Available online at www.sciencedirect.com
SCIENCE DIRECT®
Theoretical Computer Science 325 (2004) 249–271
Theoretical Computer Science
www.elsevier.com/locate/tcs

Solution of some conjectures about topological properties of linear cellular automata ☆

Gianpiero Cattaneo[a], Alberto Dennunzio[a,*], Luciano Margara[b]

[a] Dipartimento di Informatica Sistemistica e Comunicazione, Università degli studi di Milano-Bicocca, via Bicocca degli Arcimboldi 8, 20126 Milano, Italy

[b] Dipartimento di Scienze dell'Informazione, Università di Bologna, via Mura Anteo Zamboni 7, Bologna, Italy

Abstract

We study two dynamical properties of linear D-dimensional cellular automata over $\mathbb{Z}_m$ namely, denseness of periodic points and topological mixing. For what concerns denseness of periodic points, we complete the work initiated in (Theoret. Comput. Sci. 174 (1997) 157, Theoret. Comput. Sci. 233 (1–2) (2000) 147, 14th Annual Symp. on Theoretical Aspects of Computer Science (STACS '97), LNCS n. 1200, Springer, Berlin, 1997, pp. 427–438) by proving that a linear cellular automata has dense periodic points over the entire space of configurations if and only if it is surjective (as conjectured in (Cattaneo et al., 2000)). For non-surjective linear CA we give a complete characterization of the subspace where periodic points are dense. For what concerns topological mixing, we prove that this property is equivalent to transitivity and then easily checkable. Finally, we classify linear cellular automata according to the definition of chaos given by Devaney in (An Introduction to Chaotic Dynamical Systems, 2nd ed., Addison-Wesley, Reading, MA, USA, 1989).

Keywords: Cellular automata; Discrete time dynamical systems; Chaos theory

☆ This work has been supported by MIUR\COFIN project "Formal Languages and Automata: Theory and Applications". This is an extended and improved version of the paper "On Some Topological Properties of Linear Cellular Automata" presented to the 24th International Symposium on Mathematical Foundations of Computer Science (MFCS '99) [18].

* Corresponding author.

E-mail addresses: cattang@disco.unimib.it (G. Cattaneo), dennunzio@disco.unimib.it (A. Dennunzio), margara@cs.unibo.it (L. Margara).

0304-3975/$ - see front matter
doi:10.1016/j.tcs.2004.06.008

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 according to a global transition map F based on a *local rule* f which acts on the value of each single variable in synchronous discrete time steps. A CA can be viewed as a Discrete Time Dynamical System (DTDS) (X, F) where $F: X \to X$ is the CA global transition map defined over the configuration space X. 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, analysis of universal model of computation, cryptography). For an introduction to the CA theory see [12]. 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 [7,8,14]. Despite their simplicity that makes it possible a detailed algebraic analysis, linear CA over $\mathbb{Z}_m$ (CA based on a linear local rule) exhibit many of the complex features of general CA. For a complete and up-to-date reference on applications of linear CA see [6].

Several important dynamical properties of linear CA, e.g., ergodicity, transitivity, sensitivity to initial conditions, and expansivity, have been studied during the last few years and in many cases exact characterizations have been obtained (see for example [13,19,4,15,17,5]). In [16] the authors investigate and completely characterize the structure of attractors for D-dimensional linear CA over $\mathbb{Z}_m$, while in [9] the authors give a closed formula for computing their Lyapunov exponents and their topological entropy.

In this paper we study two important dynamical properties of CA: denseness of periodic points and topological mixing. We first investigate the structure of the set of periodic points of linear CA. In particular we focus our attention on a problem addressed in [5] where the authors prove that for one-dimensional linear CA surjectivity is equivalent to have dense periodic points over the entire space of configurations leaving open the problem of characterizing this last property in the D-dimensional case. Then, we completely characterize topological mixing for linear CA in terms of the coefficients of their local rule.

The main contribution of this paper can be summarized as follows.

