ELSEVIER

Theoretical Computer Science 221 (1999) 157–177

Theoretical Computer Science

www.elsevier.com/locate/tcs

A complete and efficiently computable topological classification of D-dimensional linear cellular automata over Z_m [☆]

Giovanni Manzini [a,b,*] Luciano Margara [c,1]

[a] *Dipartimento di Scienze e Tecnologie Avanzate, Università del Piemonte Orientale, Via Cavour 84, I-15100 Alessandria, Italy*
[b] *IMC-CNR, Via S. Maria 46, I-56126 Pisa, Italy*
[c] *Dipartimento Scienze dell'Informazione, Università di Bologna, Mura Anteo Zamboni 7, I-40127 Bologna, Italy*

Abstract

We study the dynamical behavior of D-dimensional linear cellular automata over Z_m. We provide easy-to-check necessary and sufficient conditions for a D-dimensional linear cellular automata over Z_m to be *sensitive to initial conditions*, *positively expansive*, *strongly transitive*, and *equicontinuous*. As a consequence of our results, we have a complete and efficiently computable topological classification of D-dimensional linear cellular automata over Z_m according to the most important dynamical properties studied in the theory of discrete time dynamical systems. © 1999 Published by Elsevier Science B.V. All rights reserved.

Keywords: Linear cellular automata; Topological properties; Discrete time dynamical systems

1. Introduction

Cellular automata (CA) are dynamical systems consisting of a regular lattice of variables which can take a finite number of discrete values. The global state of the CA, specified by the values of all the variables at a given time, evolves in synchronous discrete-time steps according to a given *local rule* which acts on the value of each single variable. CA have been widely studied in a number of disciplines (e.g., computer science, physics, mathematics, biology, chemistry) with different purposes (e.g., simulation of natural phenomena, pseudo-random number generation, image processing,

[☆] A preliminary version of this paper has been presented to the 24th International Colloquium on Automata Languages and Programming (ICALP '97).

[*] Corresponding author. Departimento de Scienze e Tectnol. Avanzante, Universita di Torino, Torino, Italy. E-mail address: manzini@mfn.al.unipmr.it. (Giovanni Manzini)

[1] *E-mail address:* margara@cs.unibo.it. (Luciano Margara)

PII: S0304-3975(99)00031-6

Property	Characterization	Reference
Surjectivity	$\gcd(m, \lambda_1, \dots, \lambda_s) = 1$	[10]
Injectivity	$(\forall p \in \mathscr{P})(\exists! \lambda_i)$: $p \nmid \lambda_i$	[10]
Ergodicity	$\gcd(m, \lambda_2, \dots, \lambda_s) = 1$	[15]
Transitivity	$\gcd(m, \lambda_2, \dots, \lambda_s) = 1$	[2]
Regularity	$\gcd(m, a_{-r}, \dots, a_r) = 1$	[2]
Expansivity	$\gcd(m, a_{-r}, \dots, a_{-1}, a_1, \dots, a_r) = 1$	[13]
Sensitivity	$(\exists p \in \mathscr{P})$: $p \nmid \gcd(\lambda_2, \dots, \lambda_s)$	This paper
Pos. expansivity	$\gcd(m, a_1, \dots, a_r) = \gcd(m, a_{-1}, \dots, a_{-r}) = 1$	This paper
Equicontinuity	$(\forall p \in \mathscr{P})\ p \mid \gcd(\lambda_2, \dots, \lambda_s)$	This paper
Strong trans.	$(\forall p \in \mathscr{P})(\exists \lambda_i, \lambda_j)$: $p \nmid \lambda_i \wedge p \nmid \lambda_j$	This paper

Fig. 1. Characterization of set theoretic and topological properties of linear CA over Z_m in terms of the coefficients λ_i's (for D-dimensional CA) or a_i's (for one-dimensional CA). $\mathscr{P}$ denotes the set of prime factors of m.

analysis of universal model of computations, cryptography). CA can display a rich and complex temporal evolution whose exact determination is in general very hard, if not impossible. In particular, some properties of the temporal evolution of general CA are undecidable [4, 5, 11]. For an introduction to the CA theory and an extensive and up-to-date bibliography see [8].

In this paper we restrict our attention to the class of linear CA (CA based on a linear local rule defined over the ring Z_m). Despite of their apparent simplicity, linear CA may exhibit complex features and have found many applications (see [3]). Several important properties of linear CA have been studied during the last few years [1, 2, 9, 10, 12–15] and in some cases exact characterizations have been obtained (see Fig. 1).

We investigate the topological behavior of linear D-dimensional CA over Z_m. We focus our attention on a number of topological properties which are widely recognized as fundamental in the determination of the qualitative behavior of any discrete-time dynamical system, namely *sensitivity to initial conditions, positive expansivity, equicontinuity*, and *strong transitivity*. The main contribution of this paper consists in efficiently computable criteria for deciding whether a linear CA satisfies one of the above four properties. Our criteria are reported in Fig. 1 and are given in terms of the coefficients of the linear local map associated to the CA. Note that, using our criteria, one can easily construct a linear CA which satisfies any combination of the above properties. The criteria we propose require only gcd computations and can be checked in polynomial time in log m and in the number of coefficients of the local rule. The dimension of the lattice does not explicitly affect the computational cost of our criteria. The results of this paper hold for every dimension $D \geqslant 1$ and for every $m \geqslant 2$. Our results show that linear CA over Z_m have dynamical aspects that linear CA over finite fields, such as Z_p with p prime, cannot have. Fig. 2 illustrates the differences between possible topological behaviors of linear CA over Z_m for m composite and m prime.

Since many definitions of chaotic dynamical system are based on topological properties such as transitivity and sensitivity to initial conditions [6], the diagram of Fig. 2

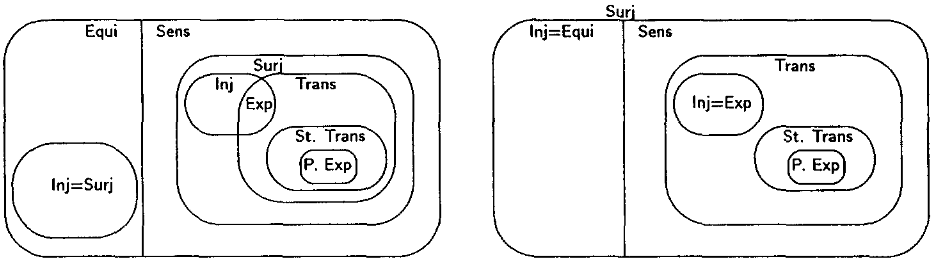

Fig. 2. Diagram of properties of D-dimensional linear CA over Z_m for m composite (left) and m prime (right). All inclusions are proper. Note that the classes of positively expansive CA and expansive CA are empty in any dimension greater than 1.

can be *interpreted* as a *hierarchical* definition of chaos. We have five classes of increasing degrees of chaoticity, namely equicontinuous CA, sensitive but not transitive CA, transitive but not strongly transitive CA, strongly transitive but not positively expansive CA, and, finally, positively expansive CA. Some of the inclusions of Fig. 2 hold also for general CA. Unfortunately, in the general case the problem of deciding whether a given CA satisfies one of the above-mentioned topological properties is not even known to be decidable.

The rest of this paper is organized as follows. In Section 2 we give basic definitions and notations. In Section 3 we state our results. Section 4 contains the proofs of the main theorems. Section 5 contains some concluding remarks. The proof of some technical lemmas have been confined to the appendix.

2. Basic definitions

For $m \geqslant 2$, let Z_m, denote the ring of integers modulo m. We consider the *space of configurations*

$$\mathscr{C}_m^D = \{c \mid c : Z^D \to Z_m\},$$

which consists of all functions from Z^D into Z_m. Each element of $\mathscr{C}_m^D$ can be visualized as an infinite D-dimensional lattice in which each cell contains an element of Z_m.

