the generalisation of [4, Lemma 3.2] to $(\mathbb{Z}/m\mathbb{Z})^n$.

Lemma 3. *Let $\mathcal{F}$ be a LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ with associated matrix $M(X) \in (\mathbb{L}_m)^{n \times n}$. Let $m_1, m_2 \in \mathbb{Z}/m\mathbb{Z}$ be such that $m = m_1 \cdot m_2$ and* $\gcd(m_1, m_2) = 1$. *The LCA $\mathcal{F}$ is topologically transitive if and only if both the LCA over $(\mathbb{Z}/m_1\mathbb{Z})^n$ and $(\mathbb{Z}/m_2\mathbb{Z})^n$ having associated matrices $M(X) \bmod m_1 \in (\mathbb{L}_{m_1})^{n \times n}$ and $M(X) \bmod m_2 \in (\mathbb{L}_{m_2})^{n \times n}$, respectively, are too.*

In [9] we showed the equivalence of chaos, topological transitivity, ergodicity, and other mixing and ergodic properties for a class of CA wider than LCA over $(\mathbb{Z}/m\mathbb{Z})^n$, namely, that of Additive CA over a finite abelian group. Furthermore, the decidability of those properties for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ was proved in [7] (while in [10] we showed how all the decidability results are transferred from LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ to Additive CA over a finite abelian group). Precisely, as far as LCA are concerned, the following holds

Theorem 4 *([9,7]). Let $\mathcal{F}$ be a LCA over $(\mathbb{Z}/m\mathbb{Z})^n$. The following statement are equivalent:*

(i) $\mathcal{F}$ is chaotic;
(ii) $\mathcal{F}$ is topologically transitive;

(*iii*) *$\mathcal{F}$ is ergodic;*
(*iv*) *$\mathcal{F}$ is surjective and for every natural $h > 0$ it holds that $\mathcal{F}^h - I$ is surjective (I is the identity map).*

In particular, whenever $\mathcal{F}$ is a LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$ for some prime p and some natural $k > 0$, they are equivalent to the following condition

$$\det(M(X) \bmod p) \neq 0 \quad \textit{and} \quad \gcd(\chi_{M(X) \bmod p}(t), t^{p^h - 1} - 1) = 1 \textit{ for all } h \in \{1, \dots, n\} \ , \tag{1}$$

where $M(X) \in (\mathbb{L}_{p^k})^{n \times n}$ is the matrix associated with $\mathcal{F}$.

We stress that condition (1) is the heart of all the results stated in Theorem 4. Indeed in [7], once proved its equivalence with all the properties mentioned in that theorem, condition (1) allowed us to immediately get the following algorithm deciding chaos for LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$ and with input $(M(X), p)$, where $M(X) \in (\mathbb{L}_{p^k})^{n \times n}$ is the matrix associated with the LCA under investigation[1]:

EXISTING($M(X), p$)

```
1  χ_{M(X) mod p}(t) = characteristic polynomial of M(X) mod p
2  if det(M(X) mod p) ≠ 0
3       for i = 1 to M(X).size // M(X).size is the number n of rows and columns of M(X)
4            if gcd(χ_{M(X) mod p}(t), t^{p^i − 1} − 1) ≠ 1
5                 return false
6       return true
7  else
8       return false
```

Moreover, condition (1), or, in other terms, Algorithm EXISTING, allowed us in [7] to prove the decidability of chaos and all the equivalent properties for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ also when m is any natural greater than 1 by exploiting the explicit prime factor decomposition of m itself. As a matter of fact, if the prime factor decomposition $p_1^{k_1} \cdots p_l^{k_l}$ of m is known, any LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ with associated matrix $M(X) \in (\mathbb{L}_m)^{n \times n}$ is chaotic if and only if every LCA over $(\mathbb{Z}/p_j^{k_j}\mathbb{Z})^n$ with associated matrix $M(X) \bmod p_j^{k_j} \in (\mathbb{L}_{p_j^{k_j}})^{n \times n}$ is chaotic, or, equivalently, every call EXISTING($M(X) \bmod p_j^{k_j}, p_j$) outputs true.

Although this way of proceeding is enough to prove that chaos is decidable for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$, it is far from being efficient, first of all because the prime decomposition of m is required. Moreover, since computing the gcd of two polynomials of degree at most d costs $O(d^2)$ operations using classical methods, or $O(d \cdot \log^2(d) \cdot \log(\log d))$ operations using fast methods, Algorithm EXISTING on its own has an exponential computational complexity in the worst case since its run may compute the gcd of two polynomials one of them having degree $p^n - 1$.

4. An efficient algorithm deciding chaos for LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$

In this section we provide an efficient algorithm that decides chaos for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ when m is explicitly known to be the prime power p^k, for some known prime $p > 1$ and natural $k > 0$. Since by Theorem 4 chaos is equivalent to topological transitivity for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$, the algorithm along with all the results we are going to provide in the sequel will refer to topological transitivity.

First of all, consider the following algorithm with input any matrix $M(X) \in \mathbb{L}_p^{n \times n}$, for an arbitrary natural $n > 1$ and an arbitrary prime p, and involving $\xi(X, X^{-1})$, i.e., the characteristic polynomial $\chi_{M(X)}(t)$ of $M(X)$ expressed as polynomial in the variables X and X^{-1} and, hence, with coefficients that are elements from $(\mathbb{Z}/p\mathbb{Z})[t]$.

DECIDE-P-TT($M(X)$)

```
1  χ_{M(X)}(t) = characteristic polynomial of M(X)
2  ξ(X, X^{-1}) = χ_{M(X)}(t) expressed as polynomial in the variables X and X^{-1}
3  γ(t) = gcd of the coefficients of ξ(X, X^{-1})
4  if deg(γ(t)) < 1
5       return true
6  else
7       return false
```

We are going to show that DECIDE-P-TT (*i*) outputs true when it is invoked with input $M(X)$ iff the one-dimensional LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ having $M(X)$ as associated matrix is topologically transitive; (*ii*) it can be exploited for deciding topological transitivity for LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$; (*iii*) it is more efficient than EXISTING, avoiding the exponential factor $p^n - 1$ in the computational complexity of EXISTING.

Before proceeding, let us illustrate by an example how DECIDE-P-TT works in two distinct situations.

[1] Here we report the correct version of the algorithm deciding chaos for LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$, i.e., without the typos present in [7].

Example 5. Let $p = 5$ and $n = 2$. Consider the LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ with associated matrix

$$M(X) = \begin{bmatrix} 0 & 1 \\ 1+X & X \end{bmatrix} .$$

We get $\chi_{M(X)}(t) = t^2 + 4Xt + 4X + 4$, $\xi(X, X^{-1}) = (4t+4)X + t^2 + 4$, and $\gamma(t) = \gcd(4t+4, t^2+4) = 1+t$. Hence, DECIDE-P-TT($M(X)$) outputs false, while it outputs true if, for instance,

$$M(X) = \begin{bmatrix} 0 & 1 \\ X & X \end{bmatrix} ,$$

a situation leading to $\chi_{M(X)}(t) = t^2 + 4Xt + 4X$, $\xi(X, X^{-1}) = (4t+4)X + t^2$, and, $\gamma(t) = \gcd(4t+4, t^2) = 1$.