- We prove (Theorem 4.6) that for linear D-dimensional CA over $\mathbb{Z}_m$ ($D \geqslant 1$, $m \geqslant 2$) surjectivity is equivalent to have dense periodic points (implicitly characterizing this last property).
- For non-surjective linear D-dimensional CA over $\mathbb{Z}_m$ we explicitly characterize (Corollary 5.2) the largest subspace where periodic points are dense taking advantage of the results obtained in [16] on the attractors of linear CA over $\mathbb{Z}_m$.
- We prove (Theorem 6.2) that for linear D-dimensional CA over $\mathbb{Z}_m$ transitivity is equivalent to topological mixing (implicitly characterizing this last property).
- We completely characterize (Corollary 7.2) the class of chaotic linear D-dimensional CA over $\mathbb{Z}_m$ ($D \geqslant 1$, $m \geqslant 2$) according to one of the most popular definition of chaos, given by Devaney in [10].

The rest of this paper is organized as follows. In Section 2 we give basic definitions and notations. In Section 3 we prove some technical lemmas which will be useful for proving our main results. In Section 4 we prove that for linear CA surjectivity is equivalent to denseness of periodic points. In Section 5 we characterize the subspace where non-surjective linear CA have dense periodic points. In Section 6 we characterize topologically mixing linear CA. In Section 7 we provide an easy-to-check property on the coefficients of the local rule of linear CA which is equivalent to Devaney's definition of chaos. In Section 8 we state some open problems.

2. Basic definitions

2.1. Cellular automata

For $m \geqslant 2$, let $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$. We consider the *space of configurations*

$$\mathcal{C}_m^D = \{c \mid c\colon \mathbb{Z}^D \to \mathbb{Z}_m\},$$

which consists of all functions from $\mathbb{Z}^D$ into $\mathbb{Z}_m$. We can visualize this situation as an infinite D-dimensional lattice $\mathbb{Z}^D$ in which any element of $\mathcal{C}_m^D$ assigns to each cell of the lattice an element of $\mathbb{Z}_m$. Let $s \geqslant 1$. A *neighborhood frame* of size s is an ordered set of distinct vectors $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_s \in \mathbb{Z}^D$. Given a mapping $f\colon \mathbb{Z}_m^s \to \mathbb{Z}_m$, called the *local rule*, a D-dimensional CA based on f is the pair $(\mathcal{C}_m^D, F)$, where $F : \mathcal{C}_m^D \to \mathcal{C}_m^D$ is the *global transition map* defined as follows:

$$F(c)(\vec{v}) = f(c(\vec{v} + \vec{u}_1), \ldots, c(\vec{v} + \vec{u}_s)), \tag{1}$$

where $c \in \mathcal{C}_m^D, \quad \vec{v} \in \mathbb{Z}^D$.

In other words, the content of cell $\vec{v} \in \mathbb{Z}^D$ in the configuration $F(c)$ is a function of the content of cells $\vec{v} + \vec{u}_1, \ldots, \vec{v} + \vec{u}_s$ in the configuration c. Note that the local rule f and the neighborhood frame completely determine F.

In order to study the topological properties of D-dimensional CA, we introduce a distance over the space of the configurations. Let $\delta\colon \mathbb{Z}_m \times \mathbb{Z}_m \to \{0, 1\}$ defined by

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

Given $a, b \in \mathcal{C}_m^D$ the Tychonoff distance $d(a, b)$ is given by

$$d(a, b) = \sum_{\vec{v} \in \mathbb{Z}^D} \frac{\delta(a(\vec{v}), b(\vec{v}))}{2^{|\vec{v}|_\infty}}, \tag{2}$$

where, as usual, $\|\vec{v}\|_\infty$ denotes the maximum of the absolute value of the components of $\vec{v}$. It is easy to verify that d is a metric on $\mathcal{C}_m^D$ and that the metric topology induced by d coincides with the product topology induced by the discrete topology of $\mathbb{Z}_m$. With this topology, $\mathcal{C}_m^D$ is a compact and totally disconnected space and F is a (uniformly) continuous map.