Let $s \geqslant 1$. A *neighborhood frame* of size s is an ordered set of distinct vectors $\boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_s \in Z^D$. Given any function $f : Z_m^s \to Z_m$, a D-dimensional CA based on the *local rule* f is the pair $(\mathscr{C}_m^D, F)$, where $F : \mathscr{C}_m^D \to \mathscr{C}_m^D$, is the *global transition map* defined as follows. For every $c \in \mathscr{C}_m^D$ the configuration $F(c)$ is such that for every $\boldsymbol{v} \in Z^D$

$$[F(c)](\boldsymbol{v}) = f(c(\boldsymbol{v} + \boldsymbol{u}_1), \dots, c(\boldsymbol{v} + \boldsymbol{u}_s)). \tag{1}$$

In other words, the content of cell $\boldsymbol{v}$ in the configuration $F(c)$ is a function of the content of the cells $\boldsymbol{v} + \boldsymbol{u}_1, \dots, \boldsymbol{v} + \boldsymbol{u}_s$ in the configuration c. Note that the local rule f

and the neighborhood frame completely determine F. In this paper we consider mainly *linear* CA, that is, CA with a local rule of the form

$$f(x_1,\dots,x_s)=\sum_{i=1}^{s}\lambda_i x_i \bmod m, \tag{2}$$

with $\lambda_1,\dots,\lambda_s \in Z_m$. Note that for a linear D-dimensional CA, 1 becomes

$$[F(c)](\boldsymbol{v})=\sum_{i=1}^{s}\lambda_i c(\boldsymbol{v}+\boldsymbol{u}_i) \bmod m. \tag{3}$$

We define the *radius* of the linear CA $(\mathscr{C}_m^D,F)$ as

$$\rho(F)=\max_{1\leqslant i\leqslant s}||\boldsymbol{u}_i||_\infty, \tag{4}$$

where the maximum is restricted to the indices i such that $\lambda_i \not\equiv 0 \pmod m$. As usual, $||\boldsymbol{v}||_\infty$ denotes the maximum of the absolute value of the components of $\boldsymbol{v}$.

Example 1. A simple two-dimensional linear CA over the alphabet $\{0,1\}$ is the one in which the new value of each cell is the sum modulo 2 of its north, south, east, and west neighbors. Using our notation we have $D=2$, $m=2$, $s=4$, and

$$\boldsymbol{u}_1=\langle 1,0\rangle, \qquad \boldsymbol{u}_2=\langle -1,0\rangle, \qquad \boldsymbol{u}_3=\langle 0,1\rangle, \qquad \boldsymbol{u}_4=\langle 0,-1\rangle.$$

The local rule f is given by

$$f(x_1,x_2,x_3,x_4)=(x_1+x_2+x_3+x_4) \bmod 2.$$

The global transition map F has radius one and is defined by

$$\begin{aligned}[F(c)](i,j)&=f(c(i+1,j),c(i-1,j),c(i,j+1),c(i,j-1)) \bmod 2.\\ &=c(i+1,j)+c(i-1,j)+c(i,j+1)+c(i,j-1) \bmod 2.\end{aligned}$$

For linear one-dimensional CA we use a simplified notation. A local rule of radius r is written as

$$f(x_{-r},\dots,x_r)=\sum_{i=-r}^{r}a_i x_i \bmod m, \tag{5}$$

where at least one between a_{-r} and a_r is nonzero. Using this notation, the global map F of a one-dimensional CA with $\rho(F)=r$ becomes

$$[F(c)](i)=\sum_{j=-r}^{r}a_j c(i+j) \bmod m, \quad c\in\mathscr{C}_m^1, \quad i\in Z.$$

Example 2. The local rule

$$f(x_{-2},x_{-1},x_0,x_1,x_2)=x_{-1}-x_1+2x_2 \bmod 4$$

defines a one-dimensional CA over Z_4 whose global transition map F has radius $\rho(F)=2$ and is given by

$$[F(c)](i)=c(i-1)-c(i+1)+2c(i+2) \bmod 4.$$

The topological properties of CA are usually defined with respect to the metric topology induced by the *Tychonoff distance*. Let $\Delta : Z_m \times Z_m \to \{0,1\}$ given by

$$\Delta(i,j)=\begin{cases} 0 & \text{if } i=j, \\ 1 & \text{if } i\neq j. \end{cases}$$

For any pair $a,b\in \mathscr{C}_m^D$ the Tychonoff distance $d(a,b)$ is defined by

$$d(a,b)=\sum_{\mathbf{v}\in Z^D} \frac{\Delta(a(\mathbf{v}),b(\mathbf{v}))}{2^{\|\mathbf{v}\|_\infty}}. \tag{6}$$

It is easy to verify that d is a metric on $\mathscr{C}_m^D$ and that the topology induced by d coincides with the product topology induced by the discrete topology on Z_m. With this topology, $\mathscr{C}_m^D$ is a compact and totally disconnected space and every CA is a uniformly continuous map.

Given two configurations $a,b\in \mathscr{C}_m^D$ we define their sum $a+b$ by the rule $(a+b)(\mathbf{v})=a(\mathbf{v})+b(\mathbf{v}) \bmod m$ for every $\mathbf{v}\in Z^D$. Note that, with respect to this sum, the Tychonoff distance is translation invariant, that is, $d(a,b)=d(a+c,b+c)$. In addition, if F is linear we have $F(a+b)=F(a)+F(b)$. A special configuration is the *null* configuration 0 which has the property that $0(\mathbf{v})=0$ for all $\mathbf{v}\in Z^D$.

Throughout the paper, $F(c)$ will denote the result of the application of the map F to the configuration c, and $c(\mathbf{v})$ will denote the value assumed by c in $\mathbf{v}$. We recursively define $F^n(c)$ by $F^n(c)=F(F^{n-1}(c))$, where $F^0(c)=c$.

2.1. Topological properties

In this section we recall the definitions of some topological properties which are used to study the qualitative behavior of discrete time dynamical systems. Here, we assume we are given a space of configurations X equipped with a distance d, and a map F continuous on X according to the topology induced by d (for CA, Tychonoff distance satisfies this property). We denote by $\mathscr{B}(x,\varepsilon)$ the (open) set $\{y\in X: d(x,y)<\varepsilon\}$.

Definition 2.1 (*Sensitivity*). A dynamical system (X,F) is sensitive to initial conditions if and only if there exists $\delta>0$ such that for any $x\in X$ and for any $\varepsilon>0$, there exist $y\in\mathscr{B}(x,\varepsilon)$ and $n\geqslant 0$, such that $d(F^n(x),F^n(y))>\delta$. The value δ is called the sensitivity constant.

Intuitively, a map is sensitive to initial conditions, or simply sensitive, if there exist points arbitrarily close to x which eventually separate from x by at least δ under iteration of F. Note that not all points near x need eventually separate from x under iteration, but there must be at least one such point in every neighborhood of x.

A property stronger than sensitivity is positive expansivity. Positive expansivity differs from sensitivity in that all nearby points must eventually separate by at least δ. It is easy to verify that positively expansive CA are sensitive to initial conditions.

Definition 2.2 (*Positive expansivity*). A dynamical system (X,F) is positively expansive if and only if there exists $\delta>0$ such that for every $x,y\in X$, $x\neq y$, there exists $n\geqslant 0$ such that $d(F^n(x),F^n(y))>\delta$. The value δ is called the expansivity constant.

For invertible maps the above definition can be generalized as follows. We say that an invertible map F is *expansive* if and only if there exists $\delta>0$ such that for every $x,y\in X$, $x\neq y$, there exists $n\in Z$ such that $d(F^n(x),F^n(y))>\delta$. Here, F^n with $n<0$ denotes F^{-1} iterated $|n|$ times. In [13] the authors give a formula for the inverse of linear CA and use it to characterize expansive linear CA in terms of the coefficients of the associated local rule.

It is known (see [7, 16]), that there are no expansive or positively expansive CA $(\mathscr{C}_m^D,F)$ for $D>1$.

Definition 2.3 (*Equicontinuity at x*). A dynamical system (X,F) is equicontinuous at $x\in X$ if and only if for any $\delta>0$ there exists $\varepsilon>0$ such that for any $y\in\mathscr{B}(x,\varepsilon)$ and $n\geqslant 0$ we have $d(F^n(x),F^n(y))<\delta$.

Definition 2.4 (*Equicontinuity*). A dynamical system (X,F) is equicontinuous if and only if it is equicontinuous at every $x\in X$.

The notions of sensitivity and equicontinuity (also known as *stability*) are related. In fact, by comparing the definitions one can easily see that

$$F \text{ is not sensitive } \Leftrightarrow \exists x\text{: } F \text{ is equicontinuous at } x. \qquad (7)$$

Definition 2.5 (*Strong transitivity*). A dynamical system (X,F) is strongly transitive if and only if for all nonempty open set $U\subseteq X$ we have $\bigcup_{n=0}^{+\infty}F^n(U)=X$.

