IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 October 2023, accepted 19 October 2023, date of publication 30 October 2023, date of current version 3 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3328540

THEORY

An Easy to Check Characterization of Positive Expansivity for Additive Cellular Automata Over a Finite Abelian Group

ALBERTO DENNUNZIO[1], ENRICO FORMENTI[2], AND LUCIANO MARGARA[3]

[1]Dipartimento di Informatica, Sistemistica e Comunicazione, Università degli Studi di Milano-Bicocca, 20126 Milan, Italy
[2]CNRS, I3S, Université Côte d'Azur, 06103 Nice, France
[3]Department of Computer Science and Engineering, University of Bologna, Cesena Campus, 47521 Cesena, Italy

Corresponding author: Alberto Dennunzio (alberto.dennunzio@unimib.it)

This work was supported in part by the Ministry of University and Research (MUR) under Dipartimenti di Eccellenza (2023–2027) and the Department of Informatics, Systems and Communication, University of Milano-Bicocca, Italy.

ABSTRACT Additive cellular automata over a finite abelian group are a wide class of cellular automata (CA) that are able to exhibit most of the complex behaviors of general CA and they are often exploited for designing applications in different practical contexts. We provide an easy to check algebraic characterization of positive expansivity for Additive Cellular Automata over a finite abelian group. We stress that positive expansivity is an important property that defines a condition of strong chaos for CA and, for this reason, an easy to check characterization of positive expansivity turns out to be crucial for designing proper applications based on Additive CA and where a condition of strong chaos is required. First of all, in the paper an easy to check algebraic characterization of positive expansivity is provided for the non trivial subclass of Linear Cellular Automata over the alphabet $(\mathbb{Z}/m\mathbb{Z})^n$. Then, we show how it can be exploited to decide positive expansivity for the whole class of Additive Cellular Automata over a finite abelian group.

INDEX TERMS Cellular automata, additive cellular automata, chaos, positive expansivity.

I. INTRODUCTION

Cellular automata (CA) are well-known formal models that find application in several disciplines and their different subdomains. This is essentially due to three reasons: the huge variety of distinct CA dynamical behaviors; the emergence of complex behaviors from simple local interactions; the ease of their implementation (even at a hardware level).

In practical applications one needs to know if the CA used for modelling a certain system exhibits some specific property. However, this can be a severe issue. Indeed, a strong result by Jarkko Kari [6] states that all non-trivial dynamical behaviors are undecidable. From this seminal result, a long sequence followed.

Luckily, the undecidability issue can be tackled by imposing some constraints on the model. In the specific case of this paper, the alphabet and the global updating map are constrained to be a finite abelian group and an additive function, respectively, giving rise to *Additive CA over a finite abelian group* or, briefly, *Additive CA* (see [1], [2], [12], e.g., for studies regarding linear and group CA). We stress that such requirements do not prevent Additive CA at all from being successfully used for practical purposes. On the contrary, since Additive CA are able to exhibit most of the complex behaviors of general CA, they are often exploited for designing many applications (see, for instance, [11], [13]). Moreover, Additive CA are more expressive and they give rise to much more complex dynamics than the already investigated subclass of Linear Cellular Automata over the alphabet $(\mathbb{Z}/m\mathbb{Z})^n$ with $n = 1$.

Among the dynamical properties, positive expansivity received and still receives a significant attention by researchers since it is a stronger form of sensitive dependence on the initial conditions, the latter being the essence of a

The associate editor coordinating the review of this manuscript and approving it for publication was Ludovico Minati.

chaotic behavior. Moreover, in CA settings positive expansivity plays an important role since it is just a condition of strong chaos, since positively expansive CA are chaotic besides exhibiting sensitive dependence on the initial conditions. While the related (un)decidability issue is still an open problem for general CA, positive expansivity turns out to be decidable as far as Additive CA are concerned. Indeed, this decidability result follows from a combination of two known facts: *i*) positive expansivity is decidable for CA with sofic traces [5]; *ii*) the traces of any Additive CA are subshifts of finite type (and, hence, they are sofic), a consequence of the classical result by Kitchens and Schmidt that all group subshifts are of finite type [7]. However, the decidability result is not useful for practical purposes at all, i.e., the corresponding algorithm is impractical. Thus, besides being of theoretical interest, an easy to check characterization of positive expansivity for Additive CA would turn out to be crucial for designing proper applications based on such CA and in situations where, as often happens, a condition of strong chaos is required.

In this paper we provide an easy to check characterization of positive expansivity for Additive CA over a finite abelian group. First of all, an easy to check algebraic characterization of positive expansivity is provided for the non trivial subclass of Linear Cellular Automata over the alphabet $(\mathbb{Z}/m\mathbb{Z})^n$, where m is any natural greater than 1. Namely, for any Linear CA over $(\mathbb{Z}/m\mathbb{Z})^n$ such a characterization is expressed as an easy to check condition on the degrees of the coefficients (that are Laurent polynomials) of the characteristic polynomial of the matrix associated with the Linear CA. Then, we show how it can be exploited to decide positive expansivity for the whole class of Additive Cellular Automata over a finite abelian group.

The main and more difficult part of this work consists of the proof of an easy to check algebraic characterization of positive expansivity for Linear Cellular Automata over $(\mathbb{Z}/p\mathbb{Z})^n$, where p is any prime number (Theorem 1). To reach that result

1) first of all, we provide an easy to check algebraic characterization of positively expansive Linear Cellular Automata over $(\mathbb{Z}/p\mathbb{Z})^n$ with associated matrix that is (the traspose of one) in a rational canonical form consisting of only one block; this is the heart of our work;
2) then, we prove that such an algebraic characterization turns out to hold also for positively expansive Linear Cellular Automata over $(\mathbb{Z}/p\mathbb{Z})^n$ with associated matrix that is in a rational canonical form possibly consisting of more than one block;
3) finally, we prove that such an algebraic characterization turns out to hold also for all positively expansive Linear Cellular Automata over $(\mathbb{Z}/p\mathbb{Z})^n$.

Afterwards, the easy to check algebraic characterization of positive expansivity is extended first from Linear Cellular Automata over $(\mathbb{Z}/p\mathbb{Z})^n$ to Linear Cellular Automata over $(\mathbb{Z}/p^k\mathbb{Z})^n$, where k is any non zero natural (Theorem 2). If the prime factor decomposition of m is assumed to be known, that characterization immediately extends to Linear Cellular Automata over $(\mathbb{Z}/m\mathbb{Z})^n$ (Corollary 1). However, since the prime factor decomposition is a well-known difficult task (i.e., no algorithm has been published yet that can factor any natural in polynomial time), it should be avoided, especially for practical purposes. Actually, we have gone one step further: in Section III-B we show how the easy to check characterization of positive expansivity for Linear Cellular Automata over $(\mathbb{Z}/p\mathbb{Z})^n$ can be exploited to decide positive expansivity for Linear Cellular Automata over $(\mathbb{Z}/m\mathbb{Z})^n$ in an efficient way (i.e., without decomposing m into its prime factors and by only making use of gcd operations) and, at the end, for whole class of Additive Cellular Automata over a finite abelian group (Theorem 3).

The paper is structured as follows. Next section introduces all the necessary background and notions. Section III contains our results. Section IV is entirely devoted to the proof of Theorem 1. In the last section we draw our conclusion.

II. BASIC NOTIONS

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

Let $\mathbb{K} = \mathbb{Z}/m\mathbb{Z}$ for some natural $m > 1$ and let q be a natural with $q < m$. 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.

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

$$\forall c, c' \in \Sigma^{\mathbb{Z}},\ d(c,c') = \begin{cases} 0, & \text{if} \quad c = c', \\ 2^{-\min\{|j| : j\in\mathbb{Z},\, c_j \neq c'_j\}}, & \text{otherwise.} \end{cases}$$

Whenever the term *linear* is involved the alphabet Σ 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. On the other hand, whenever the term *additive* is involved the alphabet Σ is a finite abelian group G and the configuration space turns $G^{\mathbb{Z}}$ turns out to be an abelian group, too, where the group operation of $G^{\mathbb{Z}}$ is the componentwise extension of the group operation of G, both of them will be denoted by $+$.

A *one-dimensional CA* (or, briefly, a *CA*) over Σ is a pair $(\Sigma^{\mathbb{Z}}, \mathcal{F})$, where $\mathcal{F}\colon \Sigma^{\mathbb{Z}} \to \Sigma^{\mathbb{Z}}$ is the uniformly continuous transformation (called *global rule*) defined as $\forall c \in \Sigma^{\mathbb{Z}}, \forall i \in \mathbb{Z}, \mathcal{F}(c)_i = f(c_{i-r}, \ldots, c_{i+r})$, for some fixed natural number $r \in \mathbb{N}$ (called *radius*) and some fixed function $f\colon \Sigma^{2r+1} \to \Sigma$ (called *local rule* of radius r). In the sequel, when no misunderstanding is possible, we will sometimes identify any CA with its global rule.