Throughout the paper, $F(c)$ will denote the result of the application of the map F to the configuration c, and $c(\vec{v})$ will denote the value taken by c in $\vec{v}$. For $n \geqslant 0$, we recursively define $F^n(c)$ by $F^n(c) = F(F^{n-1}(c))$, where $F^0(c) = c$. Let $(\mathcal{C}_m^D, F)$ be a CA based on the local rule f. For any integer $n > 0$ the mapping F^n is the global transition mapping of a CA whose local rule will be denoted by $f^{(n)}$.

2.2. Linear CA over $\mathbb{Z}_m$

In order to consider the special case of linear CA, the set $\mathbb{Z}_m$ is endowed with the usual sum and product operations that make it a commutative ring. In what follows we denote by $[x]_m$ the integer x taken modulo m. Linear CA have a local rule of the form $f(x_1, \ldots, x_s) = [\sum_{i=1}^{s} \lambda_i x_i]_m$ with $\lambda_1, \ldots, \lambda_s \in \mathbb{Z}_m$. Hence, for a linear D-dimensional CA equation (1) becomes

$$(F(c))(\vec{v}) = \left[\sum_{i=1}^{s} \lambda_i c(\vec{v} + \vec{u}_i) \right]_m , \tag{3}$$

where $c \in \mathcal{C}_m^D$, $\vec{v} \in \mathbb{Z}^D$.

2.3. Topological properties of discrete time dynamical systems

In this section we recall the definitions of some topological properties which may contribute to determine the qualitative behavior of any general discrete time dynamical systems. Here, we assume that the space of configurations X is equipped with a distance d and that the map F is continuous on X according to the topology induced by d.

Definition 2.1 (Transitivity). A dynamical system (X, F) is (topologically) *transitive* if and only if for all non empty open subsets U and V of X there exists a natural number n such that $F^n(U) \cap V \neq \emptyset$.

Intuitively, a transitive map F has points which eventually move under iteration of F from one arbitrarily small neighborhood to any other. As a consequence, the dynamical system cannot be decomposed into two disjoint open sets which are invariant under the iterations of F.

Definition 2.2 (Topological mixing). A dynamical system (X, F) is *topologically mixing* if and only if for all non empty open subsets U and V of X there exists a natural number n_0 such that for every $n \geqslant n_0$ we have $F^n(U) \cap V \neq \emptyset$.

It is obvious that topological mixing implies transitivity.

Definition 2.3 (Strong transitivity). A dynamical system (X, F) is *strongly transitive* if and only if for any nonempty open set $U \subseteq X$ we have $\bigcup_{n=0}^{+\infty} F^n(U) = X$.

A strongly transitive map F has points which eventually move under iteration of F from one arbitrarily small neighborhood to any other *point*.

Definition 2.4 (Denseness of periodic points). Let

$$P(F) = \{x \in X \mid \exists n \in \mathbb{N}: \ F^n(x) = x\}$$

be the set of the periodic points of F. A dynamical system (X,F) has *dense periodic orbits* if and only if $P(F)$ is a dense subset of X, i.e., for any $x \in X$ and any $\varepsilon > 0$, there exists a periodic point $y \in P(F)$ such that $d(x,y) < \varepsilon$.

Denseness of periodic orbits is often referred to as the *element of regularity* a chaotic dynamical system must exhibit. The popular book by Devaney [10] isolates three components as being the essential features of chaos: transitivity, sensitivity to initial conditions and denseness of periodic orbits.

3. Properties of linear CA

A D-dimensional *cylinder* $\langle(\vec{v}_1,a_1),\dots,(\vec{v}_l,a_l)\rangle$, where $a_i \in \mathbb{Z}_m$ and $\vec{v}_i \in \mathbb{Z}^D$, is a particular subset of $\mathcal{C}_m^D$ defined as

$$\langle(\vec{v}_1,a_1),\dots,(\vec{v}_l,a_l)\rangle = \{c \in \mathcal{C}_m^D \mid c(\vec{v}_i) = a_i, \quad i = 1,\dots,l\}.$$

Note that cylinders form a basis of closed and open (clopen, for short) subsets of $\mathcal{C}_m^D$ according to the metric topology induced by the Tychonoff distance.