A strongly transitive map F has points which, under iteration of F, move from one arbitrarily small neighborhood to all the space of configurations X. A weaker notion is *transitivity*: a map F is transitive if and only if for every nonempty open set U the set $\bigcup_{n=0}^{+\infty}F^n(U)$ is a dense subset of X. Clearly, strongly transitive maps are transitive. If F is a linear strongly transitive CA in view of [2, Theorem 3.2] is also ergodic with respect to the normalized Haar measure.

3. Statement of the new results

In this section we state the main results of this paper. The same results are summarized in Figs. 1 and 2.

Theorem 3.1. *Let F denote the global transition map of a linear D-dimensional CA over Z_m defined by*

$$[F(c)](\boldsymbol{v}) = \sum_{i=1}^{s} \lambda_i c(\boldsymbol{v} + \boldsymbol{u}_i) \bmod m. \tag{8}$$

Assume $\boldsymbol{u}_1 = \boldsymbol{0}$, that is, λ_1 is the coefficient associated to the null displacement. The global transition map F is sensitive if and only if there exists a prime p such that

$$p \mid m \quad \textit{and} \quad p \nmid \gcd(\lambda_2, \lambda_3, \ldots, \lambda_s). \tag{9}$$

In other words, F is sensitive unless every prime which divides m divides also all the coefficients λ_i's with $i \neq 1$.

Note that we can check the above condition without knowing the factorization of m. In fact, (9) holds if and only if $\gcd(\lambda_2, \lambda_3, \ldots, \lambda_s)$ does not contain all the prime factors of m. Since each prime appears in m with a power at most $\lfloor \log_2 m \rfloor$, F is sensitive if and only if $[\gcd(\lambda_2, \lambda_3, \ldots, \lambda_s)]^{\lfloor \log_2 m \rfloor} \not\equiv 0 \pmod{m}$.

Theorem 3.2. *Let F denote the global transition map of a linear one-dimensional CA over Z_m with local rule $f(x_{-r}, \ldots, x_r) = \sum_{i=-r}^{r} a_i x_i \bmod m$. The global transition map F is positively expansive if and only if*

$$\gcd(m, a_{-r}, \ldots, a_{-1}) = 1 \qquad \textit{and} \qquad \gcd(m, a_1, \ldots, a_r) = 1. \tag{10}$$

Since positively expansive CA do not exist in any dimension $D \geqslant 2$, the above theorem completely characterizes the class of linear positively expansive CA.

Theorem 3.3. *Let F denote the global transition map of the linear D-dimensional CA over Z_m defined by* (8). *The following statements are equivalent.*

(i) *F is equicontinuous in at least one point,*

(ii) *F is equicontinuous at every point,*

(iii) *for each prime p such that $p \mid m$ we have $p \mid \gcd(\lambda_2, \lambda_3, \ldots, \lambda_s)$.*

By Theorem 3.3 and (7), we get that a linear CA is either sensitive or equicontinuous. Hence, F is equicontinuous if and only if $[\gcd(\lambda_2, \lambda_3, \ldots, \lambda_s)]^{\lfloor \log_2 m \rfloor} \equiv 0 \pmod{m}$. As a corollary to Theorem 3.3 we have the following result which will be proven in Section 4.3.

Corollary 3.4. *Let F denote the global transition map of any surjective and equicontinuous linear D-dimensional CA over Z_m. Then F is injective.*

Since injective CA are surjective, Corollary 3.4 implies that, for equicontinuous CA, injectivity is equivalent to surjectivity.

Theorem 3.5. *Let F denote the global transition map of a linear D-dimensional CA over Z_m defined by* (8). *The global transition map F is strongly transitive if and only* *if for each prime p such that $p|m$, there exist at least two coefficients λ_i, λ_j such that $p \nmid \lambda_i$ and $p \nmid \lambda_j$.*

Note that we can check whether F is strongly transitive without knowing the factorization of m. In fact, the above condition is equivalent to

$$\gcd(m, \lambda_2, \lambda_3, \ldots, \lambda_s) = \gcd(m, \lambda_1, \lambda_3, \ldots, \lambda_s) = \cdots = \gcd(m, \lambda_1, \lambda_2, \ldots, \lambda_{s-1}) = 1.$$

4. Proof of the main theorems

We now prove the results stated in Section 3. In our proofs we make use of the *formal power series* (fps) representation of the configuration space $\mathscr{C}_m^D$ (see [10, Section. 3] for details). For $D=1$, to each configuration $c \in \mathscr{C}_m^1$ we associate the fps

$$P_c(X) = \sum_{i \in Z} c(i) X^i.$$

The advantage of this representation is that the computation of a linear map is equivalent to power series multiplication. Let $F : \mathscr{C}_m^1 \to \mathscr{C}_m^1$ be a linear map with local rule $f(x_{-r}, \ldots, x_r) = \sum_{i=-r}^{r} a_i x_i$. We associate to F the finite fps $A_f(X) = \sum_{i=-r}^{r} a_i X^{-i}$. Then, for any $c \in \mathscr{C}_m^1$ we have

$$P_{F(c)}(X) = P_c(X) A_f(X) \bmod m.$$

Note that each coefficient of $P_{F(c)}(X)$ is well defined since $A_f(X)$ has only finitely many nonzero coefficients. Note also that the finite fps associated to F^n is $A_f^n(X)$.

More in general, to each configuration $c \in \mathscr{C}_m^D$ we associate the formal power series

$$P_c(X_1, \ldots, X_D) = \sum_{i_1, \ldots, i_D \in Z} c(i_1, \ldots, i_D) X_1^{i_1} \cdots X_D^{i_D}.$$

The computation of a linear map F over $\mathscr{C}_m^D$ is equivalent to the multiplication by a finite fps $A(X_1, \ldots, X_D)$ which can be easily obtained by the local rule f and the neighborhood frame $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_s$. The finite fps associated to the map F defined by (8) is

$$A(X_1, \ldots, X_D) = \sum_{i=1}^{s} \lambda_i X_1^{-\boldsymbol{u}_i(1)} \cdots X_D^{-\boldsymbol{u}_i(D)},$$

where $\boldsymbol{u}_i(j)$ denotes the jth component of vector $\boldsymbol{u}_i$.

Example 3. The finite fps associated to the map F defined in Example 1 is $A(X, Y) = X + X^{-1} + Y + Y^{-1}$. The finite fps associated to the one-dimensional defined in Example 2 is $A(X) = 2X^{-2} - X^{-1} + X$.

Throughout the paper, given a fps $H(X)$ and $i \in Z$, we use $\langle H(X) \rangle_i$ to denote the coefficient of X^i in $H(X)$.

4.1. Sensitivity

In this section we characterize sensitive linear CA. We prove our results only in the two-dimensional case, since the proofs for the other dimensions are similar.

Let $F:\mathscr{C}_m^2 \to \mathscr{C}_m^2$ denote the global transition map of a two-dimensional CA. For any integer $k>0$, let $\mathscr{V}_k^2$ denote the set of configurations $c \in \mathscr{C}_m^2$ such that $c(\boldsymbol{v})=0$ for $\|\boldsymbol{v}\|_\infty < k$. It is straightforward to verify that F is sensitive if and only if there exists $\delta>0$ such that for any configuration $c \in \mathscr{C}_m^2$ we have

$$\forall k>0, \quad \exists c' \in \mathscr{V}_k^2\colon \quad d(F^n(c+c'),F^n(c))>\delta \quad \text{for some } n \geqslant 0. \tag{11}$$

In fact, (11) implies that we can find a configuration, arbitrarily close to c, whose distance from c exceeds δ after a sufficiently large number of iterations.

If F is linear we can get rid of the particular configuration c. We have

$$d(F^n(c+c'),F^n(c)) = d(F^n(c)+F^n(c'),F^n(c)) = d(F^n(c'),0).$$

Hence, F is sensitive if and only if there exists $\delta>0$ such that

$$\forall k>0, \quad \exists c' \in \mathscr{V}_k^2\colon \quad d(F^n(c'),0)>\delta \quad \text{for some } n \geqslant 0. \tag{12}$$

This observation leads to the following lemma.