We recall that a CA $(\Sigma^{\mathbb{Z}}, \mathcal{F})$ is *positively expansive* if for some constant $\varepsilon > 0$ it holds that for any pair of distinct configurations $c, c' \in \Sigma^{\mathbb{Z}}$ there exists a natural number ℓ such that $d(\mathcal{F}^{\ell}(c), \mathcal{F}^{\ell}(c')) \geq \varepsilon$. We stress that CA positive expansivity is a condition of strong *chaos*. Indeed, on a hand, positive expansivity is a stronger condition than *sensitive dependence on the initial conditions*, the latter being the essence of the chaos notion. On the other hand, any positively expansive CA is also *topologically transitive* and, at the same time, it has *dense periodic orbits*. Therefore, any positively expansive CA is chaotic according to the Devaney definition of chaos (see [4], for the definitions of chaos, sensitive dependence on the initial conditions, topological transitivity, and denseness of dense periodic orbits). Finally, we recall that if a CA $\mathcal{F}$ is positively expansive then $\mathcal{F}$ is surjective.

A. LINEAR AND ADDITIVE CA

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

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

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

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

We now recall the notion of Additive CA, a wider class than LCA. An *Additive CA* over G is a CA $(G^{\mathbb{Z}}, \mathcal{F})$ where the global rule $\mathcal{F} : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$ is an endomorphism of $G^{\mathbb{Z}}$. We stress that the local rule $f : G^{2r+1} \to G$ of an Additive CA of radius r over a finite abelian group G can be written as $\forall (x_{-r}, \ldots, x_r) \in G^{2r+1}, f(x_{-r}, \ldots, x_r) = \sum_{i=-r}^{r} f_i(x_i)$, where the functions f_i are endomorphisms of G. Moreover, as a consequence of the application of the fundamental theorem of finite abelian groups to Additive CA (see [3], for details), without loss of generality we can assume that

$G = \mathbb{Z}/p^{k_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{k_n}\mathbb{Z}$ for some naturals $k_1, \ldots, k_n$ with $k_1 \geq k_2 \geq \ldots \geq k_n$.

Let $\hat{G} = (\mathbb{Z}/p^{k_1}\mathbb{Z})^n$ and let $\psi : G \to \hat{G}$ be the map defined as $\forall h \in G, \forall i = 1, \ldots, n, \psi(h)^i = h^i\, p^{k_1-k_i}$, where, for a sake of clarity, we stress that h^i denotes the i-th component of h, while $p^{k_1-k_i}$ is just the $(k_1 - k_i)$-th power of p. Let $\Psi : G^{\mathbb{Z}} \to \hat{G}^{\mathbb{Z}}$ be the componentwise extension of ψ, i.e., the function defined as $\forall \boldsymbol{c} \in G^{\mathbb{Z}}, \forall j \in \mathbb{Z}, \Psi(\boldsymbol{c})_j = \psi(\boldsymbol{c}_j)$. The function Ψ turns out to be continuous and injective.

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

Let $(G^{\mathbb{Z}}, F)$ be any Additive CA and let $f : G^{2r+1} \to G$ be its local rule defined, by $2r+1$ endomorphisms $f_{-r}, \ldots, f_r$ of G. For each $z \in \{-r, \ldots, r\}$, let $A_z = (a_{i,j}^{(z)})_{1\leq i\leq n,\, 1\leq j\leq n} \in (\mathbb{Z}/p^{k_1}\mathbb{Z})^{n\times n}$ be the matrix such that $\forall i, j \in \{1, \ldots, n\}$, $a_{i,j}^{(z)} = p^{k_j-k_i} \cdot f_z(e_j)^i$. The *LCA associated with the Additive CA* $(G^{\mathbb{Z}}, F)$ is $(\hat{G}^{\mathbb{Z}}, L)$, where L is defined by $A_{-r}, \ldots, A_r$ or, equivalently, by $A = \sum_{z=-r}^{r} A_z X^{-z} \in \mathbb{Z}/p^{k_1}\mathbb{Z}\left[X, X^{-1}\right]^{n\times n}$. We stress that the following diagram commutes

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

i.e., $L \circ \Psi = \Psi \circ F$. Therefore, $(\hat{G}^{\mathbb{Z}}, L)$ is said to be the LCA associated with $(G^{\mathbb{Z}}, F)$ *via the embedding* Ψ. In general, $(G^{\mathbb{Z}}, F)$ is not topologically conjugated (i.e., homeomorphic) to $(\hat{G}^{\mathbb{Z}}, L)$ but $(G^{\mathbb{Z}}, F)$ is a subsystem of $(\hat{G}^{\mathbb{Z}}, L)$ and the latter condition alone is not enough in general to lift dynamical properties from a one system to the other one. Despite this obstacle, in the sequel we will succeed in doing such a lifting, as far as positive expansivity is concerned.

III. RESULTS

The following two notions are fundamental throughout this paper.

Definition 1 (Positive and Negative Degree): The positive *(resp.,* negative*) degree of any given polynomial $\alpha \in \mathbb{L}_m$ with $\alpha \neq 0$, denoted by* $\deg^+(\alpha)$ *(resp.,* $\deg^-(\alpha)$*), is the maximum (resp, minimum) value among the degrees of the monomials of α. Such notions extend to any element $\upsilon \neq 0$ of $\mathbb{S}_m^n$ when υ is considered as a formal power series with coefficients in $(\mathbb{Z}/m\mathbb{Z})^n$ instead of a vector of n elements from $\mathbb{S}_m$ and with the additional defining clause that* $\deg^+(\upsilon) = +\infty$ *(resp.,* $\deg^-(\upsilon) = -\infty$*) if that maximum (resp., minimum) does not exist. Furthermore, the previous notions are extended to both $\alpha = 0$ and $\upsilon = 0$ as follows:* $\deg^+(0) = -\infty$ *and* $\deg^-(0) = +\infty$.

Example 1: The following are the values of the positive and negative degree of some polynomials:
$\deg^+(X^{-3} + X^{-2}) = -2$, $\deg^+(X^{-3} + X^{-2} + 1) = 0$, $\deg^+(X^{-3} + X^{-2} + 1 + X^4) = 4$, $\deg^+(1) = 0$
$\deg^-(X^3 + X^2) = 2$, $\deg^-(X^3 + X^2 + 1) = 0$, $\deg^-(X^{-3} + 1 + X^4) = -3$, $\deg^-(1) = 0$

Definition 2 (Expansive Polynomial and Expansive Matrix): Let $\pi(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_{n-1}t^{n-1} + t^n$ be any polynomial

from $\mathbb{L}_m[t]$. *We say that* $\pi(t)$ *is* expansive *if both the following two conditions are satisfied*:

(*i*) $\deg^+(\alpha_0) > 0$ *and* $\deg^+(\alpha_0) > \deg^+(\alpha_i)$ *for every* $i \in \{1, \ldots, n-1\}$;

(*ii*) $\deg^-(\alpha_0) < 0$ *and* $\deg^-(\alpha_0) < \deg^-(\alpha_i)$ *for every* $i \in \{1, \ldots, n-1\}$;

A matrix $A \in \mathbb{L}_m^{n\times n}$ *is said to be* expansive *if its characteristic polynomial is expansive.*

Remark 1: We stress that if a polynomial $\pi(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_{n-1}t^{n-1} + t^n$ *is expansive then it must necessarily hold that* $\alpha_0 \neq 0$.

Lemma 1: For any three polynomials $\pi, \rho, \tau \in \mathbb{L}_p[t]$ *such that* $\pi = \rho \cdot \tau$ *it holds that* π *is expansive if and only if* ρ *and* τ *are both expansive.*

Proof: Choose arbitrarily three polynomials

$$\pi(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_{n-1}t^{n-1} + t^n$$
$$\rho(t) = \beta_0 + \beta_1 t + \cdots + \beta_{n_1-1}t^{n_1-1} + t^{n_1}$$
$$\tau(t) = \gamma_0 + \gamma_1 t + \cdots + \gamma_{n_2-1}t^{n_2-1} + t^{n_2}$$

such that $\pi = \rho \cdot \tau$. Obviously,

$$\alpha_i = \sum_{i_1 \leq i, i_2 \leq i : i = i_1 + i_2} \beta_{i_1}\gamma_{i_2} \tag{1}$$

for every $i \in \{0, \ldots, n-1\}$ and, in particular, $\alpha_0 = \beta_0\gamma_0$.

Assume that both ρ and τ are both expansive. Hence, $\alpha_0 = \beta_0\gamma_0 \neq 0$ and

$$\begin{aligned}\deg^+(\alpha_0) = \deg^+(\beta_0\gamma_0) &= \deg^+(\beta_0) + \deg^+(\gamma_0)\\ &> \deg^+(\beta_{i_1}) + \deg^+(\gamma_{i_2}) = \deg^+(\beta_{i_1}\gamma_{i_2}),\end{aligned}$$

for every $i_1 \in \{1, \ldots, n_1 - 1\}$ and $i_2 \in \{1, \ldots, n_2 - 1\}$ such that $\beta_{i_1} \neq 0$ and $\gamma_{i_2} \neq 0$ (by Definition 2 a symmetric inequality regarding $\deg^-$ also holds). Let $i \in \{1, \ldots, n-1\}$ be any index such that $\alpha_i \neq 0$. We can write

$$\deg^+(\alpha_i) \leq \deg^+(\beta_{i_1}\gamma_{i_2}) < \deg^+(\alpha_0)$$

for every $i_1 \in \{1, \ldots, n_1 - 1\}$ and $i_2 \in \{1, \ldots, n_2 - 1\}$ such that $i = i_1 + i_2$, $\beta_{i_1} \neq 0$ and $\gamma_{i_2} \neq 0$. Clearly, condition (*ii*) from Definition 2 also holds, as far as $\deg^-(\alpha_i)$ is concerned. Thus, π is expansive.