We now prove that DECIDE-P-TT is an algorithm that actually decides topological transitivity for LCA over $(\mathbb{Z}/p\mathbb{Z})^n$.

Theorem 6. *Algorithm* DECIDE-P-TT *decides topological transitivity, i.e., chaos, for LCA over* $(\mathbb{Z}/p\mathbb{Z})^n$. *In other terms, the following condition is a decidable characterisation of topological transitivity, i.e., chaos, for LCA over* $(\mathbb{Z}/p\mathbb{Z})^n$*:*

$$\deg(\gamma(t)) < 1 ,$$

where $\gamma(t)$ *is the* gcd *of the coefficients of* $\xi(X, X^{-1})$*, the latter being the polynomial characteristic* $\chi_{M(X)}(t)$ *expressed as polynomial in the variables* X *and* X^{-1} *of the matrix* $M(X)$ *associated with any LCA over* $(\mathbb{Z}/p\mathbb{Z})^n$*, for any prime* p *and any natural* $n > 1$.

Proof. Let $p > 1$, $n > 1$, and $M(X) \in (\mathbb{L}_p)^{n\times n}$ be any prime, natural, and matrix, respectively. Let $\chi_{M(X)}(t)$, $\xi(X, X^{-1})$, and $\gamma(t)$ be as in the statement and in Algorithm DECIDE-P-TT. Let $\mathcal{F}$ be the one-dimensional LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ with associated matrix $M(X)$. We are going to show that $\mathcal{F}$ is topologically transitive if and only if DECIDE-P-TT outputs true, or, equivalently, if and only if $\deg(\gamma(t)) < 1$.

We start to prove that if DECIDE-P-TT outputs false then $\mathcal{F}$ is not topologically transitive. Then, let us suppose that $\deg(\gamma(t)) \geq 1$. Without loss of generality, we can assume that $\gamma(t)$ is monic. Indeed, on the contrary, it can be transformed in a monic polynomial by a multiplicative constant (that exists since $\mathbb{Z}/p\mathbb{Z}$ is a field). Therefore, we can write $\chi_{M(X)}(t) = \xi(X, X^{-1}) = \gamma(t) \cdot \pi(t, X, X^{-1})$, where $\pi(t, X, X^{-1})$ is a suitable polynomial in the variables t, X, X^{-1}. We deal with the following two cases:

i) $t \mid \gamma(t)$. In this case the known term of $\chi_{M(X)}(t)$ is $\det(M(X)) = 0$. By Remark 2, $\mathcal{F}$ is not surjective and hence it is not even topologically transitive.

ii) $t \nmid \gamma(t)$. Let $\eta(t) \neq t$ be an irreducible monic factor of $\gamma(t)$ and let d be its degree ($0 < d \leq n$). An algebra well-known result ensures that $\eta(t)$ is also a factor of $t^{p^d-1} - 1$. By condition (1) from Theorem 4, it follows that $\mathcal{F}$ is not topologically transitive.

We now prove that if DECIDE-P-TT outputs true then $\mathcal{F}$ is topologically transitive. Assume that $\mathcal{F}$ is not topologically transitive. If, in addition, $\mathcal{F}$ is not surjective, by Remark 2 it holds that $\det(M(X)) = 0$ and, hence, $t \mid \chi_{M(X)}(t)$, this latter implying that $t \mid \gamma(t)$, too. Therefore, $\deg(\gamma(t)) \geq 1$. If, instead, $\mathcal{F}$ is surjective, by condition (1) from Theorem 4, there is a natural $h \in \{1, \ldots, n\}$ such that $\gcd(\chi_{M(X)}(t), t^{p^h-1} - 1) \neq 1$. Since $t^{p^h-1} - 1$ can be written as product of all the monic irreducible polynomials (different from t) of degree $h' \leq n$ with $h' \mid h$, there exists a polynomial $\eta(t)$ of degree h'' with $0 < h'' \leq n$ and such that $\eta(t) \mid \chi_{M(X)}(t)$. Thus, we get again $\deg(\gamma(t)) \geq 1$. Therefore, in both cases DECIDE-P-TT outputs false and this concludes the proof. □

We now show that DECIDE-P-TT can be employed to decide chaos also for LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$. First of all, let us prove the following result that will be useful in the sequel, too.

Lemma 7. *Let* $m > 1$, $s > 1$, *and* $n > 1$ *be any three naturals and let* $M(X) \in (\mathbb{L}_{m^s})^{n\times n}$ *be any matrix. The LCA* $\mathcal{F}$ *over* $(\mathbb{Z}/m^s\mathbb{Z})^n$ *with associated matrix* $M(X)$ *is topologically transitive if and only if the LCA over* $(\mathbb{Z}/m\mathbb{Z})^n$ *having* $(M(x) \bmod m)) \in (\mathbb{L}_m)^{n\times n}$ *as associated matrix is too.*

Proof. By item (iv) of Theorem 4 and item (ii) of Theorem 1, $\mathcal{F}$ is topologically transitive if and only if $\det(M(X))$ and $\det(M(X)^h - I_n)$ for every natural $h \geq 1$ are all 1×1 matrices associated with surjective LCA over $\mathbb{Z}/m^s\mathbb{Z}$. Each of them is surjective if and only if the LCA over $\mathbb{Z}/m\mathbb{Z}$ obtained by it taking the coefficients of its local rule modulo m is surjective. Indeed, by item (i) of Theorem 1, any LCA over $\mathbb{Z}/m^s\mathbb{Z}$ is surjective if and only if the gcd among m^s and the coefficients of its local rules is equal to 1, a condition which holds if and only if the gcd among m and those coefficients taken modulo m is equal to 1, since the prime factors of the coefficients keep unchanged (but with possible distinct powers) when the modulo operation is performed. Therefore, $\mathcal{F}$ is topologically transitive if and only if $\det(M(X) \bmod m)$ and $\det((M(X) \bmod m)^h - I_n)$ for every natural $h \geq 1$ are all 1×1 matrices associated with surjective LCA over $\mathbb{Z}/m\mathbb{Z}$, i.e., again by item (iv) of Theorem 4 and item (ii) of Theorem 1, if and only if the LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ having $(M(x) \bmod m) \in (\mathbb{L}_m)^{n\times n}$ as associated matrix is topologically transitive. □

Corollary 8. *Algorithm* DECIDE-P-TT *decides chaos for LCA over* $(\mathbb{Z}/p^k\mathbb{Z})^n$. *Namely, for any LCA* $\mathcal{F}$ *over* $(\mathbb{Z}/p^k\mathbb{Z})^n$ *with* p *prime and* n, k *naturals such that* $n > 1$ *and* $k > 1$, DECIDE-P-TT *with input* $(M(X) \bmod p)$ *outputs true if and only if* $\mathcal{F}$ *is chaotic, where* $M(X) \in (\mathbb{L}_{p^k})^{n\times n}$ *is the matrix associated with* $\mathcal{F}$.

Proof. By Theorem 6 and Lemma 7, DECIDE-P-TT with input $(M(X) \bmod p)$ outputs true if and only if the LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$ having $M(X) \in (\mathbb{L}_{p^k})^{n\times n}$ as associated matrix is topologically transitive. □

Regarding the computational complexity of DECIDE-P-TT, now the gcd computation always involves polynomials of degree at most n. Therefore, the exponential factor $p^n - 1$ inside the complexity of EXISTING is avoided.