Lemma 4.1. *Let F denote the global transition map of a linear D-dimensional CA over Z_m. F is sensitive if and only if*

$$\limsup_{n\to\infty} \rho(F^n) = \infty, \tag{13}$$

the radius ρ of a CA being defined by (4).

Proof. We prove the result for $D=2$. If (13) does not hold, there exists M such that $\rho(F^n)<M$ for all n. Thus, if $k>M$, for all $c \in \mathscr{V}_k^2$ we have $F^n(c) \in \mathscr{V}_{k-M}^2$. Elementary calculus shows that $c \in \mathscr{V}_t^2 \Rightarrow d(c,0) \leqslant 8(t+2)/2^t$. Hence, for any δ, if k is large enough $c \in \mathscr{V}_k^2$ implies $d(F^n(c),0) \leqslant \delta$ for all n, and F cannot be sensitive.

Assume now (13) holds. Then, for every k we can find n such that $\rho(F^n)=z>k$. Let $\lambda_i^{(n)}$, $\boldsymbol{u}_i^{(n)}$ denote the coefficients and the displacements of the local map associated to F^n. $\rho(F^n)=z$ implies that there exists j, such that $\lambda_j^{(n)} \neq 0$ and $\|\boldsymbol{u}_j^{(n)}\|_\infty = z$. Let c be such that $c(-\boldsymbol{u}_j^{(n)})=1$, and $c(\boldsymbol{v})=0$ for $\boldsymbol{v} \neq -\boldsymbol{u}_j^{(n)}$. Clearly, $c \in \mathscr{V}_k^2$ and $[F^n(c)](\mathbf{0}) = \lambda_j^{(n)} \neq 0$ which implies (12) for any δ, $0<\delta<1$. □

Proof of Theorem 3.1. Let F denote the global transition map of a linear two-dimensional CA, and let

$$A(X,Y) = \sum_{\substack{v \leqslant i \leqslant w \\ y \leqslant j \leqslant z}} a_{i,j} X^i Y^j$$

denote the finite fps associated to F. Assume (9) holds. Then, there exist a prime p and a coefficient $a_{s,u}$ such that $p|m$, $p \nmid a_{s,u}$ and at least one between s and u is nonzero.

We now prove that, as a consequence, $\limsup \rho(F^n) = \infty$. Without loss of generality, we can assume $s \neq 0$, and that for $i < s$ we have $p | a_{i,j}$. Let $\tilde{A}(X,Y) = A(X,Y) \bmod p$. By our assumptions, $\tilde{A}(X,Y)$ can be written as $X^s G(Y) + \sum_{s<i\leqslant w} X^i H_i(Y)$, with $G(Y) \neq 0$. Hence,

$$(A^n(X,Y) \bmod p) = [\tilde{A}(X,Y)]^n = X^{ns} G^n(Y) + \sum_{ns<i\leqslant nw} X^i H_i'(Y).$$

Since Z_p is an integral domain, we have $G^n(Y) \neq 0$ which implies $\rho(F^n) \geqslant n|s|$.

Assume now $p|m \Rightarrow p|\lambda_i$ for all $i \neq 1$ and every prime p. Let $m = p_1^{k_1} \cdots p_n^{k_n}$ denote the factorization of m, and let $k = \max_i k_i$. We prove that $\rho(F^n) \leqslant \rho(F)(k-1)$. Let $b_{i,j}$ denote the coefficients of the fps associated to F^n. We have

$$b_{i,j} = \sum_{\substack{i_1+\cdots+i_n=i \\ j_1+\cdots+j_n=j}} a_{i_1,j_1} a_{i_2,j_2} \cdots a_{i_n,j_n}. \tag{14}$$

If $\max(|i|,|j|) > \rho(F)(k-1)$, each term $a_{i_1,j_1} a_{i_2,j_2} \cdots a_{i_n,j_n}$ must contain at least k coefficients a_{i_h,j_h} with $\max(|i_h|,|j_h|) \neq 0$. Hence, $p|m \Rightarrow p^k | (a_{i_1,j_1} \cdots a_{i_n,j_n})$, and each term in the sum (14) is a multiple of m. Hence, $\rho(F^n) \leqslant \rho(F)(k-1)$ and by Lemma 4.1 F is not sensitive. □

4.2. Positive expansivity

In this section we characterize positively expansive linear CA. Since positively expansive CA do not exist in any dimension $D \geqslant 2$ we can restrict ourselves to the one-dimensional case.

Let $F : \mathscr{C}_m^1 \to \mathscr{C}_m^1$ denote the global transition map of a one-dimensional CA. It is straightforward to verify that F is positively expansive if and only if there exists $\delta > 0$ such that for any configuration $c \in \mathscr{C}_m^1$ we have

$$\forall c' \in \mathscr{C}_m^1, \quad c' \neq 0, \quad \exists n \geqslant 0: \quad d(F^n(c+c'), F^n(c)) > \delta.$$

Reasoning as in Section 4.1, if F is linear we can get rid of the particular configuration c. We have

$$d(F^n(c+c'), F^n(c)) = d(F^n(c) + F^n(c'), F^n(c)) = d(F^n(c'), 0).$$

Hence, F is positively expansive if and only if for any $c' \neq 0$ we have $d(F^n(c'), 0) > \delta$ for a sufficiently large n. Clearly, this is equivalent to assuming that there exists $M > 0$ such that

$$\forall c' \in \mathscr{C}_m^1, \quad c' \neq 0, \quad \exists n \geqslant 0: \quad [F^n(c')](i) \neq 0 \text{ for some } i \text{ with } |i| < M.$$

For any integer $k > 0$, let $\mathscr{W}_k$ denote the set of configurations $c \in \mathscr{C}_m^1$ such that $c(i) = 0$ for $|i| < k$ and at least one between $c(k)$ and $c(-k)$ is different from zero. Since δ can be chosen arbitrarily, we have that F is positively expansive if and only if $\exists \tilde{k}$ such that for all $k > \tilde{k}$

$$\forall c \in \mathscr{W}_k, \quad \exists n \geqslant 0: \quad [F^n(c)](i) \neq 0 \quad \text{for some } i \text{ with } |i| < M. \tag{15}$$

If we visualize each configuration as a biinfinite array, 15 tells us that the essential feature of positively expansive CA is that *any* pattern of nonzero values can "propagate" from positions arbitrarily away from 0 up to a position i with $|i|<M$. Informally, we say that any nonzero pattern can propagate for an arbitrarily large distance. For a comparison, sensitive one-dimensional linear CA can be seen as those CA in which for each $t>0$ there exists a nonzero pattern which propagates by at least t positions.

The following lemma shows a relationship between the coefficients a_i's of the local rule (5) and the propagation of one-sided nonzero patterns.

Lemma 4.2. *Let* $m=p_1^{k_1}\cdots p_h^{k_h}$, *and let* $c\in\mathscr{C}_m^1$ *such that* $c(v)\neq 0$ *and* $c(i)=0$ *for* $i>v$. *If* $\gcd(m,a_{-1},\dots,a_{-r})=1$, *then there exists n such that* $[F^n(c)](i)\neq 0$ *for some* i *with* $|i|<r(\max_{j=1,\dots,h} p_j^{k_j}(k_j-1)!)$.

Proof. Let $C(X)=\sum_{i\leqslant v} c_iX^i$ be the fps associated to c. Since $m\nmid c_v$, there exists a prime p and an integer k such that $p^k|m$ and $p^k\nmid c_v$. Since $\gcd(m,a_{-1},\dots,a_{-r})=1$, we can find t, $0<t\leqslant r$, such that

$$p\nmid a_{-t} \quad\text{and}\quad p\,|\,a_{-i} \quad \text{for } t<i\leqslant r. \tag{16}$$

Let $A(X)=\sum_{i=-r}^{r} a_{-i}X^i$ denote the finite fps associated to F. We prove the lemma by showing that if n is a positive multiple of $p^k(k-1)!$ then

$$[F^n(c)](v+nt)=\langle C(X)A^n(X)\rangle_{v+nt}\not\equiv 0\,(\operatorname{mod} m),$$

since this implies that we can have a nonzero in every position v' such that $v'>v$ and $v'\equiv v\,(\operatorname{mod} tp^k(k-1)!)$.