We first recall a result proved in [15] which holds for strongly transitive linear CA and states that for every cylinder $C \subseteq \mathcal{C}_m^D$ it is possible to find a natural number t_C such that every configuration of $\mathcal{C}_m^D$ can be reached after exactly t_C iterations of the map F starting from one element of C.

Lemma 3.1 (Manzini and Margara [15]). *Let F be a strongly transitive linear D-dimensional CA over $\mathcal{C}_m^D$. Then for every cylinder $C \subseteq \mathcal{C}_m^D$ there exists a natural number t_C such that*

$$\forall x \in \mathcal{C}_m^D \quad \exists c \in C: F^{t_C}(c) = x.$$

This fact, with a little abuse of notation, will be denoted by $F^{t_C}(C) = \mathcal{C}_m^D$ in the sequel.

Next lemma shows that any linear D-dimensional CA over $\mathcal{C}_{pq}^D$ with p and q relatively prime is topologically conjugated to the map $G = ([F]_p, [F]_q)$ (where, for every $c \in \mathcal{C}_m^D$ we define $[F]_p(c) := [F(c)]_p$ such that $\forall \vec{v} \in \mathbb{Z}^D, [F(c)]_p(v) = [F(c)(v)]_p$). We say that two dynamical systems (X,F) and (X',F') are *conjugated* (resp., *topologically conjugated*) if there exists a bijective mapping (resp., a homeomorphism) $\psi: X \to X'$ such that $\psi(F(x)) = F'(\psi(x))$. If the mapping ψ is continuous and surjective, then (X,F) is said to be topologically semi-conjugated to (X',F') and the system (X',F') is called factor of (X,F).

Lemma 3.2. *Let F be a linear D-dimensional CA over $\mathcal{C}_m^D$ with $m = pq$ and* $\gcd(p,q) = 1$. *Then F is topologically conjugated to the map $G: \mathcal{C}_p^D \times \mathcal{C}_q^D \to \mathcal{C}_p^D \times \mathcal{C}_q^D$*

defined by

$$G(x_1,x_2) = ([F]_p(x_1),[F]_q(x_2)),$$

where $x_1 \in \mathcal{C}_p^D, \quad x_2 \in \mathcal{C}_p^D$.

Proof. We define $\psi : \mathcal{C}_m^D \to \mathcal{C}_p^D \times \mathcal{C}_q^D$ and $\psi^{-1} : \mathcal{C}_p^D \times \mathcal{C}_q^D \to \mathcal{C}_m^D$ as follows: $\psi(x) = ([x]_p,[x]_q)$ and $\psi^{-1}(x_1,x_2) = x_2 + q[(x_1 - x_2)\hat{q}]_p$, where $\hat{q}$ is such that $[q\hat{q}]_p = 1$. Note that $\hat{q}$, the inverse of q modulo p, exists since p and q are relatively prime. The set $\mathcal{C}_p^D \times \mathcal{C}_q^D$ is endowed with the distance $d_\infty = \max\{d(x_1,y_1),d(x_2,y_2)\}$. The following properties of the map ψ are true:
(1) $\psi^{-1}(\psi(x)) = x$ and $\psi(\psi^{-1}(x_1,x_2)) = (x_1,x_2)$,
(2) ψ and ψ^{-1} are continuous, and
(3) $G = \psi \circ F \circ \psi^{-1}$.

To prove property 1 we proceed as follows.

$$\begin{aligned}\psi(\psi^{-1}(x_1,x_2)) &= ([x_2 + q[(x_1 - x_2)\hat{q}]_p]_p,[x_2 + q[(x_1 - x_2)\hat{q}]_p]_q) \\ &= ([x_2]_p + [x_1]_p - [x_2]_p,[x_2]_q) = (x_1,x_2).\end{aligned}$$

To prove that $\psi^{-1}(\psi(x)) = x$ we note that for every $x \in \mathcal{C}_m^D$ there exist $k \in \mathcal{C}_q^D$ and $h \in \mathcal{C}_p^D$ such that $[x]_q + hq = x = [x]_p + kp$ and then $[x]_p = [x]_q + hq - kp$. We may write

$$\begin{aligned}\psi^{-1}(\psi(x)) = \psi^{-1}([x]_p,[x]_q) &= [x]_q + q[([x]_p - [x]_q)\hat{q}]_p \\ &= [x]_q + q[(hq - kp)\hat{q}]_p = [x]_q + q[h]_p = x.\end{aligned}$$