We prove now that if π is expansive then ρ and τ are both expansive. Assume that the consequent is not true. We deal with the two following cases: (1) ρ is expansive but τ is not (by symmetry, we do not consider the situation in which τ is expansive but ρ is not); (2) neither ρ nor τ are expansive.

(1) Suppose that ρ is expansive but τ is not. If $\gamma_0 = 0$ then it trivially follows that π is not expansive. Otherwise, let *min* be the minimum index such that $deg^+(\gamma_{min}) = \max_{0\leq i_2<n_2}\{deg^+(\gamma_{i_2}) : \gamma_{i_2} \neq 0\}$. Since ρ is expansive, $\beta_0\gamma_{min}$ is the (only) addend of maximum degree in the sum from Equation (1) considered for $i = min$. Thus, $deg^+(\alpha_{min}) = deg^+(\beta_0\gamma_{min})$. Furthermore, $deg^+(\alpha_{min}) = deg^+(\beta_0) + \deg^+(\gamma_{min}) \geq deg^+(\beta_0) + \deg^+(\gamma_0) = deg^+(\beta_0\gamma_0) = deg^+(\alpha_0)$. In a symmetric way, one also gets that $deg^-(\alpha_i) \leq deg^-(\alpha_0)$ for some $i \in \{1, \ldots, n-1\}$.

(2) Suppose that neither ρ nor τ are expansive. If $\beta_0 = 0 \vee \gamma_0 = 0$ then it trivially follows that π is not expansive. Otherwise, let max_1 and max_2 be the maximum indexes such that $\deg^+(\beta_{max_1}) = \max_{0\leq i_1<n_1}\{\deg^+(\beta_{i_2}) : \beta_{i_2} \neq 0\}$ and $\deg^+(\gamma_{max_2}) = \max_{0\leq i_2<n_2}\{\deg^+(\gamma_{i_2}) : \gamma_{i_2} \neq 0\}$, respectively. Consider now Equation (1) for $i = max_1 + max_2$. Take any pair of indexes i_1, i_2 of the sum such that $i_1 \neq max_1$, $i_2 \neq max_2$, $\beta_{i_1} \neq 0$, and $\gamma_{i_2} \neq 0$. If $i_1 < max_1$ (and then $i_2 > max_2$), resp., if $i_1 > max_1$ (and then $i_2 < max_2$), we get that

$$\begin{aligned}\deg^+(\beta_{i_1}) + \deg^+(\gamma_{i_2}) &< \deg^+(\beta_{i_1}) + \deg^+(\gamma_{max_2})\\ &\leq \deg^+(\beta_{max_1}) + \deg^+(\gamma_{max_2}),\end{aligned}$$

resp.,

$$\begin{aligned}\deg^+(\beta_{i_1}) + \deg^+(\gamma_{i_2}) &< \deg^+(\beta_{max_1}) + \deg^+(\gamma_{i_2})\\ &\leq \deg^+(\beta_{max_1}) + \deg^+(\gamma_{max_2}).\end{aligned}$$

Hence, $\deg^+(\beta_{i_1}\gamma_{i_2}) < \deg^+(\beta_{max_1}\gamma_{max_2})$. This implies that $deg^+(\alpha_{max_1+max_2}) = \deg^+(\beta_{max_1}\gamma_{max_2})$. Moreover, $deg^+(\alpha_{max_1+max_2}) = \deg^+(\beta_{max_1}\gamma_{max_2}) \geq \deg^+(\beta_0\gamma_0) = \deg^+(\alpha_0)$ and in a symmetric way, one also gets that $deg^-(\alpha_i) \leq deg^-(\alpha_0)$ for some $i \in \{1, \ldots, n-1\}$.

Therefore, in both cases it follows that π is not expansive and this concludes the proof. □

In the sequel, we will often make use of the following

Definition 3: Let $K \subseteq \mathbb{S}_m^n$. *For any* $s \in \mathbb{Z}$ *we define the following sets:*

$Right(K, s) = \{\upsilon \in K : deg^-(\upsilon) = s\}$,
$Right^*(K, s) = \{\upsilon \in K : deg^-(\upsilon) \geq s\}$,
$Left(K, s) = \{\upsilon \in K : deg^+(\upsilon) = s\}$,
$Left^*(K, s) = \{\upsilon \in K : deg^+(\upsilon) \leq s\}$.

Definition 3 along with the notion of positively expansive CA when reformulated for LCA and the compactness of the configuration space immediately allow stating the following

Lemma 2: Let $\mathcal{F}$ *be any LCA over* $(\mathbb{Z}/m\mathbb{Z})^n$ *and let* $A \in \mathbb{L}_m^{n\times n}$ *be the matrix associated with* $\mathcal{F}$, *where* m *and* n *are any two naturals with* $m > 1$ *and* $n > 1$. *The LCA* $\mathcal{F}$ *is not positively expansive if and only if there exists an integer* $s > 0$ *such that at least one of the following two conditions holds*

- $\exists \upsilon \in Left(\mathbb{S}_m^n, 0) \setminus \{0\} : \forall \ell > 0,\ A^\ell \upsilon \in Left^*(\mathbb{S}_m^n, s)$
- $\exists \upsilon \in Right(\mathbb{S}_m^n, 0) \setminus \{0\} : \forall \ell > 0,\ A^\ell \upsilon \in Right^*(\mathbb{S}_m^n, -s)$

On the contrary, the LCA $\mathcal{F}$ *is positively expansive if and only if there exists a natural number* $\hat{\ell} > 0$ *such that for any* $d \in \mathbb{Z}$ *and any* $\upsilon \in Left(\mathbb{S}_m^n, d)$ *it holds that* $A^\ell \upsilon \in Left(\mathbb{S}_m^n, d+1)$ *for some* $\ell \leq \hat{\ell}$ *and, symmetrically, for any* $d \in \mathbb{Z}$ *and any* $\upsilon \in Right(\mathbb{S}_m^n, d)$ *it holds that* $A^\ell \upsilon \in Right(\mathbb{S}_m^n, d-1)$ *for some* $\ell \leq \hat{\ell}$.

Lemma 3: Let $\mathcal{F}$ *be any surjective LCA over* $(\mathbb{Z}/m\mathbb{Z})^n$ *and let* $A \in \mathbb{L}_m^{n\times n}$ *be the matrix associated with* $\mathcal{F}$, *where* m *and* n

are any two naturals with $m > 1$ and $n > 1$. Then there exists an integer constant $c \geq 0$ (that only depends on A) such that all the following conditions $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$, and $\mathcal{C}_4$ hold.

- $\mathcal{C}_1$: $\forall \upsilon \in Left(\mathbb{S}^n_m, 0)\ \exists \omega \in Left(\mathbb{S}^n_m, h)$ *for some* $-c \leq h \leq c$ *such that* $A\omega = \upsilon$
- $\mathcal{C}_2$: $\forall \upsilon \in Right(\mathbb{S}^n_m, 0)\ \exists \omega \in Right(\mathbb{S}^n_m, h)$ *for some* $-c \leq h \leq c$ *such that* $A\omega = \upsilon$
- $\mathcal{C}_3$: $\forall \upsilon \in Left(\mathbb{S}^n_m, 0)$, $A\upsilon \in Left(\mathbb{S}^n_m, h)$ *for some* $-c \leq h \leq c$
- $\mathcal{C}_4$: $\forall \upsilon \in Right(\mathbb{S}^n_m, 0)$, $A\upsilon \in Right(\mathbb{S}^n_m, h)$ *for some* $-c \leq h \leq c$

Proof: It is an immediate consequence of the fact that $\mathcal{F}$ is open and, hence, it is both left and right closing (see [8]). □

We now state the result that is the heart of our work, i.e., providing an easy to check characterization of positive expansivity for LCA over $(\mathbb{Z}/p\mathbb{Z})^n$. Since its proof is very long, we place it in Section IV.

Theorem 1: Let $\mathcal{F}$ be any LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ where p and n are any two naturals such that p is prime and $n > 1$. The LCA $\mathcal{F}$ is positively expansive if and only if the matrix associated with $\mathcal{F}$ is expansive.

A. AN EASY TO CHECK CHARACTERIZATION OF POSITIVE EXPANSIVITY FOR LCA OVER $(\mathbb{Z}/p^k\mathbb{Z})^n$

The following Theorem extends the characterization result provided by Theorem 1 from LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ to LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$.

Theorem 2: Let $\mathcal{G}$ be any LCA over $(\mathbb{Z}/p^k\mathbb{Z})^n$ and let $B \in \mathbb{L}^{n\times n}_{p^k}$ be the matrix associated with $\mathcal{G}$, where p, k, n are any three naturals such that p is prime, $k > 1$, and $n > 1$. The LCA $\mathcal{G}$ is positively expansive if and only if the LCA $\mathcal{F}$ over $(\mathbb{Z}/p\mathbb{Z})^n$ having A as associated matrix is too, where $A = (B \bmod p) \in \mathbb{L}^{n\times n}_p$. Equivalently, $\mathcal{G}$ is positively expansive if and only if the matrix $B \bmod p$ is expansive.