5. An efficient algorithm deciding chaos for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$

We are now going to provide an efficient algorithm that decides topological transitivity, i.e., chaos, for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ when m is any natural with $m > 1$ and nothing is known about the prime factor decomposition of m. We anticipate that the results of Section 4, especially the decidable characterisation of chaos for LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ provided in Theorem 6, will be essential for proving the correctness of the algorithm. Moreover, a crucial point of our procedure is that it exploits the Euclidean algorithm for the computation of a gcd of two polynomials in an unconventional way, i.e., outside of the standard settings, namely, in a situation where the involved polynomials belong to $\mathbb{Z}/m\mathbb{Z}[t]$ without $\mathbb{Z}/m\mathbb{Z}$ being necessarily a field.

So, we start by explaining the unconventional way in which the Euclidean algorithm is used. Consider two polynomials from $\mathbb{Z}/m\mathbb{Z}[t]$ and with leading coefficients that are both coprime with m. Although $\mathbb{Z}/m\mathbb{Z}$ is not in general a field, let us run the Euclidean algorithm with input those two polynomials until its execution possibly encounters a division of two polynomials that can not be performed because the leading coefficient of the divisor is not coprime with m. We stress that, if such a situation does not happens, i.e., the leading coefficient of the divisor is coprime with m, every division can be performed, allowing the run of the Euclidean algorithm to go on. All this leads us to introduce the following notion.

Definition 9 *(Crash).* Let $\pi(t), \pi'(t) \in \mathbb{Z}/m\mathbb{Z}[t]$ be two polynomial with leading coefficients that are both coprime with m. The run of the Euclidean algorithm with input $(\pi(t), \pi'(t))$ has a *crash*, and in that case it halts without reaching as final reminder a null polynomial, if the non null polynomial computed as reminder at a certain iteration has a leading coefficient that is not coprime with m.

When used in the above illustrated unconventional way, the Euclidean algorithm has the following property.

Proposition 10. *Let* $\pi(t), \pi'(t) \in \mathbb{Z}/m\mathbb{Z}[t]$ *be two polynomial with leading coefficients that are both coprime with* m. *Regarding the Euclidean algorithm executed on input* $(\pi(t), \pi'(t))$, *one of the following two mutually exclusive facts happens:*

(1) *it has a crash;*
(2) *it reaches a null final reminder and it outputs the last non null reminder which is a polynomial* $\pi_E(t) \in \mathbb{Z}/m\mathbb{Z}[t]$ *with leading coefficient that is coprime with* m; *furthermore, if* $\delta(t) \in \mathbb{Z}/m\mathbb{Z}[t]$ *is any polynomial such that* $\delta(t) \mid \pi(t)$ *and* $\delta(t) \mid \pi'(t)$ *then* $\delta(t) \mid \pi_E(t)$.

Proof. The dichotomy between *(1)* and *(2)* directly follows from the notion of crash. We only need to prove what is further stated in *(2)*. So, assume that *(2)* happens and let $\delta(t) \in \mathbb{Z}/m\mathbb{Z}[t]$ be any polynomial such that $\delta(t) \mid \pi(t)$ and $\delta(t) \mid \pi'(t)$. Then, $\delta(t) \mid \rho_1(t)$ where $\rho_1(t)$ is the reminder computed by the first iteration of the Euclidean algorithm when ran on input $(\pi(t), \pi'(t))$. By repetition, $\delta(t)$ divides the reminder computed by each step, i.e., by each division, executed by Euclidean algorithm. Hence, $\delta(t)$ divides $\pi_E(t)$. □

Remark 11. Although $\mathbb{Z}/m\mathbb{Z}$ is not in general a field, on the basis of item *(2)* of Proposition 10, with an terminological abuse we will say that $\pi_E(t)$ is a gcd of $\pi(t)$ and $\pi'(t)$ when no crash occurs during the run of the Euclidean algorithm on input $(\pi(t), \pi'(t))$.

Notation In the sequel, we will denote by U-GCD$(\pi(t), \pi'(t))$ the unconventional version of the Euclidean algorithm for the computation of a gcd of two given polynomials $\pi(t), \pi'(t) \in \mathbb{Z}/m\mathbb{Z}[t]$ and returning the triple $(crash, g, \gamma(t))$, where $crash$ is true if U-GCD$(\pi(t), \pi'(t))$ has a crash and in that case $g \neq 1$ is the gcd of m and the leading coefficient of the last reminder computed, false, otherwise, and in that case $\gamma(t)$ is a gcd of $\pi(t)$ and $\pi'(t)$.

Consider the following procedures DEC-TT and REDUCE with input parameters $(m, \gamma(t), c, \vec{\kappa}(t))$ and (m, b), respectively, where m is any natural greater than 1 and, regarding the first input,

- $\gamma(t)$ is any polynomial from $\mathbb{Z}/m\mathbb{Z}[t]$;
- $\vec{\kappa}(t) = (\kappa_1(t), \ldots, \kappa_z(t)) \in (\mathbb{Z}/m\mathbb{Z}[t])^z$ is the vector of all the z coefficients of the characteristic polynomial $\xi(X, X^{-1}) = \chi_{M(X)}(t)$ of any matrix $M(X) \in (\mathbb{L}_m)^{n\times n}$ when $\chi_{M(X)}(t)$ is expressed as polynomial in the variables X and X^{-1} and no matter about the order those coefficients appear inside $\vec{\kappa}(t)$;
- c is any natural with $1 \leq c \leq z$,

while, concerning REDUCE,

- $b \in \mathbb{Z}/m\mathbb{Z}$ is any element such that $b > 1$ and there exists $a \in \mathbb{Z}/m\mathbb{Z}$ with $b = \gcd(m, a)$.

DEC-TT$(m, \gamma(t), c, \vec{\kappa}(t))$

```
1  γ^cur(t) = γ(t)
2  for nc = c to κ⃗(t).length − 1
3       (crash, g, γ^next(t)) = U-GCD(γ^cur(t), κ_{nc+1}(t))
4       if crash = true
5            (m_1, m_2) = REDUCE(m, g)
6            if m_2 ≠ 1
7                 return DEC-TT(m_1, γ^cur(t) mod m_1, nc, κ⃗(t) mod m_1) AND DEC-TT(m_2, γ^cur(t) mod m_2, nc, κ⃗(t) mod m_2)
8            else
9                 return DEC-TT(m_1, γ^cur(t) mod m_1, nc, κ⃗(t) mod m_1)
10      else
11           γ^cur(t) = γ^next(t)
12 if deg(γ^cur(t)) < 1
13      return true
14 else
15      return false
```

REDUCE(m, b)

```
1  g = b
2  i = 0
3  while DIVISIBLE(m, g^{i+1})// DIVISIBLE returns true iff the second argument divides the first one
4       i = i + 1
5  if m = = g^i
6       return (g, 1)
7  if GCD(m/g^i, g^i) = = 1// GCD computes the (standard) gcd of two numbers
8       return (m/g^i, g^i)
9  g = GCD(m/g^i, g)
10 goto 2
```

As we will prove later, DEC-TT is just the algorithm that decides if the LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ defined by any matrix $M(X) \in (\mathbb{L}_m)^{n\times n}$ is topologically transitive, and that, to provide the answer, has to be called with arguments $m, \kappa_1(t), 1, \vec{\kappa}(t)$, where $\vec{\kappa}(t)$ is the vector of the coefficients of the characteristic polynomial $\xi(X, X^{-1})$ of $M(X)$, as above explained.