Let us prove now 2. Firstly we show that ψ is continuous. For any $x,y \in \mathcal{C}_m^D$ we trivially have that $d_\infty(\psi(y),\psi(x)) \leqslant d(y,x)$. Thus $\forall x \in \mathcal{C}_m^D \forall \varepsilon > 0 \exists \delta = \varepsilon : \forall y \in \mathcal{C}_m^D$, condition $d(y,x) < \delta$ implies $d_\infty(\psi(y),\psi(x)) \leqslant d(y,x) < \delta = \varepsilon$.

Let $\underline{x} = (x_1,x_2)$, $\underline{y} = (y_1,y_2)$ be two elements of $\mathcal{C}_p^D \times \mathcal{C}_q^D$. In order to prove that ψ^{-1} is continuous, we proceed as follows:

$$\begin{aligned}d(\psi^{-1}(\underline{y}),\psi^{-1}(\underline{x})) &= d(y_2 + q[(y_1 - y_2)\hat{q}]_p,x_2 + q[(x_1 - x_2)\hat{q}]_p) \\ &\leqslant d(y_2,x_2) + d(q[(y_1 - y_2)\hat{q}]_p,q[(x_1 - x_2)\hat{q}]_p) \\ &\leqslant d(y_2,x_2) + d(y_1,x_1) + d(y_2,x_2).\end{aligned}$$

Thus $\forall \underline{x} \in \mathcal{C}_p^D \times \mathcal{C}_q^D, \forall \varepsilon > 0, \exists \delta = \varepsilon/3 : \forall \underline{y} \in \mathcal{C}_p^D \times \mathcal{C}_q^D$, condition $d_\infty(\underline{y},\underline{x}) < \delta$ implies $d(\psi^{-1}(\underline{y}),\psi^{-1}(\underline{x})) < 3\delta = \varepsilon$.

To prove property 3 we proceed as follows:

$$\begin{aligned}\psi \circ F \circ \psi^{-1}(x_1,x_2) &= \psi \circ F(x_2 + q[(x_1 - x_2)\hat{q}]_p) \\ &= ([F(x_2 + q[(x_1 - x_2)\hat{q}]_p)]_p,[F(x_2 + q[(x_1 - x_2)\hat{q}]_p)]_q) \\ &= (y_1,y_2).\end{aligned}$$

From the linearity of F we have

$$y_1 = [F(x_2) + qF([(x_1 - x_2)\hat{q}]_p)]_p = [F(x_2) + q\hat{q}(F(x_1) - F(x_2))]_p$$
$$= [F]_p(x_1).$$

Analogously, we have

$$y_2 = [F(x_2) + qF([(x_1, x_2)\hat{q}]_p)]_q = [F]_q(x_2).$$

Then $G = \psi \circ F \circ \psi^{-1}$ as claimed. $\square$

Lemma 3.2 will be useful to prove both Theorem 4.6 and Theorem 6.2 in the sequel.

Lemma 3.3 (D'amico et al. [9]). *Let F be a linear D-dimensional CA over $\mathcal{C}_{p^k}^D$ with local rule*

$$f(x_1, \ldots, x_s) = \left[\sum_{i=1}^{s} \lambda_i x_i\right]_{p^k}$$

and neighborhood vectors $\vec{u}_1, \ldots, \vec{u}_s$, where p is prime number. Define

$$I = \{i \mid \gcd(\lambda_i, p) = 1\}, \quad \hat{f} = \left[\sum_{i \in I} \lambda_i x_i\right]_{p^k}$$

and let $\hat{F}$ be the global map associated to $\hat{f}$. Then, there exists $h \geqslant 1$ such that for all $c \in \mathcal{C}_{p^k}^D$, we have $F^h(c) = \hat{F}^h(c)$.