Let $\tilde{A}(X)=A(X)\operatorname{mod}p^k$. By (16) we know that $\tilde{A}(X)$ satisfies the hypothesis of Lemma A.4 in the appendix. Hence, if n is a multiple of $p^k(k-1)!$, we have $\tilde{A}^n(X)=\sum_{i=-nr}^{nt}\tilde{a}_iX^i$ with $\gcd(\tilde{a}_{nt},p^k)=1$. We have

$$\begin{aligned}[F^n(c)](v+nt) &\equiv \langle \tilde{A}^n(X)C(X)\rangle_{v+nt}\,(\operatorname{mod} p^k)\\ &\equiv \left\langle\left(\sum_{i=-nr}^{nt}\tilde{a}_iX^i\right)\left(\sum_{i\leqslant v}c_iX^i\right)\right\rangle_{v+nt} (\operatorname{mod} p^k)\\ &\equiv \tilde{a}_{nt}c_v\,(\operatorname{mod} p^k).\end{aligned}$$

Since by hypothesis $p^k\nmid c_v$ and $p\nmid \tilde{a}_{nt}$, $[F^n(c)](v+nt)$ is not a multiple of p^k. We conclude that $[F^n(c)](v+nt)$ is nonzero modulo m as claimed. □

Lemma 4.2 proves that if $\gcd(m,a_{-1},\dots,a_{-r})=1$ any left-sided nonzero pattern can propagate arbitrarily far away to the right. Similarly, $\gcd(m,a_1,\dots,a_r)=1$ implies that any right-sided nonzero, pattern can propagate arbitrarily far away to the left. Having established these two facts we are now able to prove Theorem 3.2.

Proof of Theorem 3.2. Let $m=p_1^{k_1}\cdots p_h^{k_h}$, and assume (10) holds. We show that F is positively expansive by proving that (15) holds with $M=\tilde{k}=1+r[\max_i p_i^{k_i}(k_i-1)!]$. For any $k>\tilde{k}$ let $c\in\mathscr{W}_k$. If $c(i)=0$ for $i>-k$, or $c(i)=0$ for $i<k$ the thesis follows

by Lemma 4.2 and the observation following it. For the general case in which c assumes nonzero values both for $i<-k$ and $i>k$, we write $c=c_{\mathrm{L}}+c_{\mathrm{R}}$, where c_{L} (resp. c_{R}) is such that $c_{\mathrm{L}}(i)=0$ for $i>-k$ (resp. $c_{\mathrm{R}}(i)=0$ for $i<k$). By linearity we have $F^n(c)=F^n(c_{\mathrm{L}})+F^n(c_{\mathrm{R}})$. Hence, for a suitable n we must have $[F^n(c)](i)\neq 0$ for some i with $|i|<M$, *unless* the nonzero patterns generated by $F^n(c_{\mathrm{L}})$ and $F^n(c_{\mathrm{R}})$ cancel each other for $|i|<M$. However, since F has radius r and $M\geqslant 1+2r$, the nonzero patterns generated by $F^n(c_{\mathrm{L}})$ and $F^n(c_{\mathrm{R}})$ cannot cancel each other unless at least one of them has already reached the region with $|i|<M$. This proves that (15) holds for any $c\in\mathscr{W}_k$ and the map F is positively expansive as claimed.

Finally, we prove that (10) is a necessary condition for positive expansivity. Assume for example $\gcd(a_1,\ldots,a_r)=q_1>1$, and let $q_2=m/q_1$. For any integer $k>0$ let $c_k\in\mathscr{W}_k$ denote the configuration defined by $c_k(i)=q_2$ if $i=k$ and $c_k(i)=0$ otherwise. We show that for every $n>0$ and $i<k$ we have $[F^n(c_k)](i)=0$ which implies that F is not positively expansive. Since the fps associated to c_k is q_2X^k, we have

$$[F^n(c_k)](i)=\langle q_2X^kA^n(X)\rangle_i=q_2\langle A^n(X)\rangle_{i-k}. \tag{17}$$

By hypothesis, for $j<0$, $\langle A(X)\rangle_j$ is a multiple of q_1. One can easily verify that also for $A^n(X)$ we have that $j<0$ implies $q_1|\langle A^n(X)\rangle_j$. By (17) we get that, for $i<k$, $[F^n(c_k)](i)\equiv 0\,(\mathrm{mod}\, m)$ as claimed. □

4.3. Equicontinuity

In this section we characterize equicontinuous linear CA. Our result relies on the fact that linear CA are either equicontinuous at every point or sensitive to initial conditions.

Lemma 4.3. *Let x be any configuration. A linear map F is equicontinuous at x if and only if F is equicontinuous at* 0.

Proof. Assume F is equicontinuous at 0. Then, for any $\delta>0$ there exists $\varepsilon_\delta>0$ such that for any configuration $y\in\mathscr{B}(0,\varepsilon_\delta)$ and for any $n\geqslant 0$

$$d(F^n(0),F^n(y))=d(0,F^n(y))<\delta. \tag{18}$$

Assume by contradiction that F is not equicontinuous at x. Then, there exist $\delta>0$, a configuration $y\in\mathscr{B}(x,\varepsilon_\delta)$, and an integer $n\geqslant 0$ such that $d(F^n(x),F^n(y))\geqslant\delta$. Let $y'=(y-x)\,\mathrm{mod}\, m$. Since d is translation invariant we have $y'\in\mathscr{B}(0,\varepsilon_\delta)$. For the linearity of F we get

$$d(0,F^n(y'))=d(F^n(x),F^n(x)+F^n(y'))=d(F^n(x),F^n(y))\geqslant\delta. \tag{19}$$

Comparing (18) and (19) we get a contradiction. In a similar way, one can prove that F equicontinuous at x implies F equicontinuous at 0. □

Proof of Theorem 3.3. Obviously (ii)⇒(i). By Lemma 4.3 we have that for linear CA (i)⇒(ii). To prove that (i)⇔(iii) we simply note that by (7) to get a characterization for equicontinuous maps it suffices to negate the characterization for sensitive maps. □

Proof of Corollary 3.4. We use the characterization of injective and surjective CA proven in [10] and shown in Fig. 1. Let F be a surjective map defined by (8), and let λ_1 be the coefficient associated to the null displacement. Let p be any prime which divides m. Since F is equicontinuous then

$$p|\lambda_j \quad \text{for } 2 \leqslant j \leqslant s.$$

In addition, since F is surjective $p \nmid \lambda_1$. Hence, there exists a unique coefficient λ_i such that $p \nmid \lambda_i$ and the map F is injective. □

4.4. Strong transitivity

In this section we prove the characterization of strongly transitive linear CA. The proof is quite complex and we will need some preliminary lemmas. To simplify the notation we first give the proof for the one-dimensional case. The extension for $D > 1$ is given in Section 4.4.1.

Let $\mathscr{V}_k^1 = \{x \in \mathscr{C}_m^1 \mid x(i) = 0 \text{ for } |i| < k\}$. For any $x \in \mathscr{C}_m^1$ let

$$\mathscr{D}(x,k) = x + \mathscr{V}_k^1 = \{y \in \mathscr{C}_m^1 \mid y = x + z,\ z \in \mathscr{V}_k^1\}.$$

Since we are considering the topology induced by d, for any nonempty open subset $U \subseteq \mathscr{C}_m^1$, we can find $x \in \mathscr{C}_m^1$ and $\varepsilon > 0$ such that $\mathscr{B}(x,\varepsilon) \subseteq U$. Elementary calculus shows that

$$\mathscr{D}(x, 3 + \lceil \log(1/\varepsilon) \rceil) \subseteq \mathscr{B}(x,\varepsilon) \subseteq U,$$

hence F is strongly transitive if and only if

$$\forall x \in \mathscr{C}_m^1, \quad \forall k > 0, \quad \bigcup_{n=0}^{+\infty} F^n(\mathscr{D}(x,k)) = \mathscr{C}_m^1. \tag{20}$$

We are now ready to establish a simple condition which, for linear maps, implies strong transitivity.