Proof: We start to prove that if $\mathcal{G}$ is positively expansive then $\mathcal{F}$ is too. Let us suppose that $\mathcal{F}$ is not positively expansive and the first condition from Lemma 2 holds, i.e., there exists $\upsilon \in Left(\mathbb{S}^n_p, 0)$ with $\upsilon \neq 0$ such that $A^\ell\upsilon \in Left^*(\mathbb{S}^n_p, s)$ for every natural $\ell > 0$, where $s > 0$ is some integer constant depending on $\mathcal{F}$ (the proof is symmetric if one supposes that the second condition holds). Set $\omega = p^{k-1}\upsilon$. Clearly, $\omega \in Left(\mathbb{S}^n_{p^k}, 0)$ and $\omega \neq 0$. Since B can be written as $A + pN$ for some matrix $N \in \mathbb{L}^{n\times n}_{p^{k-1}}$, it holds that for every natural $\ell > 0$

$$B^\ell\omega = (A + pN)^\ell p^{k-1}\upsilon = p^{k-1}A^\ell\upsilon,$$

where all the sums and products of coefficients of the Laurent polynomials/series inside the previous equalities are now meant in $\mathbb{Z}_{p^k}$. Hence, although $A \in \mathbb{L}^{n\times n}_p$ and $\upsilon \in \mathbb{S}^n_p$, in general $A^\ell\upsilon$ now belongs to $\mathbb{S}^n_{p^k}$ instead of $\mathbb{S}^n_p$ and, as a consequence, we can not immediately conclude that $B^\ell\omega = p^{k-1}A^\ell\upsilon \in Left^*(\mathbb{S}^n_{p^k}, s)$ immediately follows just from the hypothesis as it is, i.e., $A^\ell\upsilon \in Left^*(\mathbb{S}^n_p, s)$ when $A^\ell\upsilon$ is considered as an element of $\mathbb{S}^n_p$. However, since $A^\ell\upsilon \in \mathbb{S}^n_{p^k}$ can be written as $(A^\ell\upsilon) \bmod p + p\omega'$ for some $\omega' \in \mathbb{S}^n_{p^{k-1}}$ and, by hypothesis, $(A^\ell\upsilon) \bmod p \in Left^*(\mathbb{S}^n_p, s)$, we get that $B^\ell\omega = p^{k-1}[(A^\ell\upsilon) \bmod p + p\omega'] = p^{k-1}[(A^\ell\upsilon) \bmod p] \in Left^*(\mathbb{S}^n_{p^k}, s)$ for every natural $\ell > 0$. Therefore, by Lemma 2, $\mathcal{G}$ is not positively expansive.

We now prove that if $\mathcal{F}$ is positively expansive then $\mathcal{G}$ is too. Let us suppose that $\mathcal{G}$ is not positively expansive and the first condition from Lemma 2 holds, i.e., there exists $\omega \in Left(\mathbb{S}^n_{p^k}, 0)$ with $\omega \neq 0$ such that $B^\ell\omega \in Left^*(\mathbb{S}^n_{p^k}, s)$ for every natural $\ell > 0$, where $s > 0$ is some integer constant depending on $\mathcal{G}$ (again, the proof is symmetric if one supposes that the second condition holds). We deal with the following two mutually exclusive cases.

> If there is no ω' such that $\omega = p\omega'$, then set $\upsilon = \omega \bmod p$. Clearly, $\upsilon \neq 0$ and $\upsilon \in Left(\mathbb{S}^n_p, h)$ for some integer $h \leq 0$. Moreover, it holds that $A^\ell\upsilon = (B \bmod p)^\ell(\omega \bmod p) = (B^\ell\omega) \bmod p \in Left^*(\mathbb{S}^n_p, s)$ for every natural $\ell > 0$.
>
> Otherwise, let $j \in \{1, \ldots, k-1\}$ and $\omega' \in \mathbb{S}^n_{p^k}$ be such that $\omega = p^j\omega'$, where j is the largest natural such that all the coefficients of the n Laurent series forming ω are multiple of p^j. Set $\upsilon = \omega' \bmod p$. Clearly, $\upsilon \neq 0$ and $\upsilon \in Left(\mathbb{S}^n_p, h)$ for some integer $h \leq 0$. Since $p^jB^\ell\omega' = B^\ell\omega \in Left^*(\mathbb{S}^n_{p^k}, s)$, either $B^\ell\omega' \in Left^*(\mathbb{S}^n_{p^k}, s)$ or $B^\ell\omega' \notin Left^*(\mathbb{S}^n_{p^k}, s)$ happens, but, in both situations it must hold that $(B^\ell\omega') \bmod p \in Left^*(\mathbb{S}^n_p, s)$. Therefore, it follows that $A^\ell\upsilon = (B \bmod p)^\ell(\omega' \bmod p) = (B^\ell\omega') \bmod p \in Left^*(\mathbb{S}^n_p, s)$ for every natural $\ell > 0$.

In both cases, the first condition of Lemma 2 is satisfied as far as $\mathcal{F}$ is concerned. Thus, $\mathcal{F}$ is not positively expansive and this concludes the proof that $\mathcal{G}$ is positively expansive if and only if $\mathcal{F}$ is positively expansive. By Theorem 1, it follows that $\mathcal{G}$ is positively expansive if and only if the matrix $B \bmod p$ is expansive. □

At this point, we are able to extend the characterization result regarding positive expansivity to the whole class of LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ where m is any natural with $m > 1$.

Corollary 1: Any LCA $\mathcal{F}$ over $(\mathbb{Z}/m\mathbb{Z})^n$ is positively expansive if and only if $A \bmod p_j$ is expansive for every $j \in \{1, \ldots, l\}$, where A is the matrix associated with $\mathcal{F}$ and $p_1, \ldots, p_l$ are all the primes appearing in the prime factor decomposition of m (i.e., $m = p_1^{k_1} \cdots p_l^{k_l}$ is the prime factor decomposition of m).

Proof: For each $j \in \{1, \ldots, l\}$, let $\mathcal{F}_j$ be the LCA over $(\mathbb{Z}/(p_j)^{k_j}\mathbb{Z})^n$ having $(A \bmod (p_j)^{k_j}) \in \mathbb{L}^{n\times n}_{(p_j)^{k_j}}$ as associated matrix. Since $\mathcal{F}$ is positively expansive if and only if every LCA $\mathcal{F}_j$ is too, by Lemma 2 and Theorem 1, it follows that $\mathcal{F}$ is positively expansive if and only if every matrix $(A \bmod p_j) \in \mathbb{L}^{n\times n}_{p_j}$ is expansive. Therefore, the statement is true. □

B. BYPASSING THE PRIME FACTOR DECOMPOSITION OF m IN THE CHARACTERIZATION OF POSITIVE EXPANSIVITY FOR LCA OVER $(\mathbb{Z}/m\mathbb{Z})^n$

The characterization of positively expansive LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ provided by Corollary 1 requires that the prime factor decomposition of m is known. We now illustrate how deciding positive expansivity without decomposing m into prime factors and by only making use of gcd operations.

Let $m = p_1^{k_1} \cdots p_l^{k_l}$ be the prime factor decomposition of m and let A be the matrix associated with a given LCA $\mathcal{F}$ over $(\mathbb{Z}/m\mathbb{Z})^n$. By Corollary 1, $\mathcal{F}$ is positively expansive if and only if both the following conditions are satisfied:

(C1) for every $j \in \{1, \ldots, l\}$ it holds that $\deg^+(\alpha_0 \bmod p_j) > 0$ and $\deg^-(\alpha_0 \bmod p_j) < 0$;

(C2) for every $i \in \{1, \ldots, n-1\}$ it holds that

(C2a) for every $j \in \{1, \ldots, l\}$, $\deg^+(\alpha_0 \bmod p_j) > \deg^+(\alpha_i \bmod p_j)$

and

(C2b) for every $j \in \{1, \ldots, l\}$, $\deg^-(\alpha_0 \bmod p_j) < \deg^-(\alpha_i \bmod p_j)$,

where $\pi(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_{t-1} t^{t-1} + t^n$ is the characteristic polynomial of A.

It is not difficult to see that, by the characterization of positively expansive LCA over $\mathbb{Z}/m\mathbb{Z}$ provided in [9], condition (C1) can be rewritten in an equivalent form as follows:

$$\alpha_0 \in \mathbb{L}_m \text{ is the } 1 \times 1 \text{ matrix associated with a positively expansive LCA over } \mathbb{Z}/m\mathbb{Z},$$

i.e.,

$$\gcd(m, A_1, \ldots, A_r) = \gcd(m, A_{-1}, \ldots, A_{-r}) = 1,$$

where $A_{-r}, \ldots, A_r \in \mathbb{Z}/m\mathbb{Z}$ define α_0. Therefore, (C1) is an efficiently testable condition.

We are now going to provide a method that checks condition (C2) without decomposing m in prime factors and under the assumption that condition (C1) is satisfied. To proceed, for any $a \in \mathbb{Z}/m\mathbb{Z}$ define

$$y_a = \begin{cases} \prod_{j \in \mathcal{P}_a} p_j^{k_j}, & \text{if } \mathcal{P}_a \neq \emptyset \\ 1, & \text{otherwise,} \end{cases}$$

where $\mathcal{P}_a = \{j \in \{1, \ldots, l\} : \gcd(a, p_j) = 1\}$. We emphasize that y_a is the greatest divisor of m having as prime factors all (and only) those prime factors of m that are not prime factors of a. Moreover, y_a can be computed without knowing $p_1, \ldots, p_l$ and $k_1, \ldots, k_l$, i.e., without the need of decomposing m into its prime factors. Indeed, consider the elements of the sequence m_ℓ recursively defined by $m_{\ell+1} = m_\ell / \gcd(m_\ell, a)$, where $m_0 = m$. Clearly, there exists ℓ^* such that $m_{\ell^*+1} = m_{\ell^*}$ and it holds that $y_a = m_{\ell^*+1} = m_{\ell^*}$.