Let F be a surjective linear D-dimensional CA over $\mathcal{C}_m^D$. We call F a *shift-like* CA of radius r if and only if there exist $\lambda \in \mathbb{Z}_m$ and $\vec{u} \in \mathbb{Z}^D$ with $\|\vec{u}\|_\infty = r$ such that

$$(F(c))(\vec{v}) = [\lambda c(\vec{v} + \vec{u})]_m \quad \text{where} \quad c \in \mathcal{C}_m^D, \ \vec{v} \in \mathbb{Z}^D.$$

Note that shift-like CA are surjective by definition and then from the characterization of surjective linear CA given in [13] (a CA F is surjective iff $\gcd(\lambda_1, \ldots, \lambda_s, m) = 1$) we conclude that λ and m are relatively prime. Since $[\lambda^{\varphi(m)}]_m = 1$ (where φ is the Euler function), we also have that

$$(F^{\varphi(m)}(c))(\vec{v}) = \lambda^{\varphi(m)} c(\vec{v} + \varphi(m)\vec{u}) = c(\vec{v} + \varphi(m)\vec{u})$$

and then $F^{\varphi(m)}$ is a *true* shift CA if $r > 0$, the identity CA if $r = 0$.

In view of the above considerations, the dynamical behavior of shift-like CA can be easily analyzed. In particular, shift-like CA with radius zero are equicontinuous and then not topologically transitive, while shift-like CA with radius greater than zero are topologically mixing and then transitive but not strongly transitive. Finally, all shift-like CA have dense periodic points. For what concerns true shifts, it easy to show that they exhibit a stronger kind of sensitivity, called strong sensitive dependence to initial conditions as introduced in [2].

Lemma 3.4. *Let F be a surjective but not strongly transitive linear D dimensional CA over $\mathcal{C}_{p^k}^D$ with local rule $f(x_1,\ldots,x_s)=\left[\sum_{i=1}^{s} \lambda_i x_i\right]_{p^k}$, where p is a prime number. Then there exists a positive integer h such that the map F^h is a shift-like CA.*

Proof. Since F is surjective then $\gcd(p^k,\lambda_1,\ldots,\lambda_s)=1$, so there exists at least one λ_i such that $\gcd(\lambda_i, p)=1$. Since F is not strongly transitive then for every pair of coefficients we have that p divides at least one of them (see [15]). As a consequence of the above considerations, the set $I=\{i \mid \gcd(\lambda_i, p)=1\}$ contains exactly one element. The thesis follows from Lemma 3.3. □

4. Periodic points for surjective linear CA

In this section we prove that for linear CA over $\mathbb{Z}_m$ surjectivity implies denseness of periodic points. Since the converse implication was already proven to be true in [5] (for general CA), we conclude that surjectivity is equivalent to denseness of periodic points.

To this end we need the definition of permutive map. A map $f:\mathcal{A}^s\to\mathcal{A}$ is *permutive* in the variable x_i if for any $(a,a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_s)$ belonging to $\mathcal{A}^s$ there exists $x\in\mathcal{A}$ such that $f(a_1,\ldots,a_{i-1},x,a_{i+1},\ldots,a_s)=a$. In other words, f is permutive in the variable x_i if we can force f to output an arbitrary element of $\mathcal{A}$ by acting on the variable i, independently of the values taken by all the other variables. We say that f is leftmost (rightmost) permutive if it is permutive in x_1 (x_s).

Lemma 4.1. *Let F be a one-dimensional CA defined over $\mathcal{A}^{\mathbb{Z}}$ with local rule f, where $\mathcal{A}$ is a possibly infinite alphabet. Let $u_1,\ldots,u_s$ be the neighbor vectors associated with variables $x_1,\ldots,x_s$ of f. Assume that $u_1<0$ and $u_s>0$. Moreover, assume that f is permutive in the variable x_1 and x_s. Then F has dense periodic points over $\mathcal{A}^{\mathbb{Z}}$.*

Proof. Thanks to the permutivity of f, with a light modification of Theorem 1 in [11], it is possible to prove that the one-dimensional CA F is topologically transitive.