If a crash never occurs, the behaviour of DEC-TT is exactly the same as that of DECIDE-P-TT, as if m was a prime number (even though is not): the gcd of the coefficients of the characteristic polynomial $\xi(X, X^{-1})$ is iteratively computed (lines 2–11 where, by the assumption, the line 11 is executed at every iteration) and, then, once its degree is suitably checked, a true/false answer is returned (lines 12–15) according to Lemma 16 (see next Section).

Otherwise, DEC-TT makes use of the procedure REDUCE that, invoked with arguments m g, where g is the gcd of m and the leading coefficient of the last reminder determined by U-GCD, computes and returns a pair $(m_1, m_2) \in (\mathbb{Z}/m\mathbb{Z})^2$ of coprime numbers such that either $m = m_1 \cdot m_2$ with $m_2 \neq 1$ or $m_2 = 1$ and $m = (m_1)^s$ for some natural $s > 1$. In other words, by means of REDUCE, either m is decomposed into the product of two coprime smaller numbers m_1 and m_2 or it is expressed as a power of some and smaller number m_1. In this way, at lines 6–9, DEC-TT compute the answer in a recursive way by exploiting Lemmata 3 and 7. We emphasize that the third argument of the recursive calls of DEC-TT is the value nc of the current iteration and, correspondingly, in the second argument $\gamma^{curr}(t)$ appears, i.e., the gcd of $\kappa_1(t), \ldots, \kappa_{nc}(t)$. Indeed, to compute the gcd of those polynomials (now taken modulo m_1 or m_2), the run of each recursive call of DEC-TT do not need to restart from the beginning, i.e., from the first polynomial, but it can exploits the polynomial $\gamma^{curr}(t)$ that has been already determined by the caller by the execution of line 3 during the previous iteration.

Remark 12. We stress that the overall crashes occurring in the runs of all the recursive calls of DEC-TT executed starting from DEC-TT$(m, \kappa_1(t), 1, \vec{\kappa}(t))$ *provide* a factor decomposition of m as $m = m_1^{s_1} \cdots m_\ell^{s_\ell}$ where the m_e's (with $e \in \{1, \ldots, \ell\}$) are pairwise coprime and they are computed by means of REDUCE. Precisely, the m_e's are the values of the first argument of the calls DEC-TT corresponding to the leaves of the tree of recursive calls having DEC-TT$(m, \kappa_1(t), 1, \vec{\kappa}(t))$ as root.

We also point out that if the m_e's were known before the initial call DEC-TT$(m, \kappa_1(t), 1, \vec{\kappa}(t))$, during the run of every hypothetical call DEC-TT$(m_e, \kappa_1(t), 1, \vec{\kappa}(t))$ no crash would occur and, hence, every DEC-TT$(m_e, \kappa_1(t), 1, \vec{\kappa}(t))$ computes a gcd of $\kappa_1(t) \bmod m_e, \ldots, \kappa_z(t) \bmod m_e$.

Furthermore, we want to highlight that the answer returned by DEC-TT$(m, \kappa_1(t), 1, \vec{\kappa}(t))$ is true if and only if every DEC-TT$(m_e, \kappa_1(t), 1, \vec{\kappa}(t))$ returns true, or, equivalently, if and only if for every $e \in \{1, \dots, \ell\}$ it holds that $h_e < 1$, where h_e is the degree of a gcd of $\kappa_1(t) \bmod m_e, \dots, \kappa_z(t) \bmod m_e$.

Finally, we remark that the set $\{m_1^{s_1}, \dots, m_\ell^{s_\ell}\}$ can be viewed as a partition of $\{p_1^{k_1}, \dots, p_l^{k_l}\}$, where $p_1^{k_1} \cdots p_l^{k_l}$ is the prime factor decomposition of m. Indeed, each $m_e^{s_e}$ is the product of some $p_j^{k_j}$'s and these latter are factors only of that $m_e^{s_e}$.

We now state the main result of the paper, namely, that Algorithm DEC-TT actually decides topological transitivity, i.e., chaos, for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ and it carries out the decision task without decomposing m into prime factors, the latter being the reason why it is efficient. Since the proof of the main result is very long, it is located in the next section.

Theorem 13. *Let $m > 1$ and $n > 0$ be any two naturals.* DEC-TT *decides topological transitivity, i.e., chaos, for one-dimensional LCA over $(\mathbb{Z}/m\mathbb{Z})^n$.*

6. Proof of Theorem 13

We first review some needed concepts and facts regarding the Chinese reminder theorem.

Let $m = p_1^{k_1} \cdots p_l^{k_l}$ be the prime factor decomposition of m. The Chinese reminder theorem ensures that there exists an isomorphism

$$\mathcal{I} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_l^{k_l}\mathbb{Z}$$

known as direct decomposition of $\mathbb{Z}/m\mathbb{Z}$ and defined for any $x \in \mathbb{Z}/m\mathbb{Z}$ as $\mathcal{I}(x) = (x \bmod p_1^{k_1}, \dots, x \bmod p_l^{k_l})$. Moreover, there exist $a_1, \dots, a_l \in \mathbb{Z}/m\mathbb{Z}$ such that for any $(x_1, \dots, x_l) \in \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_l^{k_l}\mathbb{Z}$ it holds that $\mathcal{I}^{-1}(x_1, \dots, x_l) = a_1 x_1 + \dots a_l x_l$. The following Lemma regarding $\mathcal{I}$ will be useful in the sequel.

Lemma 14 *([2]). Let $\mathcal{I} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_l^{k_l}\mathbb{Z}$ be the isomorphism derived from Chinese reminder theorem and let $a_1, \dots, a_l \in \mathbb{Z}/m\mathbb{Z}$ be the coefficients defining $\mathcal{I}^{-1}$. The following facts hold:*

i) for each $i \in \{1, \dots l\}$, $\mathcal{I}(a_i) = (0, \dots, 0, 1, 0, \dots, 0)$, where 1 appears in position i;
ii) $\sum_{i=1}^{l} a_i = 1$;
iii) $a_i^2 = a_i$ for each $i \in \{1, \dots l\}$;
iv) $a_i \cdot a_j = 0$, for each $i, j \in \{1, \dots l\}$ with $i \neq j$.