In the sequel, we will deal with how to test condition (C2a) for every $i \in \{1, \ldots, n-1\}$ (the argument regarding condition (C2b) is symmetric). For any $i \in \{0, 1, \ldots, n-1\}$ and any monomial $a_d^{(i)} X^d$ of degree d inside α_i, with a little abuse of notation, let us denote by $y_{i,d}$ the quantity $y_{a_d^{(i)}}$. Clearly, for every $j \in \mathcal{P}_{a_d^{(i)}}$ it holds that $a_d^{(i)} \bmod p_j \neq 0$.

Fix now $i \in \{1, \ldots, n-1\}$. The following procedure to be repeated for every $i \in \{1, \ldots, n-1\}$ tests condition (C2a), i.e., as far as α_i is concerned, it checks whether $\deg^+(\alpha_0 \bmod p_j) > \deg^+(\alpha_i \bmod p_j)$ for every $j \in \{1, \ldots, l\}$. The procedure consists of the following steps:

(S1) Let $a_{d_0}^{(0)} X^{d_0}$ be the monomial of maximum degree inside α_0 with $y_{0,d_0} \neq 1$. If condition (C1) is satisfied then $d_0 > 0$. We stress that $a_{d_0}^{(0)} \bmod p_j \neq 0$ for every $j \in \mathcal{P}_{a_{d_0}^{(0)}}$.

(S2) Consider the monomials $a_d^{(i)} X^d$ of degree $d \geq d_0$ inside α_i (while jump to step (S3.2) if $\deg^+(\alpha_i) < d_0$). For each of such monomials compute $y_{i,d}$ and $g_d = \gcd(y_{0,d_0}, y_{i,d})$.

(S3.1) If $g_d > 1$ for some $d \geq d_0$, it means that there exists $j \in \mathcal{P}_{a_{d_0}^{(0)}} \cap \mathcal{P}_{a_d^{(i)}} \neq \emptyset$ such that $\deg^+(\alpha_0 \bmod p_j) \leq \deg^+(\alpha_i \bmod p_j)$ and, hence, (C2a) is not satisfied.

(S3.2) Otherwise, since $a_{d_0}^{(0)} \bmod p_j \neq 0$ and $a_d^{(i)} \bmod p_j = 0$ for every $j \in \mathcal{P}_{a_{d_0}^{(0)}}$ and every $d \geq d_0$, the inequality inside condition (C2a) holds for every $j \in \mathcal{P}_{a_{d_0}^{(0)}}$. To check if it also holds for every $j \notin \mathcal{P}_{a_{d_0}^{(0)}}$, replace m by $m/y_{0,d_0}$, and, referring to this new value of m, if $m \neq 1$, restart from step (S1) with $(\alpha_0 - a_{d_0}^{(0)} X^{d_0}) \bmod m$ and $\alpha_1 \bmod m$ in place of α_0 and α_1, respectively, inside the new background $\mathbb{Z}/m\mathbb{Z}$. If, on the contrary, $m = 1$, it means that condition (C2a) is satisfied.

C. AN EASY TO CHECK CHARACTERIZATION OF POSITIVE EXPANSIVITY FOR ADDITIVE CA OVER A FINITE ABELIAN GROUP

Finally, we lift the characterization result regarding positive expansivity for LCA over $(\mathbb{Z}/m\mathbb{Z})^n$ to the whole class Additive CA over any finite abelian group. We stress that although the characterization result is stated for Additive CA over $G = \mathbb{Z}/p^{k_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{k_n}\mathbb{Z}$, this is not a restriction. Indeed, any finite abelian group is isomorphic to a direct sum of a certain number of its subgroups (with pairwise coprime cardinality), each of them being as such a G, and an Additive CA over a finite abelian group splits into the direct sum of Additive CA over those subgroups. Hence, the former CA turns out to be positively expansive if and only if all the CA components of that sum are positively expansive.

Theorem 3: Let $\mathcal{F} : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$ be any Additive CA over a finite abelian group G, where $G = \mathbb{Z}/p^{k_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{k_n}\mathbb{Z}$ for some prime p and some non zero naturals $k_1, \ldots, k_n$ with $k_1 \geq k_2 \geq \ldots \geq k_n$. Let $\mathcal{L}$ be the LCA over $\hat{G}$ associated with $\mathcal{F}$ via the embedding Ψ, where $\hat{G} = (\mathbb{Z}/p^{k_1}\mathbb{Z})^n$. It holds that $\mathcal{F}$ is positively expansive if and only if $\mathcal{L}$ is positively expansive if and only if A is expansive, where A is the matrix associated with $\mathcal{L}$.

Proof: We are going to show that $\mathcal{F}$ is positively expansive if and only if $\mathcal{L}$ is too. By Theorem 2, this is enough to conclude that the statement is true.

We start to prove that if $\mathcal{L}$ is positively expansive then $\mathcal{F}$ is too. Let us suppose that $\mathcal{F}$ is not positively expansive. Choose an arbitrary $\varepsilon > 0$. So, there exist $c, c' \in G^{\mathbb{Z}}$ with $c \neq c'$ such that $d(\mathcal{F}^{\ell}(c), \mathcal{F}^{\ell}(c')) \leq \varepsilon$ for every natural ℓ. Consider the two configurations $\Psi(c), \Psi(c') \in \hat{G}^{\mathbb{Z}}$. Clearly, $\Psi(c) \neq \Psi(c')$. Moreover, for every natural ℓ it holds that $d(\mathcal{L}^{\ell}(\Psi(c)), \mathcal{L}^{\ell}(\Psi(c'))) = d(\Psi(\mathcal{F}^{\ell}(c)), \Psi(\mathcal{F}^{\ell}(c'))) = d(\mathcal{F}^{\ell}(c), \mathcal{F}^{\ell}(c')) \leq \varepsilon$. Hence, $\mathcal{L}$ is not positively expansive.

We now prove that if $\mathcal{F}$ is positively expansive then $\mathcal{L}$ is too. Let us suppose that $\mathcal{L}$ is not positively expansive. Choose an arbitrary $\varepsilon > 0$. So, there exist $b, b' \in \hat{G}^{\mathbb{Z}}$ with $b \neq b'$ such that $d(\mathcal{L}^{\ell}(b), \mathcal{L}^{\ell}(b')) \leq \varepsilon$ for every natural ℓ. Let *min* be the minimum natural such that $p^{min} \cdot (b - b') \neq 0$ and $p^{min+1} \cdot (b - b') = 0$. We get that $p^{min} \cdot b, p^{min} \cdot b' \in \Psi(G^{\mathbb{Z}})$ and $p^{min} \cdot b \neq p^{min} \cdot b'$. Let $c, c' \in G^{\mathbb{Z}}$ be the two configurations such that $\Psi(c) = p^{min} \cdot b$ and $\Psi(c') = p^{min} \cdot b'$. Clearly, $c \neq c'$. For every natural ℓ it holds that $d(\mathcal{F}^{\ell}(c), \mathcal{F}^{\ell}(c')) = d(\Psi(\mathcal{F}^{\ell}(c)), \Psi(\mathcal{F}^{\ell}(c'))) = d(\mathcal{L}^{\ell}(\Psi(c)), \mathcal{L}^{\ell}(\Psi(c'))) = d(\mathcal{L}^{\ell}(b), \mathcal{L}^{\ell}(b')) \leq \varepsilon$. Hence $\mathcal{F}$ is not positively expansive. □

IV. PROOF OF THEOREM 1

We now recall some useful notions and known fact from abstract algebra. In the sequel, the standard acronyms PID and UFD stand for principal ideal domain and unique factorization domain, respectively.

Let $\mathbb{P}$ be PID and let $A \in \mathbb{P}^{n\times n}$. The *elementary divisors*, or *invariants*, or *invariant factors* associated with A are the elements $a_1, \ldots, a_n \in \mathbb{P}$ defined as follows: $\forall i \in \{1, \ldots, n\}$, $a_i = \Delta_i(A)/\Delta_{i-1}(A)$, where $\Delta_i(A)$ is the greatest common divisor of the i-minors of A and $\Delta_0(A) = 1$.