Lemma 4.4. *Let F be a linear one-dimensional map over Z_m. If, for all k, there exists n_k such that $F^{n_k}(\mathscr{V}_k^1) = \mathscr{C}_m^1$, then F is strongly transitive.*

Proof. For all $x \in \mathscr{C}_m^1$ and $k > 0$ we have

$$\bigcup_{n=0}^{+\infty} F^n(\mathscr{D}(x,k)) \supseteq F^{n_k}(x + \mathscr{V}_k^1) = F^{n_k}(x) + F^{n_k}(\mathscr{V}_k^1) = \mathscr{C}_m^1. \qquad \square$$

To prove the "if" part of Theorem 3.5 we use Lemma 4.4 and the power series representation of CA. Lemma 4.5 establishes the result for the special case in which m is a prime power, while Lemma 4.6 proves the result in the general case.

Lemma 4.5. *Let $A(X)=\sum_{-r\leqslant i\leqslant r} a_iX^i$ denote a finite fps over Z_{p^k} (p prime). Suppose there exist two coefficients a_i, a_j such that $\gcd(p,a_i)=\gcd(p,a_j)=1$, and let n be any multiple of $p^k(k-1)!$. Then, for each fps $C(X)$ we can find $B(X)=\sum_{i\in Z} b_iX^i$ such that*

$$B(X)\in \mathcal{V}^1_{\lfloor n/2\rfloor} \quad \textit{and} \quad B(X)A^n(X)\equiv C(X)\,(\operatorname{mod} p^k). \tag{21}$$

Proof. Let

$$s=\min\{i \mid \gcd(a_i,p)=1\}, \qquad t=\max\{i \mid \gcd(a_i,p)=1\}.$$

Let n be any multiple of $p^k(k-1)!$. By Lemmas A.3 and A.4 in the appendix we know that $A^n(X)$ has the form

$$A^n(X)\equiv \sum_{i=ns}^{nt} a'_iX^i\,(\operatorname{mod} p^k)$$

with $\gcd(a'_{ns},p)=\gcd(a'_{nt},p)=1$.

Let $C(X)=\sum_{i\in Z} c_iX^i$, and $z=\lfloor n/2\rfloor$. By Lemma A.1 there exists $B_+(X)=\sum_{i\geqslant z} b'_iX^i$ such that

$$B_+(X)A^n(X)\equiv \sum_{i\geqslant z+ns} c_iX^i\,(\operatorname{mod} p^k).$$

Similarly, by Lemma A.2 there exists $B_-(X)=\sum_{i<z+ns-nt} b''_iX^i$ such that

$$B_-(X)A^n(X)\equiv \sum_{i<z+ns} c_iX^i\,(\operatorname{mod} p^k).$$

Let $B(X)=B_-(X)+B_+(X)$. Clearly, $B(X)A^n(X)\equiv C(X)\,(\operatorname{mod} p^k)$, and $b_{z+ns-nt}=\cdots=b_{z-1}=0$. Since $z+ns-nt\leqslant \lfloor n/2\rfloor-n\leqslant -\lfloor n/2\rfloor$ we have that $B(X)$ satisfies (21) and the lemma follows. □

Lemma 4.6. *Let $A(X)=\sum_{-r\leqslant i\leqslant r} a_iX^i$ denote a finite fps over Z_m. Suppose that for each prime p which divides m there exist two coefficients a_i, a_j such that $\gcd(p,a_i)=\gcd(p,a_j)=1$. Then, for any integer $q>0$ there exists n such that for each fps $C(X)=\sum_{i\in Z} c_iX^i$ we can find a fps $B(X)=\sum_{i\in Z} b_iX^i$ such that*

$$B(X)\in \mathcal{V}^1_q \quad \textit{and} \quad B(X)A^n(X)\equiv C(X)\,(\operatorname{mod} m). \tag{22}$$

Proof. Let $m=p_1^{k_1}p_2^{k_2}\ldots p_h^{k_h}$, and $k=\max_i k_i$. Let n denote a multiple of $m(k-1)!$ such that $n>2q$. Clearly, n is a multiple of $p_i^{k_i}(k_i-1)!$ for $i=1,\ldots,h$. By Lemma 4.5 we know that given $C(X)$ we can find $B_i(X)=\sum_{j\in Z} b^{(i)}_jX^j$ such that

$$b^{(i)}_{-q+1}=\cdots=b^{(i)}_{q-2}=b^{(i)}_{q-1}=0 \quad \text{and} \quad B_i(X)A^n(X)\equiv C(X)\,(\operatorname{mod} p_i^{k_i}).$$

We now use the Chinese Remainder theorem. Since $\gcd c(p_i^{k_i}, m/p_i^{k_i}) = 1$, we can find β_i such that $\beta_i(m/p_i^{k_i}) \equiv 1 \pmod{p_i^{k_i}}$. Let

$$B(X) = \sum_{i=1}^{h} \beta_i \left(\frac{m}{p_i^{k_i}}\right) B_i(X).$$

For $i = 1,\dots,h$, we have $B(X) \equiv B_i(X) \pmod{p_i^{k_i}}$. Hence, $B(X)A^n(X) \equiv C(X) \pmod{p_i^{k_i}}$ for all i, which implies 22. □

Proof of Theorem 3.5 (Case $D = 1$). The "if" part follows directly from Lemmas 4.4 and 4.6. To prove the "only if" part let $A(X) = \sum_{-r \leqslant i \leqslant r} a_i X^i$ denote the finite fps associated to the map F. Assume there exist a prime p and an index j such that $p \mid m$ and $p \mid a_i$ for all $i \neq j$. Let $a_i^{(n)}$, $-rn \leqslant i \leqslant rn$, denote the coefficients of $A^n(X)$. It is straightforward to verify that, for $i \neq jn$, we have that $p \mid a_i^{(n)}$. Consider now any configuration $b \in \mathscr{V}_1^1$. The corresponding fps $B(X) = \sum_{i \in Z} b(i) X^i$ is such that $b(0) = 0$. We have

$$[F^n(b)](nj) = \langle A^n(X)B(X)\rangle_{nj} = \sum_{i=-rn}^{rn} a_i^{(n)} b(nj - i).$$

Since $b(0) = 0$, all terms in the summation are multiple of p and $p \mid [F^n(b)](nj)$. Hence, the configuration c such that $c(i) = 1$ for all $i \in Z$ clearly does not belong to $F^n(\mathscr{V}_1^1)$, and by (20) F cannot be strongly transitive. □

4.4.1. Extension to the D-dimensional case

We now show how the results of the previous section can be extended to characterize D-dimensional strongly transitive linear CA. As usual, we consider only the case $D = 2$, since the general case is analogous. As for the one-dimensional case we, define the set

$$\mathscr{V}_k^2 = \{x \in \mathscr{C}_m^2 \mid x(\mathbf{v}) = 0 \text{ for } \|\mathbf{v}\|_\infty < k\}.$$

It is straightforward to verify that a result analogous to Lemma 4.4 holds also for $D = 2$. That is, if, for all k, there exists n_k such that $F^{n_k}(\mathscr{V}_k^2) = \mathscr{C}_m^2$, then F is strongly transitive. In view of this, to prove the "if" part of Theorem 3.5 we need results analogous to Lemmas 4.5 and 4.6. We only state and prove the result for $m = p^k$. The extension to the general case follows using the Chinese Remainder theorem as in Lemma 4.6.

Lemma 4.7. *Let*

$$A(X, Y) = \sum_{\substack{v \leqslant i \leqslant w \\ x \leqslant j \leqslant y}} a_{i,j} X^i Y^j,$$

denote a finite fps over Z_{p^k} (p prime). Suppose there exist two coefficients $a_{s,h}$ and $a_{t,l}$ such that $\gcd(p, a_{s,h}) = \gcd(p, a_{t,l}) = 1$, *and let n be a multiple of $p^k(k-1)!$.*

Then, for each fps $C(X,Y)$ we can find $B(X,Y)=\sum_{i,j\in Z} b_{i,j}X^iY^j$ such that

$$B(X,Y)\in \mathscr{V}^2_{\lfloor n/2\rfloor} \quad \textit{and} \quad B(X,Y)A^n(X,Y)\equiv C(X,Y)\,(\mathrm{mod}\, p^k). \tag{23}$$

Proof. By interchanging, if necessary, the role of X and Y we can assume that $s<t$. Moreover, reasoning as in the proof of Lemma 4.5, we can assume that $p|a_{i,j}$ for $i<s$ and $i>t$. By Lemma A.7 and the observation following it, we know that, if n is a multiple of $p^k(k-1)!$, $A^n(X,Y)$ has the form

$$A^n(X,Y)\equiv \sum_{\substack{ns\leqslant i\leqslant nt\\ nx\leqslant j\leqslant ny}} a'_{i,j}X^iY^j\,(\mathrm{mod}\, p^k)$$

and there exist j_n, h_n such that $\gcd(a'_{ns,j_n},p)=\gcd(a'_{nt,h_n},p)=1$.