Lemma 15. *Let $m > 1$ and $m = p_1^{k_1} \cdots p_l^{k_l}$ be its prime factor decomposition. Let $\vec{\kappa}(t) = (\kappa_1(t), \dots, \kappa_z(t))$ be any vector of z polynomials from $\mathbb{Z}/m\mathbb{Z}[t]$, each of them with a leading coefficient that is coprime with m and such that no crash occurs during the run of* DEC-TT$(m, \kappa_1(t), 1, \vec{\kappa}(t))$. *Let $\pi_E(t) \in \mathbb{Z}/m\mathbb{Z}[t]$ be the non null reminder computed by the last execution of* U-GCD *in that run, i.e., a gcd of $\kappa_1(t), \dots, \kappa_z(t)$. If $h = \deg(\pi_E(t)) > 0$, then for each $j \in \{1, \dots, l\}$ the polynomial $\upsilon_j(t) = (\pi_E(t) \bmod p_j^{k_j}) \in \mathbb{Z}/p_j^{k_j}\mathbb{Z}[t]$ has degree $\deg(\upsilon_j(t)) > 0$ and it divides every $(\kappa_i(t) \bmod p_j^{k_j})$ with $1 \le i \le z$.*

Proof. Choose arbitrarily $j \in \{1, \dots, l\}$ and $i \in \{1, \dots, z\}$. We prove that $\upsilon_j(t) \in \mathbb{Z}/p_j^{k_j}\mathbb{Z}[t]$ divides $(\kappa_i(t) \bmod p_j^{k_j})$. By hypothesis, $\pi_E(t)$ divides $\kappa_i(t)$, i.e., $\kappa_i(t) = \pi_E(t) \cdot \varphi(t)$, for some polynomial $\varphi(t) \in \mathbb{Z}/m\mathbb{Z}[t]$. It easily follows that $\upsilon_j(t)$ divides $(\kappa_i(t) \bmod p_j^{k_j})$. We now prove that $\deg(\upsilon_j(t)) > 0$. Since $h > 0$, it is enough to show that $u_h \bmod p_j^{k_j} > 0$, where u_h is the leading coefficient of $\pi_E(t)$. For a sake of argument, suppose that $u_h \bmod p_j^{k_j} = 0$. Thus, we get $\gcd(u_h, m) \ge p_j^{k_j} > 1$, that is contradicted by item *(2)* of Proposition 10. □

Lemma 16. *Let m be an arbitrary natural with $m > 1$ and let $M(X) \in (\mathbb{L}_m)^{n \times n}$ be the matrix associated with a LCA $\mathcal{F}$ over $(\mathbb{Z}/m\mathbb{Z})^n$. Let $\vec{\kappa}(t) = \kappa_1(t), \dots, \kappa_z(t) \in \mathbb{Z}/m\mathbb{Z}[t]$ be the vector of the coefficients of the characteristic polynomial $\xi(X, X^{-1}) = \chi_{M(X)}(t)$ of $M(X)$ when $\chi_{M(X)}(t)$ is expressed as polynomial in the variables X, X^{-1}, no matter about the order those coefficients appear inside $\vec{\kappa}(t)$. If each of the leading coefficients of $\kappa_1(t), \dots, \kappa_z(t) \in \mathbb{Z}/m\mathbb{Z}[t]$ is coprime with m and no crash occurs during the run of* DEC-TT$(m, \kappa_1(t), 1, \vec{\kappa}(t))$, *then the LCA $\mathcal{F}$ is topologically transitive if and only if* DEC-TT$(m, \kappa_1(t), 1, \vec{\kappa}(t))$ *returns true, or, equivalently, if and only if $h = \deg(\pi_E(t)) = 0$, where $\pi_E(t) \in \mathbb{Z}/m\mathbb{Z}[t]$ is the non null reminder computed by the last call of* U-GCD *in that run, i.e., a gcd of $\kappa_1(t), \dots, \kappa_z(t)$.*

Proof. Let $m = p_1^{k_1} \cdots p_l^{k_l}$ be the prime factor decomposition of m.

Assume that $h > 0$. We are going to prove that $\mathcal{F}$ is not topologically transitive. By Lemma 15, for each $j \in \{1, \dots, l\}$ the polynomial $(\pi_E(t) \bmod p_j^{k_j}) \in \mathbb{Z}/p_j^{k_j}\mathbb{Z}[t]$ divides every $(\kappa_i(t) \bmod p_j^{k_j})$ with $1 \le i \le z$. Moreover, it holds that $\deg(\pi_E(t) \bmod p_j^{k_j}) > 0$.

Furthermore, for each $j \in \{1,\dots,l\}$ not only the polynomial $((\pi_E(t) \bmod p_j^{k_j}) \bmod p_j) = (\pi_E(t) \bmod p_j) \in \mathbb{Z}/p_j\mathbb{Z}[t]$ divides every $((\kappa_i(t) \bmod p_j^{k_j}) \bmod p_j) = (\kappa_i(t) \bmod p_j)$ but also its degree is non null. Indeed, by hypothesis, for each $j \in \{1,\dots,l\}$, p_j can not be a factor of the leading coefficient of $(\pi_E(t) \bmod p_j^{k_j})$. Hence, $\deg((\pi_E(t) \bmod p_j^{k_j}) \bmod p_j) > 0$. Therefore, the gcd of $((\kappa_1(t) \bmod p_j^{k_j}) \bmod p_j), \dots, ((\kappa_z(t) \bmod p_j^{k_j}) \bmod p_j)$ has non null degree. Since $\chi_{M(X)} \bmod q = \chi_{M(X) \bmod q}$, this implies that, by Theorem 6, for each $j \in \{1,\dots,l\}$ each LCA over $(\mathbb{Z}/p_j\mathbb{Z})^n$ having $(M(X) \bmod p_j)$ as associated matrix is not topologically transitive, or, equivalently, by Lemma 7, each LCA over $(\mathbb{Z}/p_j^{k_j}\mathbb{Z})^n$ having $(M(X) \bmod p_j^{k_j})$ as associated matrix is not topologically transitive. Therefore, $\mathcal{F}$ is not topologically transitive.

Conversely, suppose now that $h = 0$. We will prove that $\mathcal{F}$ is topologically transitive. Clearly, for each $j \in \{1,\dots,l\}$ the polynomial $(\pi_E(t) \bmod p_j^{k_j})$ of null degree divides every $(\kappa_i(t) \bmod p_j^{k_j})$ with $1 \le i \le z$. We now want to show that for each $j \in \{1,\dots,l\}$ there exists no polynomial $\upsilon^j(t) \in \mathbb{Z}/p_j^{k_j}\mathbb{Z}[t]$ with $\deg(\upsilon^j(t)) > 0$ dividing every $(\kappa_i(t) \bmod p_j^{k_j})$ with $1 \le i \le z$. This ensures that each LCA over $(\mathbb{Z}/p_j^{k_j}\mathbb{Z})^n$ having $(M(X) \bmod p_j^{k_j})$ as associated matrix is topologically transitive and then $\mathcal{F}$ is too. So, we proceed by assuming, for a sake of argument, that there exists $o \in \{1,\dots,l\}$ and a polynomial $\upsilon^o(t) \in \mathbb{Z}/p_o^{k_o}\mathbb{Z}[t]$ with $\deg(\upsilon^o(t)) > 0$ dividing every $(\kappa_i(t) \bmod p_o^{k_o})$ with $1 \le i \le z$. By Lemma 14, $\kappa_i(t) = a_1(\kappa_i(t) \bmod p_1^{k_1}) + \dots + a_l(\kappa_i(t) \bmod p_l^{k_l})$, where $a_1,\dots,a_l$ defines define $\mathcal{I}^{-1}$. Hence, for every i with $1 \le i \le z$ we can write