The companion matrix of a monic polynomial $\pi(t) = \alpha_0 + \ldots + \alpha_{n-1}t^{n-1} + t^n$ is

$$C_\pi = \begin{pmatrix} 0 & 0 & 0 & -\alpha_0 \\ 1 & \cdots & 0 & -\alpha_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & -\alpha_{n-1} \end{pmatrix}.$$

A matrix C is in rational canonical form if it is block diagonal

$$C = \begin{pmatrix} C_{\pi_1} & \mathbb{O} & \cdots & \mathbb{O} \\ \mathbb{O} & C_{\pi_2} & \cdots & \mathbb{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{O} & \mathbb{O} & \cdots & C_{\pi_s} \end{pmatrix},$$

where each C_{π_i} is the companion matrix of some monic polynomial π_i of non null degree and π_i divides π_j for $i \leq j$. It is well-known that if $A \in \mathbb{F}^{n\times n}$ is any matrix where $\mathbb{F}$ is a field all the following facts hold:

- A is similar to a unique matrix in rational canonical form and this latter is called the rational canonical form of A;
- the monic polynomials $\pi_1, \ldots, \pi_s$ defining the blocks of the rational canonical form of A are the nonconstant invariant factors of $tI - A$;
- $\chi_A(t) = \prod_{i=1}^{s} \pi_i(t)$, where π_s is the minimal polynomial of A;
- there exist $v_1, \ldots, v_s \in \mathbb{F}^n$ such that

$$\{v_1, Av_1, \ldots, A^{d_1-1}v_1, \ldots, v_s, Av_s, \ldots, A^{d_s-1}v_s\}$$

is a basis of $\mathbb{F}^n$ with respect to which A becomes in rational canonical form C, i.e., $A = P^{-1}CP$, where $d_i = \deg(\pi_i)$ and P is the matrix having the elements of that basis as columns.

We now report the following known result which will be very useful in the sequel (see [10, Proposition 1], for instance).

Lemma 4: Let U be a UFD and let $\mathbb{F}_U$ be the field of fractions of U. For any monic polynomials $\pi \in U[t]$ and $\rho, \tau \in \mathbb{F}_U[t]$, it holds that if $\pi = \rho \cdot \tau$ then $\rho, \tau \in U[t]$.

The following is an important consequence of Lemma 4.

Lemma 5: Let U be a UFD and let $\mathbb{F}_U$ be the field of fractions of U. Let $A = U^{n\times n}$ and let $\pi_1, \ldots, \pi_s \in \mathbb{F}_U[t]$ be the invariant factors of $tI - A$ when A is considered as an element of $\mathbb{F}_U^{n\times n}$. Then, for every $i \in \{1, \ldots, s\}$ it holds that $\pi_i \in U[t]$.

Proof: Since $\pi_1, \ldots, \pi_s, \chi_A$ are all monic and $\chi_A(t) = \prod_{i=1}^{s} \pi_i(t) \in U[t]$, by a repeated application of Lemma 4, we get that every $\pi_i \in U[t]$. □

We now deal with the algebraic structures of our interest, namely, the PID $\mathbb{L}_p$ and the UFD $\mathbb{L}_p[t]$. Clearly, $\mathbb{L}_p$ is also an UFD, but, since $\mathbb{L}_p$ is not a field, $\mathbb{L}_p[t]$ is not a PID, while $\mathbb{F}_p[t]$ is, where $\mathbb{F}_p$ is the field of fraction of $\mathbb{L}_p$. Therefore, we can not refer to invariant factors when the involved set is $\mathbb{L}_p[t]$, while we can as far as $\mathbb{F}_p[t]$ is concerned.

Lemma 6: For any matrix $A \in \mathbb{L}_p^{n\times n}$ with $\det(A) \neq 0$ there exist two matrices $Q, C \in \mathbb{L}_p^{n\times n}$ such that $\det(Q) \neq 0$, C is in rational canonical form, $QA = CQ$, and $\chi_A = \chi_C$.

Proof: Choose arbitrarily a matrix $A \in \mathbb{L}_p^{n\times n}$. Cleary, it holds that $A \in \mathbb{F}_p^{n\times n}$, where $\mathbb{F}_p$ is the field of fractions of $\mathbb{L}_p$. Hence, there exist $v_1, \ldots, v_s \in \mathbb{F}^n$ such that, $A = P^{-1}CP$, $C \in \mathbb{F}_p^{n\times n}$ is the matrix in canonical rational form, the blocks of which are defined by the invariant factors $\pi_1, \ldots, \pi_s \in \mathbb{F}_p[t]$ of $tI - A$, and P is the matrix having the elements of the basis $\{v_1, Av_1, \ldots, A^{d_1-1}v_1, \ldots, v_s, Av_s, \ldots, A^{d_s-1}v_s\}$ of $\mathbb{F}_p^n$ as columns, where $d_i = \deg(\pi_i)$. Clearly, $\chi_A = \chi_C$.

Let $\alpha \in \mathbb{L}_p$ be such that $v_i' = \alpha v_i \in \mathbb{L}_p$ for each $i \in \{1, \ldots, s\}$. Set $Q = \alpha P$. It is clear that $Q \in \mathbb{L}_p^{n\times n}$, as desired. Furthermore, by Lemma 5, it follows that $C \in \mathbb{L}_p^{n\times n}$, too. Moreover, we get that $A = P^{-1}CP = \alpha\alpha^{-1}P^{-1}CP = \alpha^{-1}P^{-1}C\alpha P = Q^{-1}CQ$. Therefore, $QA = CQ$ and this concludes the proof. □

Lemma 7: For any $A, B, Q \in \mathbb{L}_p^{n\times n}$ such that $\det(Q) \neq 0$ and $AQ = QB$ it holds that the LCA $\mathcal{F}$ over $(\mathbb{Z}/p\mathbb{Z})^n$ having A as associated matrix is positively expansive if and only if the LCA $\mathcal{G}$ over $(\mathbb{Z}/p\mathbb{Z})^n$ having B as associated matrix is, too.

Proof: First of all, it is easy to see that $A^\ell Q = QB^\ell$ for every natural $\ell > 0$. Moreover, $\det(A) = 0$ if and only if $\det(B) = 0$. So, the thesis turns out to be trivially true if $\det(A) = \det(B) = 0$. Therefore, in the sequel of the proof, we will assume that $\det(A) \neq 0$ and $\det(B) \neq 0$, i.e., both $\mathcal{F}$ and $\mathcal{G}$ are surjective.

We now start to prove that if $\mathcal{F}$ is positively expansive then $\mathcal{G}$ is too. Suppose that $\mathcal{G}$ is not positively expansive and the first condition from Lemma 2 holds, i.e., there exists $\upsilon \in Left(\mathbb{S}_p^n, 0)$ with $\upsilon \neq 0$ such that $B^\ell \upsilon \in Left^*(\mathbb{S}_p^n, s)$ for every natural $\ell > 0$, where $s > 0$ is some integer constant depending on $\mathcal{G}$ (the proof is symmetric if one supposes that the second condition holds). Since Q is the matrix associated with a surjective LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ condition $\mathcal{C}_3$ of Lemma 3 is satisfied as far as Q is concerned. Hence, setting $\omega = Q\upsilon$, for some natural constant $c > 0$ depending on Q and some integer h with $-c \leq h \leq c$, it holds that $A^\ell \omega = QB^\ell \upsilon \in Left^*(\mathbb{S}_p^n, h)$ for every natural $\ell > 0$. Clearly, $\omega \neq 0$ since $det(Q) \neq 0$. In addition, it holds that $\omega \in Left(\mathbb{S}_p^n, h')$ for some integer h'. Thus, it follows that $\mathcal{F}$ is not positively expansive.

We now prove that if $\mathcal{G}$ is positively expansive then $\mathcal{F}$ is too. Assume that $\mathcal{F}$ is not positively expansive and the first condition from Lemma 2 holds, i.e., there exists $\upsilon \in Left(\mathbb{S}_p^n, 0)$ with $\upsilon \neq 0$ such that $A^\ell \upsilon \in Left^*(\mathbb{S}_p^n, s)$ for every natural $\ell > 0$, where $s > 0$ is some integer constant depending on $\mathcal{G}$ (again, the proof is symmetric if one supposes that the second condition holds). Since Q is the matrix associated with a surjective LCA over $(\mathbb{Z}/p\mathbb{Z})^n$, condition $\mathcal{C}_1$ of Lemma 3 is satisfied as far as Q is concerned. Thus, for some natural constant $c > 0$ depending on Q and some integer h with $-c \leq h \leq c$, there exists $\omega \in Left(\mathbb{S}_p^n, h)$ such that $Q\omega = \upsilon$. Clearly, $\omega \neq 0$ since $\upsilon \neq 0$. Furthermore, $QB^\ell \omega = A^\ell Q\omega = A^\ell \upsilon \in Left^*(\mathbb{S}_p^n, s)$ for every natural $\ell > 0$. Therefore, there exists an integer constant $s' > s > 0$ such that $B^\ell \omega \in Left^*(\mathbb{S}_p^n, s')$ for every natural $\ell > 0$. So, by Lemma 2, $\mathcal{G}$ is not positively expansive and this concludes the proof. □

In the sequel, with an abuse of notation, $\deg^+(\varphi)$ stands for $\deg^+(\alpha) - \deg^+(\beta)$ for any fraction $\varphi = \alpha/\beta \in \mathbb{F}_p$ with $\alpha, \beta \in \mathbb{L}_p$ and $\alpha, \beta \neq 0$, where $\mathbb{F}_p$ is the field of fractions of $\mathbb{L}_p$.