Let $C(X,Y)=\sum_{i,j\in Z} c_{i,j}X^iY^j$, and $z=\lfloor n/2\rfloor$. By Lemmas A.5 and A.6, we know that there exist

$$B_+(X,Y)=\sum_{i\geqslant z,\, j\in Z} b^+_{i,j}X^iY^j, \qquad B_-(X,Y)=\sum_{i<z+ns-nt,\, j\in Z} b^-_{i,j}X^iY^j$$

such that

$$B_+(X,Y)A^n(X,Y)\equiv \sum_{i\geqslant z+ns,\, j\in Z} c_{i,j}X^iY^j\,(\mathrm{mod}\, p^k),$$

$$B_-(X,Y)A^n(X,Y)\equiv \sum_{i<z+ns,\, j\in Z} c_{i,j}X^iY^j\,(\mathrm{mod}\, p^k).$$

The fps $B(X,Y)=B_-(X,Y)+B_+(X,Y)$ clearly satisfies (23) and the lemma follows. □

Proof of Theorem 3.5 (Case $D=2$). The "if" part follows from the observations at the beginning of this subsection and by Lemma 4.7. To prove the "only if" part, assume there exist a prime p and an index j such that $p|m$ and $p|\lambda_i$ for all $i\neq j$. Reasoning as in the case $D=1$, we can see that the configuration c such that $c(\boldsymbol{v})=1$ for all $\boldsymbol{v}\in Z^2$ does not belong to $F^n(\mathscr{V}^2_1)$ for any $n\geqslant 0$, and, as a consequence, F cannot be strongly transitive. □

5. Conclusions

One of the most interesting and at the same time challenging problem in CA theory is to make explicit the connection between the *global behavior* of a given CA and the local rule on which it is based. In particular, it is of great importance to understand which properties of the local rule influence the qualitative behavior of the entire CA. The qualitative behavior of any dynamical system can be suitably characterized according to the topological properties it satisfies. Among them are the positive expansivity, sensitivity to initial conditions, strong transitivity, and equicontinuity. In this paper we have provided necessary and sufficient conditions on the local rule in order to satisfy the above properties. Finally, by merging set theoretic (injectivity and surjectivity) and topological characterizations we have obtained a complete picture of the relationships between some of the most important CA properties.

Appendix A: Formal power series over Z_{p^k}

In order to simplify the main proofs of the paper, we introduce the following lemmas which prove some properties of fps over Z_{p^k} (p prime).

It is well known that $\gcd(a,m)=1$ implies that there exists a unique integer b, $1 \leqslant b < m$, such that $ab \equiv 1 \pmod m$. In the following we use $[a]_m^{-1}$ to denote such integer.

Lemma A.1. *Let* $A(X)=\sum_{v\leqslant i\leqslant w} a_i X^i$ *denote a finite fps over* Z_{p^k} *(p prime). If* $\gcd(p^k,a_v)=1$, *then, given a fps of the form* $C(X)=\sum_{i\geqslant R} c_i X^i$, *there exists a fps* $B(X)=\sum_{i\geqslant R-v} b_i X^i$ *such that*

$$B(X)A(X)\equiv C(X) \pmod{p^k}.$$

Proof. First note that we can restrict ourselves to the case $R=0$, the general case being analogous. Let $\beta=[a_v]_{p^k}^{-1}$; β exists since $\gcd(a_v,p^k)=1$. Consider the finite fps $D(X)=\beta X^{-v}$. We have

$$D(X)A(X)\equiv 1+\sum_{i=1}^{w-v} e_i X^i \pmod{p^k}.$$

We show that there exists a sequence of values $d_0,d_1,\ldots$ such that $B(X)=\sum_{i\geqslant 0} d_i X^i D(X)$ has the desired properties. We set $d_0=c_0$, and for $i>0$

$$d_i=c_i-\left\langle\left(\sum_{j=0}^{i-1} d_j X^j D(X)\right)A(X)\right\rangle_i .$$

A straightforward induction shows that, for $i\geqslant 0$,

$$\left(\sum_{j=0}^{i} d_j X^j D(X)\right)A(X)\equiv\sum_{j=0}^{i} c_j X^j+\sum_{j>i} z_j^{(i)} X^j \pmod{p^k},$$

which implies that $B(X)A(X)\equiv C(X) \pmod{p^k}$ as claimed. □

With a similar proof we get the following lemma.

Lemma A.2. *Let* $A(X)=\sum_{v\leqslant i\leqslant w} a_i X^i$ *denote a finite fps over* Z_{p^k} *(p prime). If* $\gcd(p^k,a_w)=1$, *then, given a fps of the form* $C(X)=\sum_{i\leqslant R} c_i X^i$, *there exists a fps* $B(X)=\sum_{i\leqslant R-w} b_i X^i$ *such that*

$$B(X)A(X)\equiv C(X) \pmod{p^k}.$$

The hypotheses of Lemmas A.1 and A.2 are rather strong. The following results show that a weaker assumption on $A(X)$ ensures that we can apply Lemmas A.1 or A.2 to $A^n(X)$ when n is a multiple of $p^k(k-1)!$.

Lemma A.3. *Let $A(X)=\sum_{v\leqslant i\leqslant w} a_iX^i$ denote a finite fps over Z_{p^k} (p prime). Suppose there exists an index s such that $p\nmid a_s$, and $p\mid a_i$ for $i<s$. If n is a multiple of $p^k(k-1)!$ then $A^n(X)$ has the form*

$$A^n(X)=\sum_{i=ns}^{nw} a_i'X^i$$

with $\gcd(a_{ns}', p^k)=1$.

Proof. We rewrite $A(X)$ as $A(X)=G(X)+pH(X)$, where $G(X)$ contains all terms a_iX^i such that $p\nmid a_i$. Note that by our hypothesis, a_sX^s is the term with the lowest degree in $G(X)$. Let n be a multiple of $p^k(k-1)!$. We have

$$\begin{aligned}A^n(X)&=(G(X)+pH(X))^n\\&=G^n(X)+\sum_{i=1}^{n}\binom{n}{i}p^iH^i(X)G^{n-i}(X)\\&=G^n(X)+\left(\sum_{i=1}^{k-1}\binom{n}{i}p^iH^i(X)G^{n-i}(X)\right)\\&\quad+p^k\left(\sum_{i=k}^{n}\binom{n}{i}p^{i-k}H^i(X)G^{n-i}(X)\right)\\&=G^n(X)+p^k\left(\sum_{i=k}^{n}\binom{n}{i}p^{i-k}H^i(X)G^{n-i}(X)\right),\end{aligned}$$

where the last equality holds since, being n a multiple of $p^k(k-1)!$, for $i<k$, $\binom{n}{i}$ is a multiple of p^k. Hence, $A^n(X)\equiv G^n(X)\pmod{p^k}$ and the lemma follows. □

Analogously, we can prove the following lemma.

Lemma A.4. *Let $A(X)=\sum_{v\leqslant i\leqslant w} a_iX^i$ denote a finite fps over Z_{p^k} (p prime). Suppose there exists an index t such that $p\nmid a_t$, and $p|a_i$ for $i>t$. If n is a multiple of $p^k(k-1)!$ then $A^n(X)$ has the form*

$$A^n(X)=\sum_{i=nv}^{nt} a_i'X^i$$

with $\gcd(a_{nt}', p^k)=1$.

A.1. Extension to formal power series in two variables

The following results generalize Lemmas A.1–A.4 to finite fps in two variables. We make use of the following notation. Given the fps $H(X,Y)$ and $i\in Z$, $\langle H(X,Y)\rangle_i$

denotes the coefficient of X^i within $H(X,Y)$. Note that $\langle H(X,Y)\rangle_i$ is a fps in the variable Y.