Let $\underline{w}=(w_{-k}\cdots w_0\cdots w_k)\in\mathcal{A}^{2k+1}$ be any word on alphabet $\mathcal{A}$ of length $2k+1$, where k is an arbitrarily chosen positive integer. Since F is topologically transitive then there exist a strictly positive integer n and $V_0,W_0\in\mathcal{A}^{\mathbb{Z}}$ such that

$$V_0=(\ldots,\alpha_2,\alpha_1,w_{-k},\ldots,w_0,\ldots,w_k,\beta_1,\beta_2,\ldots)$$
$$W_0=(\ldots,\alpha_2',\alpha_1',w_{-k},\ldots,w_0,\ldots,w_k,\beta_1',\beta_2',\ldots)$$

and

$$F^n(V_0)=W_0.$$

Note that w is centered at the origin of the lattice, i.e., $V_0(0)=W_0(0)=w_0$.

It is easy to show that the local rule $f^{(n)}$ associated to the CA whose global transition mapping is F^n is also leftmost and rightmost permutive. Let us now prove that we are

able to find a configuration $V_1 \in \mathcal{A}^{\mathbb{Z}}$ such that
- $V_1(j) = V_0(j)$ for $|j| \leqslant k+1$,
- $W_1(j) = V_1(j)$ for $|j| \leqslant k+1$,

where $W_1 = F^n(V_1)$.

Indeed let $U^{(n)} = \{z_1, \ldots, z_t\}$ be the neighborhood frame of $f^{(n)}$ with $z_1 < z_2 < \cdots < z_t$, $z_1 = nu_1 < 0$ and $z_t = nu_s > 0$. Since the values $F^n(V_0)(-k), \ldots, F^n(V_0)(k)$ depend only on $V_0(-k+z_1), \ldots, V_0(k+z_t)$ we set $V_1(j) = V_0(j)$ for $j = -k+z_1, \ldots, k+z_t$ being sure that $V_1(j) = V_0(j)$ for $|j| \leqslant k+1$, and thus that $F^n(V_1)(-k) = F^n(V_0)(-k) = W_0(-k) = V_0(-k) = V_1(-k), \ldots, F^n(V_1)(k) = F^n(V_0)(k) = W_0(k) = V_0(k) = V_1(k)$. In order to obtain $F^n(V_1)(-k-1) = V_1(-k-1) = V_0(-k-1) = \alpha_1$, we observe that $F^n(V_1)(-k-1) = f^{(n)}(V_1(-k-1+z_1), V_1(-k-1+z_2), \ldots, V_1(-k-1+z_t))$. Applying the leftmost permutivity of $f^{(n)}$ there exists $x \in \mathcal{A}$ such that $f^{(n)}(x, V_1(-k-1+z_2), \ldots, V_1(-k-1+z_t)) = \alpha_1$. Thus it is sufficient to set $V_1(-k-1+z_1) = x$. Analogously we can set $V_1(k+1+z_t) = y$ where $y \in \mathcal{A}$ is found applying the right permutivity of $f^{(n)}$ in order to obtain $F^n(V_1)(k+1) = V_1(k+1) = V_0(k+1) = \beta_1$. The values of $V_1(j)$ for $j < -k-1+z_1$ and $j > k+1+z_t$ can be chosen arbitrarily.

By repeating the above procedure we are able to construct a sequence of pairs of configurations (V_i, W_i) such that $F^n(V_i) = W_i$ and $V_i(j) = V_{i-1}(j) = W_i(j)$ for $j = -i-k, \ldots, k+i$ and $i = 1, 2, \ldots$.

It is easy to show that $\{V_i\}_{i \in \mathbb{N}}$ and $\{W_i\}_{i \in \mathbb{N}}$ are Cauchy sequences having the same limit W. Moreover we have that $F^n(W) = W$. Indeed $W = \lim_{i\to\infty} W_i = \lim_{i\to\infty} F^n(V_i) = F^n(W)$. Since w can be arbitrarily chosen, we obtain that for any configuration $\underline{x} \in \mathcal{A}^{\mathbb{Z}}$ and for any real number $\varepsilon > 0$, there exists a periodic point W (constructed by the previous procedure starting from the word $w = x_{-k} \cdots x_k$ with $1/2^k < \varepsilon$) such that $d(\underline{x}, W) < \varepsilon$ and we conclude that F has dense periodic orbits. □

Let us note that the previous lemma is valid even if the space $\mathcal{A}^{\mathbb{Z}}$ is not compact.