Lemma 8: Let $\upsilon_1, \ldots, \upsilon_n$ be arbitrary elements of $\mathbb{L}_p$, where p and n are any two naturals such that p is prime and $n > 1$, and let $\varphi_1, \ldots, \varphi_n$ be arbitrary elements of $\mathbb{F}_p$ such that $\max\{\deg^+(\varphi_1), \ldots, \deg^+(\varphi_n)\} \geq 0$. Let min be the minimum index such that $\deg^+(\varphi_{min}) = \max\{\deg^+(\varphi_1), \ldots, \deg^+(\varphi_n)\}$. Regarding the sequence

$$\{\upsilon_1, \ldots, \upsilon_n, \ldots, \upsilon_j, \ldots\} \subset \mathbb{F}_p,$$

where, for each $j > n$,

$$\upsilon_j = \varphi_n \upsilon_{j-1} + \ldots + \varphi_1 \upsilon_{j-n}.$$

call pick any natural $J > 0$ such that $deg^+(\upsilon_j) \leq deg^+(\upsilon_J)$ for every natural j with $0 < j < J$. It holds that for any pick J there exists a pick $J' \in \{J+1, \ldots, J+n-min+1\}$. In particular, for any pick the number of positions within which there is a further pick does not depend on the values of the initial elements $\upsilon_1, \ldots, \upsilon_n$ of the sequence.

Proof: Clearly, the set of picks is non empty since $1, \ldots, n$ are picks. Let J be any pick. If there exists $j \in \{J+1, \ldots, J+n-min\}$ such that $deg^+(\upsilon_j) \geq deg^+(\upsilon_J)$, necessarily there must be a further pick inside the integer interval $\{J+1, \ldots, J+n-min\}$. Otherwise, it holds that $deg^+(\upsilon_j) < deg^+(\upsilon_J)$ for every $j \in \{J+1, \ldots, J+n-min\}$ and, since

$$\begin{aligned} \deg^+(\upsilon_{J+n-min+1}) &= \deg^+(\upsilon_J \varphi_{min}) \\ &= \deg^+(\upsilon_J) + \deg^+(\varphi_{min}) \\ &\geq \deg^+(\upsilon_J), \end{aligned}$$

it follows that the natural $J + n - min + 1$ turns out to be a pick. □

The following result is the heart of our work. It provides a decidable characterization of positively expansive LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ with associated matrix such that its transpose is in a rational canonical form consisting of only one block.

Lemma 9: Let $A \in \mathbb{L}_p^{n\times n}$ be the matrix such that its transpose A^T is the companion matrix of any monic polynomial $-\alpha_0 + \ldots - \alpha_{n-1}t^{n-1} + t^n$ from $\mathbb{L}_p[t]$, i.e.,

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{n-2} & \alpha_{n-1} \end{pmatrix}, \tag{2}$$

where p and n are any two naturals such that p is prime and $n > 1$, and let $\mathcal{F}$ be the LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ having A as associated matrix. The LCA $\mathcal{F}$ is positively expansive if and only if A is expansive if and only if A^T is expansive if and only if $\alpha_0 + \ldots + \alpha_{n-1}t^{n-1} + t^n$ is expansive.

Proof: It is clear that the matrix A is expansive if and only if its transpose A^T is expansive if and only if $\chi_A(t) = -\alpha_0 + \ldots - \alpha_{n-1}t^{n-1} + t^n$ is expansive if and only if $\alpha_0 + \ldots + \alpha_{n-1}t^{n-1} + t^n$ is expansive. Since $\mathcal{F}$ is surjective if and only if $-\alpha_0 \neq 0$, the thesis turns out to be trivially true if $\alpha_0 = 0$. Hence, in the sequel of the proof we can assume that $\alpha_0 \neq 0$.

We start to prove that if A is expansive then $\mathcal{F}$ is positively expansive. For a sake of argument, suppose that A is expansive but $\mathcal{F}$ is not positively expansive and, in particular, the first condition from Lemma 2 holds, i.e., there exists $\upsilon = (\upsilon_1, \ldots, \upsilon_n) \in Left(\mathbb{S}_p^n, 0)$ with $\upsilon \neq 0$ such that $A^\ell \upsilon \in Left^*(\mathbb{S}_p^n, s)$ for every natural $\ell > 0$, where $s > 0$ is some integer constant depending on $\mathcal{F}$ (the proof is symmetric if one supposes that the second condition holds). Consider the infinite sequence

$$\{\upsilon_1, \ldots, \upsilon_n, \upsilon_{1+n}, \ldots, \upsilon_{\ell+n}, \ldots\},$$

where $\upsilon_{\ell+n} = \alpha_0 \upsilon_\ell + \ldots + \alpha_{n-1}\upsilon_{\ell+n-1}$ for each natural $\ell > 0$. Clearly, it holds that $A^\ell \upsilon = (\upsilon_{\ell+1}, \ldots, \upsilon_{\ell+n})$ for each

$\ell > 0$. The first condition from Lemma 2 ensures that there exists an integer $s' \leq s$ such that $\deg^+(\upsilon_j) \leq s'$ for every natural $j > 0$ and $\deg^+(\upsilon_j) = s'$ for at least one $j > 0$. Let $min > 0$ be the minimum index such that $\deg^+(\upsilon_{min}) = s'$. Since

$$\upsilon_{min+n} = \alpha_0\upsilon_{min} + \ldots + \alpha_{n-1}\upsilon_{min+n-1},$$

A is expansive, and p is prime, we get $\deg^+(\upsilon_{min+n}) = \deg^+(\alpha_0\upsilon_{min}) > s'$, which contradicts that $\deg^+(\upsilon_j) \leq s'$ for every natural $j > 0$.

We now prove that if $\mathcal{F}$ is positively expansive then A is expansive. Set

$$\varphi_n = -\frac{\alpha_1}{\alpha_0}, \varphi_{n-1} = -\frac{\alpha_2}{\alpha_0}, \ldots, \varphi_2 = -\frac{\alpha_{n-1}}{\alpha_0}, \varphi_1 = \frac{1}{\alpha_0}.$$

Assume that A is not expansive, i.e., equivalently, $\alpha_0 + \ldots + \alpha_{n-1}t^{n-1} + t^n$ is not expansive, and condition (i) from Definition 2 does not hold, i.e., either $\deg^+(\alpha_0) \leq 0$ or $\deg^+(\alpha_0) \leq \max\{\deg^+(\alpha_1), \ldots, \deg^+(\alpha_{n-1})\}$ (the proof is symmetric if one supposes that condition (ii) does not hold). In both cases we get that $\max\{\deg^+(\varphi_1), \ldots, \deg^+(\varphi_n)\} \geq 0$. Let $\mathbb{F}_p$ be the field of fraction of $\mathbb{L}_p$. For any $\upsilon = (\upsilon_1, \ldots, \upsilon_n) \in \mathbb{F}_p^n$ define the sequence

$$\{\upsilon_1, \ldots, \upsilon_n, \ldots, \upsilon_j, \ldots\},$$

where, for each $j > n$,

$$\upsilon_j = \varphi_n\upsilon_{j-1} + \varphi_{n-1}\upsilon_{j-2} + \cdots + \varphi_2\upsilon_{j-n+1} + \varphi_1\upsilon_{j-n} \in \mathbb{F}_p.$$

We emphasize that $A(\upsilon_j, \ldots, \upsilon_{j-n+1}) = (\upsilon_{j-1}, \ldots, \upsilon_{j-n})$. The hypothesis of Lemma 8 are satisfied and, hence, for every natural j the integer interval $\{js + 1, \ldots, (j + 1)s\}$ contains a pick, where $s = n - min + 1$ (with min as in Lemma 8). We stress that s does not depend on $(\upsilon_1, \ldots, \upsilon_n)$. For every natural $\ell > 0$, we are now going to exhibit an integer $d^{(\ell)}$ and an element $\upsilon^{(\ell)} \in Left(\mathbb{L}_p^n, d^{(\ell)})$ such that $A^{\ell'}\upsilon^{(\ell)} \in Left^*(\mathbb{L}_p^n, d^{(\ell)})$ for each natural $\ell' \leq \ell$. By Lemma 2, this is enough to state that $\mathcal{F}$ is not positively expansive and this concludes the proof.

So, to proceed, choose an arbitrary natural $\ell > 0$ and let h be such that $hs + 1 > \ell + n$. We know that $\{hs + 1, \ldots, (h + 1)s\}$ contains at least one pick whatever the first n values $\upsilon_1, \ldots, \upsilon_n$ of the above sequence are (while the specific value of a pick inside that interval depends on the values of $\upsilon_1, \ldots, \upsilon_n$). Consider now

$$(\upsilon_1, \ldots, \upsilon_n) = \left((\alpha_0)^{h'}, \ldots, (\alpha_0)^{h'}\right),$$

where $h' = (h + 1)s$. Regarding the above sequence when its first n elements are just the components of such $(\upsilon_1, \ldots, \upsilon_n)$, let J be the value of a pick inside $\{hs + 1, \ldots, (h + 1)s\}$. Set $\upsilon^{(\ell)} = (\upsilon_J, \ldots, \upsilon_{J-n+1})$ and let $d^{(\ell)} = \deg^+(\upsilon^{(\ell)}) = \deg^+(\upsilon_J)$. At this point, we are able to state that all the following facts hold:

- $\upsilon_j \in \mathbb{L}_p$ for each natural j with $0 < j \leq h'$ and, hence, $A^j(\upsilon_{h'}, \ldots, \upsilon_{h'-n+1}) \in \mathbb{L}_p^n$ for each natural j with $0 \leq j \leq h' - n$;
- in particular, $\upsilon_J \in \mathbb{L}_p$ and $A^{\ell'}\upsilon^{(\ell)} \in \mathbb{L}_p^n$ for each natural $\ell' \leq \ell$ (since $\ell + n < hs + 1 \leq J \leq h'$);
- moreover, $\upsilon^{(\ell)} \in Left(\mathbb{L}_p^n, d^{(\ell)})$;
- finally, $A^{\ell'}\upsilon^{(\ell)} \in Left^*(\mathbb{L}_p^n, d^{(\ell)})$ for each natural $\ell' \leq \ell$ (since J is a pick);

In this way an integer $d^{(\ell)}$ and an element $\upsilon^{(\ell)}$ with the desired property have been exhibited. □

Lemma 10: Let $A \in \mathbb{L}_p^{n\times n}$ be the matrix such that its transpose A^T is the companion matrix of any monic polynomial $-\alpha_0 + \ldots - \alpha_{n-1}t^{n-1} + t^n$ from $\mathbb{L}_p[t]$, where p and n are any two naturals such that p is prime and $n > 1$, and let $\mathcal{F}$ be the LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ having A as associated matrix. The LCA $\mathcal{F}$ is positively expansive if and only if the LCA $\mathcal{G}$ over $(\mathbb{Z}/p\mathbb{Z})^n$ having A^T as associated matrix is positively expansive.