$$\kappa_i(t) = a_1(\kappa_i(t) \bmod p_1^{k_1}) + \dots + a_o\upsilon^o(t)\varphi_i^o(t) + \dots + a_l(\kappa_i(t) \bmod p_l^{k_l})$$

for some polynomial $\varphi_i^o(t) \in \mathbb{Z}/p_j^{k_j}\mathbb{Z}[t]$. By items *iii*) and *iv*) of Lemma 14, it follows that

$$(a_1 + \dots + a_o\upsilon^o(t) + \dots a_l) \cdot [a_1(\kappa_i(t) \bmod p_1^{k_1}) + \dots + a_o\varphi_i^o(t) + \dots + a_l(\kappa_i(t) \bmod p_l^{k_l})] = \kappa_i(t)$$

and, hence, $\upsilon(t) = a_1 + \dots + a_o\upsilon^o(t) + \dots + a_l$ divides every $\kappa_i(t)$. Moreover $a_o \cdot b_o \neq 0$, where $b_o \neq 0$ is the leading coefficient of $\upsilon^o(t)$. Indeed, if $a_o \cdot b_o = 0$, it would hold that $a_1 \cdot 0 + \dots + a_o \cdot b_o + \dots + a_l \cdot 0 = 0$, i.e., $\mathcal{I}(0) = (0,\dots,b_o,\dots,0)$ implying that $b_o = 0$. Therefore, we get $\deg(\upsilon(t)) > 0$ and this contradicts that $h = \deg(\pi_E(t)) = 0$. □

We are now able to prove Theorem 13.

Proof. Let $\mathcal{F}$ be any LCA $(\mathbb{Z}/m\mathbb{Z})^n$ with associated matrix $M(X) \in (\mathbb{L}_m)^{n\times n}$. Let $\vec{\kappa}(t) = \kappa_1(t),\dots,\kappa_z(t) \in \mathbb{Z}/m\mathbb{Z}[t]$ be the vector of the coefficients of the characteristic polynomial $\xi(X,X^{-1}) = \chi_{M(X)}(t)$ of $M(X)$ when $\chi_{M(X)}(t)$ is expressed in the variables X, X^{-1}, no matter about the order those coefficients appear inside $\vec{\kappa}(t)$. We are going to prove that $\mathcal{F}$ is topologically transitive iff DEC-TT$(m,\kappa_1(t),1,\vec{\kappa}(t))$ returns true.

Let $m = m_1^{s_1}\cdots m_\ell^{s_\ell}$ be the factor decomposition of m provided by the overall crashes occurred in the runs of all the recursive calls of DEC-TT executed when running DEC-TT$(m,\kappa_1(t),1,\vec{\kappa}(t))$.

By Remark 12, DEC-TT$(m,\kappa_1(t),1,\vec{\kappa}(t))$ returns true iff every DEC-TT$(m_e,\kappa_1(t) \bmod m_e,1,\vec{\kappa}(t) \bmod m_e)$ returns true. Since no crash occurs during the run of DEC-TT$(m_e,\kappa_1(t) \bmod m_e,1,\vec{\kappa}(t) \bmod m_e)$, by Lemma 16, every DEC-TT$(m_e,\kappa_1(t) \bmod m_e,1,\vec{\kappa}(t) \bmod m_e)$ returns true iff every LCA over $(\mathbb{Z}/m_e\mathbb{Z})^n$ with associated matrix $M(X) \bmod m_e$ is topologically transitive. By Lemma 7, the latter holds iff every LCA over $(\mathbb{Z}/m_e^{s_e}\mathbb{Z})^n$ with associated matrix $M(X) \bmod m_e^{s_e}$ is topologically transitive, i.e., by Lemma 3, iff $\mathcal{F}$ is topologically transitive. □

7. Applications

In this section we illustrate how our results can be exploited in applications with the achievement of improving them. Considering the rapid growing of cryptographic techniques and the fact that LCA are often involved in designing these latter, we will deal with some representative applications in the domain of cryptosystems, namely, data encryption methods. Such applications are based on one-dimensional LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ for some natural $m > 1$. It is well-known that, in order to ensure the security level expected in real scenarios, good cryptosystems have to satisfy the so-called *confusion* and *diffusion* properties (along with some variants of them). Ergodicity and chaotic behaviour are just the dynamical counterparts of the required cryptographic properties [1] and then they have to be exhibited by the dynamical system on which the cryptosystem is based. Actually, Algorithms DECIDE-P-TT and DEC-TT allow one to establish in an efficient way whether one-dimensional LCA exhibit such behaviours. Therefore, they are important tools to be used in the above mentioned applications for building one-dimensional LCA with the required properties and, then, for improving the existing methods which are based on such LCA.

Recently, in [12], the authors present an image encryption scheme based on hybrid (i.e., non-uniform) ECA composed of two different "chaotic" global rules. They state that such CA are used to establish a novel pseudo-random coupled map lattices (PRCML) model with the declared goal to enhance the chaotic properties of such a kind of model. We recall that a non-uniform cellular automata is defined by a family $\{h_j\}_{j\in\mathbb{Z}}$ of local rules $h_j : Q^{2r_j+2} \to Q$, each of them of its own radius r_j. Similarly to CA, the global rule of a non-uniform cellular automata is the map $\mathcal{F}_\nu$ defined as

$$\forall c \in Q^{\mathbb{Z}}, \quad \forall i \in \mathbb{Z}, \quad \mathcal{F}_\nu(c)_i = h_i(c_{i-r_i},\dots,c_{i+r_i})$$

A non-uniform CA over the alphabet $Q = \mathbb{Z}/m\mathbb{Z}$ is said to be linear if all its local rules are linear. An interesting subclass of non-uniform CA is the one of peculiar periodic non-uniform CA that are defined by an even natural $n > 1$ and two local rules f and g of radius r in such a way that

$$h_j = \begin{cases} f & \text{if } j \bmod n \in \{0, \dots, n/2 - 1\}, \\ g & \text{otherwise .} \end{cases}$$

In other terms, the rules f and g defining any of these non-uniform CA are distributed in the lattice space $\mathbb{Z}$ in such a way that in every segment of positions $\{jn, \dots, jn + n - 1\}$ the rule f acts in the first half of positions, while g in the second half, as far as the update of any configuration is concerned. We want to put in evidence that these periodic non-uniform CA are nothing but (i.e., they are topologically conjugated to) one-dimensional CA over Q^n each of them defined by a suitable local rule. Moreover, if f and g are linear local rules over $\mathbb{Z}/m\mathbb{Z}$, the resulting periodic non-uniform CA turns out to be LCA over $(\mathbb{Z}/m\mathbb{Z})^n$. The previous described periodic non-uniform CA are just the ones involved inside the encryption application presented in [12].

Let us discuss some important aspects regarding how they are used inside that application. First of all, we want to stress that f and g are two ECA local rules chosen from a list of rules, each of them, as stated by the authors, individually giving rise to a "chaotic" CA global transition function. However, the involved term "chaos" is inappropriate since it refers to a qualitative classification (see [16], for instance) and the list actually contains elementary rules that do not give rise to a real chaotic global behaviour at all. As an example, the ECA local rule 110 has a global transition function that is not surjective and, hence, it is not chaotic according to the formal and recognized definition of chaos from [11]. The same holds for ECA local rule 18. Secondly, the fact that combining two rules each of them exhibiting a chaotic global behaviour gives rise to a chaotic non-uniform CA should be proved, but the authors take it for granted, while it is not actually true in general.