Lemma A.5. *Let*

$$A(X,Y)=\sum_{\substack{v\leqslant i\leqslant w\\ s\leqslant j\leqslant t}} a_{i,j}X^iY^j$$

denote a finite fps over Z_{p^k} (p prime). If there exists j such that $\gcd(a_{v,j},p^k)=1$, *then for each fps $C(X,Y)$ of the form*

$$C(X,Y)=\sum_{i\geqslant R,\, j\in Z} c_{i,j}X^iY^j,$$

there exists a fps $B(X,Y)=\sum_{i\geqslant R-v,\, j\in Z} b_{i,j}X^iY^j$ such that

$$B(X,Y)A(X,Y)\equiv C(X,Y)\,(\bmod\ p^k).$$

Proof. We repeat almost verbatim the proof of Lemma A.1. Again, we can restrict ourselves to the case $R=0$. Let $\alpha(Y)=\langle A(X,Y)\rangle_v$. By hypothesis $\exists j$ such that $\gcd(a_{v,j},p^k)=1$. Hence, the CA associated to the finite fps $\alpha(Y)$ is surjective [10, Theorem 1], and there exists a finite fps $\beta(Y)$ such that $\alpha(Y)\beta(Y)\equiv 1\,(\bmod\ p^k)$. Let $D(X,Y)=X^{-v}\beta(Y)$. We have

$$D(X,Y)A(X,Y)=1+\sum_{i=1}^{w-v}X^iE_i(Y),$$

where $E_1(Y),E_2(Y),\dots,E_{w-v}(Y)$ are finite fps . As in Lemma A.1 we get the desired fps $B(X,Y)$ in the form $B(X,Y)=\sum_{i\geqslant 0}\delta_i(Y)X^iD(X,Y)$, where $\delta_0(Y),\delta_1(Y),\dots$ are defined by the following recurrence. Let $\delta_0(Y)=\langle C(X,Y)\rangle_0$, and for $i>0$

$$\delta_i(Y)=\langle C(X,Y)\rangle_i-\left\langle\left(\sum_{j=0}^{i-1}\delta_j(Y)X^jD(X,Y)\right)A(X,Y)\right\rangle_i.$$

A straightforward induction shows that for every h

$$\left(\sum_{i=0}^{h}\delta_i(Y)X^iD(X,Y)\right)A(X,Y)\equiv\sum_{0\leqslant i\leqslant h,\, j\in Z}c_{i,j}X^iY^j+\sum_{i>h,\, j\in Z}z_{i,j}^{(h)}X^iY^j\,(\bmod\ p^k)$$

and the lemma follows. □

With an analogous proof we get the following result.

Lemma A.6. *Let*

$$A(X,Y)=\sum_{\substack{v\leqslant i\leqslant w\\ s\leqslant j\leqslant t}} a_{i,j}X^iY^j$$

denote a finite fps over Z_{p^k} *(p prime). If there exists j such that* $\gcd(a_{w,j}, p^k) = 1$, *then for each fps* $C(X,Y)$ *of the form*

$$C(X,Y) = \sum_{i \leqslant R,\, j \in Z} c_{i,j} X^i Y^j,$$

there exists a fps $B(X,Y) = \sum_{i \leqslant R-w,\, j\in Z} b_{i,j} X^i Y^j$ *such that*

$$B(X,Y)A(X,Y) \equiv C(X,Y) \,(\mathrm{mod}\, p^k).$$

The following result generalizes Lemma A.3 to finite fps in two variables.

Lemma A.7. *Let*

$$A(X,Y) = \sum_{\substack{v \leqslant i \leqslant w \\ y \leqslant j \leqslant z}} a_{i,j} X^i Y^j$$

denote a finite fps over Z_{p^k} *(p prime). Suppose there exists* $a_{s,u}$ *such that* $p \nmid a_{s,u}$, *and* $i < s$ *implies* $p | a_{i,j}$. *Then, if n is a multiple of* $p^k(k-1)!$, $A^n(X)$ *has the form*

$$A^n(X,Y) = \sum_{\substack{ns \leqslant i \leqslant nw \\ ny \leqslant j \leqslant nz}} a'_{i,j} X^i Y^j \tag{24}$$

and $\exists j$ *such that* $\gcd(a'_{ns,j}, p^k) = 1$.

Proof. As in the proof of Lemma A.3 we write $A(X,Y) = G(X,Y) + pH(X,Y)$ where $G(X,Y)$ contains all terms $a_{i,j}X^iY^j$ such that $p \nmid a_{i,j}$. As in Lemma A.3, if n is a multiple of $p^k(k-1)!$, we have $A^n(X,Y) \equiv G^n(X,Y) \,(\mathrm{mod}\, p^k)$. Let $u = \min\{j \mid \gcd(a_{s,j}, p) = 1\}$. Since $a_{s,u}$ is invertible in Z_{p^k}, we can find $g(X,Y)$ such that $G(X,Y) = a_{s,u}X^sY^u(1 + g(X,Y))$. In addition, our hypotheses on s and u imply that in $g(X,Y)$ the variables X and Y appear with degree $\geqslant 1$. Hence,

$$A^n(X) = [a_{s,u}X^sY^u(1 + g(X,Y))]^n = a^n_{s,u}X^{ns}Y^{nu}(1 + g'(X,Y)),$$

where $g'(X,Y) = \sum_{i=1}^{n} \binom{n}{i} g^i(X,Y)$ still has the property that the variables X, Y appear with degree $\geqslant 1$.

This completes the proof. □

Note that the previous lemma can be generalized to get a result analogous to Lemma A.4. That is, if $\exists a_{t,u}$ such that $p \nmid a_{t,u}$ and $i > t \Rightarrow p | a_{i,j}$, then

$$A^n(X,Y) = \sum_{\substack{nv \leqslant i \leqslant nt \\ ny \leqslant j \leqslant nz}} a'_{i,j} X^i Y^j$$

and $\exists j$ such that $\gcd(a'_{nt,j}, p^k) = 1$.

References

[1] H. Aso, N. Honda, Dynamical characteristics of linear cellular automata, J. Comput. System Sci. 30 (1985) 291–317.

[2] G. Cattaneo, E. Formenti, G. Manzini, L. Margara, Ergodicity, transitivity, and regularity for additive cellular automata over Z_m, Theoret. Comput. Sci., to appear.

[3] P. Chaudhuri, D. Chowdhury, S. Nandi, S. Chattopadhyay, Additive Cellular Automata Theory and Applications, vol. 1, IEEE Press, New York, 1997.

[4] K. Čulik, J. Pachl, S. Yu, On the limit sets of cellular automata, SIAM J. Comput. 18 (1989) 831–842.

[5] K. Čulik, S. Yu, Undecidability of CA classification schemes, Complex Systems 2 (1988) 177–190.

[6] R. L. Devaney, An Introduction to Chaotic Dynamical Systems, 2nd ed., Addison-Wesley, Reading, MA, USA, 1989.

[7] M. Finelli, G. Manzini, L. Margara, Lyapunov exponents vs expansivity and sensitivity in cellular automata, J. Complexity 14 (1998) 210–233.

[8] M. Garzon, Models of Massive Parallelism, EATCS Texts in Theoretical Computer Science, Springer, Berlin, 1995.

[9] P. Guan, Y. He, Exacts results for deterministic cellular automata with additive rules, J. Statist. Phys. 43 (1986) 463–478.

[10] M. Ito, N. Osato, M. Nasu, Linear cellular automata over Z_m, J. Comput. System Sci. 27 (1983) 125–140.

[11] J. Kari, Rice's theorem for the limit set of cellular automata, Theoret. Comput. Sci. 127 (2) (1994) 229–254.

[12] G. Manzini, L. Margara, Attractors of D-dimensional linear cellular automata, 15th Annual Symp. on Theoretical Aspects of Computer Science (STACS '98), Lecture Notes in Computer Science, vol. 1373, Springer, Berlin, 1998, pp. 128–138.

[13] G. Manzini, L. Margara, Invertible linear cellular automata over Z_m: algorithmic and dynamical aspects, J. Comput. System Sci. 56 (1998) 60–67.

[14] T. Sato, Group structured linear cellular automata over Z_m, J. Comput. System Sci. 49 (1) (1994)18–23.

[15] T. Sato, Ergodicity of linear cellular automata over Z_m, Inform. Process. Lett. 61 (3) (1997)169–172.

[16] M. A. Shereshevsky, Expansiveness, entropy and polynomial growth for groups acting on subshifts by automorphisms, Indag. Math. N.S. 4 (1993) 203–210.