Proof:

Clearly, A is as in (2). It holds that $A^TQ = QA$, where

$$Q = \begin{pmatrix} -\alpha_1 & -\alpha_2 & \cdots & -\alpha_{n-1} & 1 \\ -\alpha_2 & -\alpha_3 & \iddots & 1 & 0 \\ \vdots & \iddots & \iddots & \iddots & \vdots \\ -\alpha_{n-1} & 1 & \iddots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix} \in \mathbb{L}_p^{n\times n}.$$

Since $\det(Q) \neq 0$, the thesis directly follows from Lemma 7. □

We now prove that the decidable characterization of positive expansivity provided by Lemma 9 also holds also in a more general situation, namely, for LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ with associated matrix that is in a rational canonical form possibly consisting of more than one block.

Lemma 11: Let $C \in \mathbb{L}_p^{n\times n}$ be any matrix in rational canonical form, where p and n are any two naturals such that p is prime and $n > 1$, and let $\mathcal{G}$ be the LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ having C as associated matrix. The LCA $\mathcal{G}$ is positively expansive if and only if C is expansive.

Proof: Let $C_{\pi_1} \in \mathbb{L}_p^{n_1\times n_1}, \ldots, C_{\pi_s} \in \mathbb{L}_p^{n_s\times n_s}$ with $n_1 + \ldots + n_s = n$ be the diagonal blocks inside C, where each π_i is the monic polynomial defining C_{π_i}, i.e., C_{π_i} is the companion matrix of π_i. Since $\chi_C(t) = \Pi_{i=1}^s \pi_i(t)$ and $\mathcal{G}$ is just the product $\mathcal{G}_1 \times \ldots \times \mathcal{G}_s$, where each $\mathcal{G}_i$ is the LCA over $(\mathbb{Z}/p\mathbb{Z})^{n_i}$ having $C_{\pi_i} \in \mathbb{L}_p^{n_i\times n_i}$ as associated matrix, it follows that $\mathcal{G}$ is positively expansive if and only if every $\mathcal{G}_i$ is positively expansive if and only if, by Lemma 9 and 10, every C_{π_i} is expansive, i.e., by Definition 2, if and only if every π_i is expansive, i.e., by Lemma 1, if and only if χ_C is expansive, i.e., if and only if C is expansive. □

We are now able to prove Theorem 1.

Proof of Theorem 1: Let $A \in \mathbb{L}_p^{n\times n}$ be the matrix associated with $\mathcal{F}$. By Lemma 6, there exist two matrices $Q, C \in \mathbb{L}_p^{n\times n}$ such that $\det(Q) \neq 0$, C is in rational canonical form, $QA = CQ$, and $\chi_A = \chi_C$. Let $\mathcal{G}$ be the LCA over $(\mathbb{Z}/p\mathbb{Z})^n$ having C as associated matrix. By Lemma 7, $\mathcal{F}$ is positively expansive if and only if $\mathcal{G}$ is positively expansive,

i.e., by Lemma 11, if and only if C is expansive, i.e., since $\chi_A = \chi_C$, if and only if A is expansive. □

V. CONCLUSION

We provided an easy to check algebraic characterization of positive expansivity for Additive CA over a finite abelian group. Besides having a theoretical value, this characterization turns out to be useful for designing proper applications based on these CA and where a condition of strong chaos is required. Providing (efficient) algorithms that, as far as such CA are concerned, decide other meaningful dynamical properties such as strong transitivity or compute some useful quantities as topological entropy is an important step for further research 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 dynamical properties for multidimensional Additive CA will be certainly useful in many applications involving multidimensional data.

REFERENCES

[1] P. Béaur and J. Kari, "Decidability in group shifts and group cellular automata," in *Proc. 45th Int. Symp. Math. Found. Comput. Sci. (MFCS)*, J. Esparza and D. Král, Eds. Prague, Czech Republic: Schloss Dagstuhl-Leibniz-Zentrum für Informatik, vol. 170, Aug. 2020, p. 12.

[2] T. Ceccherini-Silberstein and M. Coornaert, "On the reversibility and the closed image property of linear cellular automata," *Theor. Comput. Sci.*, vol. 412, nos. 4–5, pp. 300–306, Feb. 2011.

[3] A. Dennunzio, E. Formenti, D. Grinberg, and L. Margara, "Decidable characterizations of dynamical properties for additive cellular automata over a finite Abelian group with applications to data encryption," *Inf. Sci.*, vol. 563, pp. 183–195, Jul. 2021.

[4] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems* (Addison-Wesley Advanced Book Program). Reading, MA, USA: Addison-Wesley, 1989.

[5] P. D. Lena, "Decidable properties for regular cellular automata," in *Proc. 4th IFIP Int. Conf. Theor. Comput. Sci. (TCS)*, G. Navarro, L. E. Bertossi, and Y. Kohayakawa, Eds. Santiago, CHL, USA: Springer, vol. 209, 2006, pp. 185–196.

[6] J. Kari, "Rice's theorem for the limit sets of cellular automata," *Theor. Comput. Sci.*, vol. 127, no. 2, pp. 229–254, May 1994.

[7] B. Kitchens and K. Schmidt, "Automorphisms of compact groups," *Ergodic Theory Dyn. Syst.*, vol. 9, pp. 691–735, Sep. 1989.

[8] P. Kůrka, "Topological and symbolic dynamics," Cours Spécialisés. Société Mathématique de France, 2004, vol. 11. [Online]. Available: https://smf.emath.fr/publications/dynamique-topologique-et-symbolique

[9] G. Manzini and L. Margara, "A complete and efficiently computable topological classification of D-dimensional linear cellular automata over Zm," *Theor. Comput. Sci.*, vol. 221, nos. 1–2, pp. 157–177, Jun. 1999.

[10] M. Mazur. *Polynomials Over UFD's*. Accessed: Jun. 15, 2023. [Online]. Available: https://people.math.binghamton.edu/mazur/teach/gausslemma.pdf

[11] S. Nandi, B. K. Kar, and P. Pal Chaudhuri, "Theory and applications of cellular automata in cryptography," *IEEE Trans. Comput.*, vol. 43, no. 12, pp. 1346–1357, Dec. 1994.

[12] X. K. Phung, "Stable finiteness of twisted group rings and noisy linear cellular automata," *Can. J. Math.*, pp. 1–20, May 2023.

[13] C. F. Rubio, L. H. Encinas, S. H. White, Á. M. del Rey, and G. R. Sánchez, "The use of linear hybrid cellular automata as pseudo random bit generators in cryptography," *Neural Parallel Sci. Comp.*, vol. 12, no. 2, pp. 175–192, 2004.

ALBERTO DENNUNZIO received the M.Sc. and Ph.D. degrees in computer science from the University of Milano, in 1999 and 2004, respectively. He is currently an Associate Professor with the Informatics, System and Communication Department, University of Milano-Bicocca, Italy. His research interests include complex systems, cellular automata, including the classes of linear, higher-order, non-uniform, and asynchronous CA, along with their long-term behavior which is understood through the investigation of properties, such as stability, instability, chaos, periodic behaviors, reachability, and reversibility. In particular, formal models for describing and simulating complex systems are considered and studied.

ENRICO FORMENTI received the Ph.D. degree from Ecole Normale Supérieure de Lyon, in 1998. He is currently a Professor in computer science with Université Côte d'Azur, France. Since 2003, he has been a Full Professor with Université Nice Sophia Antipolis. His main research interests include discrete dynamical systems, chaos, tilings, and complex systems in general, but he is also interested in computational complexity, computability, and unconventional models of computation.

LUCIANO MARGARA received the Laurea degree in scienze dell'informazione and the Dottorato di Ricerca in Informatica (Ph.D.) degree in computer science from the University of Pisa, in 1991 and 1995, respectively. He is currently a Professor in computer science with the University of Bologna, Italy. He joined the University of Bologna, in 1995 (a Research Associate, from 1995 to 2000, and an Associate Professor, from 2000 to 2005). His research interests include discrete time dynamical systems, optical networks, computational complexity, and bioinformatics.

Open Access funding provided by 'Università degli Studi di Milano Bicocca' within the CRUI CARE Agreement