Anyway, they consider an actual scenario in which the ECA rules chosen for building the non-uniform CA do not always give rise to a chaotic CA global transition function and in addition nothing is ensured regarding a real chaotic behaviour of the non-uniform CA built combining two of them. As a paradigmatic example, they propose the combination of the rules 18 and 102, the first individually giving rise to a non-surjective CA that, as a consequence, can not be chaotic at all. Moreover, it is not difficult to prove that neither the obtained non-uniform CA is chaotic, although it is well known that the global CA transition function defined by the rule 102 is. Indeed, since n is sufficiently large ($n = 100$ in the paper) there exists a configuration containing a pattern that has no pre-image as far as the ECA 18 is considered and that is located inside the segment of positions where the rule 18 itself acts. In this way, neither non-uniform CA is surjective and, therefore, it is not chaotic.

However, if f and g are both linear, the results of this paper can be exploited for considerably improving the proposed application. Indeed, if the 1×1 matrices (with elements in $\mathbb{Z}/m\mathbb{Z}$) defining the local rules f and g are a_{-1}, a_0, a_1 and b_{-1}, b_0, b_1, respectively, then the periodic non-uniform CA built combining f and g is nothing but the LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ with the following associated matrix

$$M(X) = \begin{bmatrix} a_0 & a_1 & 0 & \dots & \dots & \dots & \dots & \dots & 0 & a_{-1}X \\ a_{-1} & a_0 & a_1 & 0 & \dots & \dots & \dots & \dots & 0 & 0 \\ 0 & a_{-1} & a_0 & a_1 & 0 & \dots & \dots & \dots & 0 & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ddots & 0 & a_{-1} & a_0 & a_1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & 0 & b_{-1} & b_0 & b_1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \dots & 0 & b_{-1} & b_0 & b_1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & 0 & b_{-1} & b_0 & b_1 \\ b_1X^{-1} & 0 & 0 & \dots & \dots & \dots & \dots & 0 & b_{-1} & b_0 \end{bmatrix},$$

where a_{-1}, a_0, a_1 appear in the first $n/2$ rows, while b_{-1}, b_0, b_1 in the last $n/2$ ones, and we have assumed that $n > 2$.

The characteristic polynomial $\chi_{M(X)}(t)$ of $M(X)$ can be rewritten as

$$\xi(X, X^{-1}) = \kappa_1(t)X^{-1} + \kappa_2(t) + \kappa_3(t)X \ ,$$

where

$$\kappa_1(t) = -(a_1 b_1)^{n/2},$$

$$\kappa_3(t) = (a_{-1} b_{-1})^{n/2},$$

and $\kappa_2(t)$ is a polynomial of degree n. According to the results from Section 4, when $m = 2$, the LCA with associated matrix $M(X)$ is chaotic unless $\kappa_1(t) = \kappa_3(t) = 0$. Indeed, $\gamma(t) = \gcd(\kappa_1(t), \kappa_2(t), \kappa_3(t))$ is a non null constant polynomial unless $\kappa_1(t) = \kappa_3(t) = 0$. If the linear ECA local rules f and g with number 150 and 102, respectively, are used in the application from [12], or, equivalently, the rule 18 is replaced by the rule 150, the periodic non-uniform CA built combining f and g is nothing but the LCA over $(\mathbb{Z}/2\mathbb{Z})^{100}$ with associated matrix $M(X)$ as above and in which $a_{-1} = 1, a_0 = 1, a_1 = 1, b_{-1} = 0, b_0 = 1, b_1 = 1$. In this way, we get

$$\kappa_1(t) = 1,$$

$$\kappa_3(t) = 0,$$

and, hence, the obtained non-uniform CA is really chaotic. The same holds when the rules 90 and 102 are combined, the first one also appearing inside the list from [12] and individually giving rise to a chaotic CA global transition function. Let us not that the rule 60 is inside that list and it has the same property as the rule 90, too, but, when it is combined with the rule 102, we get $\kappa_1(t) = \kappa_3(t) = 0$, and hence the obtained non-uniform CA is not chaotic, although it is built by means of two rules, both of them individually defining a chaotic CA.

We stress that the scheme can be improved by considering values of m with $m > 2$. This considerably increases the number of (non elementary) local rules inside the list. Clearly, Algorithm DEC-TT has to be used in order that the non-uniform CA obtained combining two rules from the list is chaotic.

A block cypher scheme based on a linear higher-order CA of memory $n = 2$ over $\mathbb{Z}/m\mathbb{Z}$ with $m = 2$ was proposed in [5]. Since linear higher-order CA are just LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ with associated matrix presenting a specific structure, namely, a Frobenius normal form, it is possible to analyse and improve the scheme by exploiting our results concerning LCA.

The LCA $\mathcal{F}$ involved in the cypher scheme is defined by a local rule of radius $r = 1$ and the matrix associated with $\mathcal{F}$ is

$$M(X) = \begin{bmatrix} 0 & 1 \\ 1 & a_{-1}X + a_0 + a_1X^{-1} \end{bmatrix} ,$$

where a_{-1}, a_0 and a_1 are coefficients to be suitably set up.

The functioning of the scheme is as follows. The first and the seconds half bits of a plain text are inserted inside the first and second component c^1 and c^2, respectively, of the initial configuration c of the LCA $\mathcal{F}$ and, once the L configurations $\mathcal{F}(c), \ldots, \mathcal{F}^L(c)$ with $L > 2$ have been computed, the content of $\mathcal{F}^L(c)$ is considered as the ciphered text. Since $\det(M(X)) \neq 0$, the LCA is reversible and this allows recovering the initial plain text from the ciphered one.

According to the experimental observations by the authors, the following three choices $a_{-1} = a_1 = 1$ and $a_0 = 0$, $a_0 = a_1 = 1$ and $a_{-1} = 0$, and $a_{-1} = a_0 = a_1 = 1$ lead the encryption scheme to exhibit good performances. A rigorous explanation of that follows from our results. Indeed, the polynomial characteristic of $M(X)$ is

$$\chi_{M(X)}(t) = t^2 - (a_{-1}X + a_0 + a_1X^{-1})t - 1$$

and it can be rewritten as

$$\xi(X, X^{-1}) = \kappa_1(t)X^{-1} + \kappa_2(t) + \kappa_3(t)X ,$$

where

$$\kappa_1(t) = -a_1t,$$

$$\kappa_2(t) = t^2 - a_0t - 1,$$

$$\kappa_3(t) = -a_{-1}t.$$

By running Algorithm DECIDE-P-TT in these three situations, one finds out that all the corresponding LCA are ergodic and chaotic. Therefore, the cypher scheme can be equipped by Algorithm DECIDE-P-TT to avoid bad choices and so, by ensuring confusion and diffusion, in such a way that attacks are much harder. Clearly, also Algorithm EXISTING allows getting the same conclusions, but with worse performances. Moreover, adopting Algorithm DECIDE-P-TT becomes even more relevant if the plain text is divided in a number n of parts where n is significantly greater than 2 and, as a consequence, Algorithm DECIDE-P-TT performs significantly better than Algorithm EXISTING. Furthermore, if the plain text is coded as a sequence of elements of $\mathbb{Z}/m\mathbb{Z}$ for some natural m with $m > 2$ the choices for the expression of $\mathcal{F}$ to be used increase and the cypher scheme can be equipped by Algorithm DEC-TT in order to ensure confusion and diffusion.

In [6], authors propose a (n, P)-threshold secret sharing scheme involving P participants and based on linear higher-order CA of memory n over the alphabet $\mathbb{Z}/2\mathbb{Z}$, i.e., LCA over $(\mathbb{Z}/2\mathbb{Z})^n$ with associated matrix in Frobenius normal form.

As discussed at the beginning of this section, the one-dimensional LCA $\mathcal{F}$ on which the method is based has to be chaotic in order to ensure the cryptographic properties of confusion and diffusion. Therefore, it is essential that Algorithm DECIDE-P-TT deciding chaos is inserted in the scheme just before step 4. of the setup phase from [6] with the additional requirement that steps 1. to 3., which by using a pseudo-random number generator produce the LCA $\mathcal{F}$, have to be repeated whenever they provide a non chaotic LCA. Moreover, the number of the expressions to be used for $\mathcal{F}$ increases for schemes over an alphabet $\mathbb{Z}/m\mathbb{Z}$, where m is any integer with $m > 2$. The introduction of such a choice in the scheme along with Algorithm DEC-TT makes attacks much harder.

The idea from [6] of employing linear higher-order CA of memory n in secret sharing schemes is exploited in [17] where the authors introduce a new method for sharing greyscale secret images. In the setup phase, a reversible linear higher-order CA of memory n over $\mathbb{Z}/2\mathbb{Z}$ is built, where n is the number of pixels of a secret greyscale image. Equivalently, a reversible LCA $\mathcal{F}$ over $(\mathbb{Z}/2\mathbb{Z})^n$ is built which evolves in the sharing phase starting from the initial configuration over $(\mathbb{Z}/2\mathbb{Z})^n$ containing the binary representation of the n image pixels. Although the reversibility condition over $\mathcal{F}$ is a necessary requirement for recovering the secret image, i.e., for computing back the initial configuration by means of $\mathcal{F}$, it is important that $\mathcal{F}$ is also chaotic in order to ensure the cryptographic properties of confusion and diffusion. Therefore, Algorithm DECIDE-P-TT deciding chaos should is inserted in the setup phase of the proposed method with the additional requirement that item 2., which produces $\mathcal{F}$ by using a pseudo-random number generator, have to be repeated whenever it provides a non chaotic LCA.

8. Conclusions

We provided an efficient algorithm deciding chaos for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ and we illustrated its impact in some representative applications in the domain of cryptosystems. Providing (efficient) algorithms that decide other meaningful dynamical properties for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ as, for instance, strong transitivity, is an important step for further researches in this domain. This would also allow one to build even more robust methods based on such CA in applications. Another important research direction consists in considering the multidimensional setting. Besides having a theoretical value, providing algorithms that decide chaos and other dynamical properties for multidimensional LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ will be certainly useful in many applications involving multidimensional data.

CRediT authorship contribution statement

Term, Conceptualization, Methodology, Formal Analysis, Investigation, Writing - Review & Editing has been shared by the authors.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgements

We thank Darij Grinberg for letting us know about the idea of the crash regarding the Euclidean algorithm. This work was partially supported by the MUR under the grant “Dipartimenti di Eccellenza 2023-2027” of the Department of Informatics, Systems and Communication of the University of Milano-Bicocca, Italy.

References

[1] Gonzalo Álvarez, Shujun Li, Some basic cryptographic requirements for chaos-based cryptosystems. I, J. Bifurc. Chaos 16 (8) (2006) 2129–2151.
[2] Nicolas Bourbaki, Elements of Mathematics. Algebra I: Chapters 1-3, Hermann, 1974.
[3] Lieven Le Bruyn, Michel Van den Bergh, Algebraic properties of linear cellular automata, Linear Algebra Appl. 157 (1991) 217–234.
[4] Gianpiero Cattaneo, Alberto Dennunzio, Luciano Margara, Solution of some conjectures about topological properties of linear cellular automata, Theor. Comput. Sci. 325 (2) (2004) 249–271.
[5] Zhenchuan Chai, Zhenfu Cao, Yuan Zhou, Encryption based on reversible second-order cellular automata, in: Guihai Chen, Yi Pan, Minyi Guo, Jian Lu (Eds.), Parallel and Distributed Processing and Applications - ISPA 2005 Workshops, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 350–358.
[6] Angel Martín del Rey, Joaquim Pereira Mateus, Gerardo Rodríguez Sánchez, A secret sharing scheme based on cellular automata, Appl. Math. Comput. 170 (2) (2005) 1356–1364.
[7] Alberto Dennunzio, Enrico Formenti, Darij Grinberg, Luciano Margara, Chaos and ergodicity are decidable for linear cellular automata over $(\mathbb{Z}/m\mathbb{Z})^n$, Inf. Sci. 539 (2020) 136–144.
[8] Alberto Dennunzio, Enrico Formenti, Luciano Margara, An easy to check characterization of positive expansivity for additive cellular automata over a finite abelian group, IEEE Access 11 (2023) 121246–121255.
[9] Alberto Dennunzio, Enrico Formenti, Darij Grinberg, Luciano Margara, Dynamical behavior of additive cellular automata over finite abelian groups, Theor. Comput. Sci. 843 (2020) 45–56.
[10] Alberto Dennunzio, Enrico Formenti, Darij Grinberg, Luciano Margara, Decidable characterizations of dynamical properties for additive cellular automata over a finite abelian group with applications to data encryption, Inf. Sci. 563 (2021) 183–195, https://doi.org/10.1016/j.ins.2021.02.012.
[11] Robert Luke Devaney, An Introduction to Chaotic Dynamical Systems, Addison-Wesley Advanced Book Program, Addison-Wesley, 1989.
[12] Youheng Dong, Geng Zhao, Yingjie Ma, Zhou Pan, Rui Wu, A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata, Inf. Sci. 593 (2022) 121–154, https://doi.org/10.1016/j.ins.2022.01.031.
[13] Masanobu Ito, Nobuyasu Osato, Masakazu Nasu, Linear cellular automata over $\mathbb{Z}_m$, J. Comput. Syst. Sci. 27 (1983) 125–140.
[14] Jarkko Kari, Linear cellular automata with multiple state variables, in: Horst Reichel, Sophie Tison (Eds.), STACS 2000, in: LNCS, vol. 1770, Springer-Verlag, 2000, pp. 110–121.
[15] Giovanni Manzini, Luciano Margara, A complete and efficiently computable topological classification of d-dimensional linear cellular automata over $\mathbb{Z}_m$, Theor. Comput. Sci. 221 (1–2) (1999) 157–177.
[16] S. Wolfram, Theory and Applications of Cellular Automata, World Scientific, Singapore, 1986.
[17] Jamal Zarepour-Ahmadabadi, Mohammad Ebrahim Shiri Ahmadabadi, Alimohammad Latif, An adaptive secret image sharing with a new bitwise steganographic property, Inf. Sci. 369 (2016) 467–480.