Lemma 4.2. *Given two non null vectors $\vec{u}, \vec{v} \in \mathbb{Z}^D$, there exists a non null integer $n \in \mathbb{N}$ such that the vector $\vec{u} + n\vec{v}$ has the following property: $\forall i \in \{1, \ldots, D\}$, if either $u_i \neq 0$ or $v_i \neq 0$, then $u_i + nv_i \neq 0$.*

Proof. If either $(u_i = 0) \wedge (v_i \neq 0)$ or $(u_i \neq 0) \wedge (v_i = 0)$ then we have $\forall t \in \mathbb{N}, t > 0$, $u_i + tv_i \neq 0$. On the other hand, if both the conditions $u_i \neq 0$ and $v_i \neq 0$ are satisfied we have the two following cases.

(1) $\forall t \in \mathbb{N}, u_i + tv_i \neq 0$,

(2) $\exists n_i \in \mathbb{N} : u_i + n_i v_i = 0$. In this case n_i is necessarily different from 0; moreover we are sure that $\forall t > n_i, u_i + tv_i \neq 0$.

The above considerations assure us that the thesis is verified if one chooses $n = \max_{1 \leqslant i \leqslant D} \{n_i \mid u_i + n_i v_i = 0\} + 1$ if $\exists i : u_i + n_i v_i = 0$ or $n = 1$ otherwise. □

Lemma 4.3. *Let $U \subset \mathbb{Z}^D$ be a finite set of cardinality greater than one. There exists a hyperplane H_0 in $\mathbb{R}^D$ which can be differently constructed on the basis of the set U in the two following mutually exclusive cases with the respective prescriptions:*

Case 1: Let U contains two linearly independent vectors $\vec{u}, \vec{v} \in U$, then $\vec{u}$ and $\vec{v}$ stay on opposite sides of H_0.

Case 2: *All the vectors of U are pairwise linearly dependent, then H_0 contains all the vectors of U.*

In both cases H_0 possesses the following properties: (i) H_0 is a $D-1$-*dimensional linear subspace of* $\mathbb{R}^D$; (ii) H_0 *can be expressed as a parametric form of a basis whose vectors have integer coordinates and called direction vectors*; (iii) *the integer coordinate vectors of H_0 are expressed by a linear combination of these direction vectors with integer weights.*

Proof.

- *Case* 1: Since $\vec{u}$ and $\vec{v}$ are linearly independent, there exist two components h and k such that

$$u_h v_k - u_k v_h \neq 0. \tag{4}$$

This fact implies that necessarily $(u_h \neq 0 \vee v_h \neq 0)$ and $(u_k \neq 0 \vee v_k \neq 0)$. Thus we are sure that the vector $\vec{z} = \vec{u} + n\vec{v}$ given by Lemma 4.2 has at least the two non null components $z_h \neq 0$ and $z_k \neq 0$. Let $m = \gcd(z_h, z_k) \neq 0$, we can write $\vec{z}$ in the following way:

$$\vec{z} = \begin{pmatrix} \vdots \\ \\ z_h \\ \\ \vdots \\ \\ z_k \\ \vdots \end{pmatrix} = m \begin{pmatrix} \vdots \\ 0 \\ z_h/m \\ 0 \\ \vdots \\ 0 \\ z_k/m \\ 0 \\ \vdots \end{pmatrix} + \sum_{j_i \neq h,k} z_{j_i} \vec{e}_{j_i},$$

where $\vec{e}_{j_i} = (\delta_{k\, i_j})_{k=1,\ldots,D}$, with δ_{ki_j} Kroneker delta, are the vectors of the *canonical basis* of $\mathbb{R}^D$. Vectors $\vec{d}_0 = (z_h/m)\vec{e}_h + (z_k/m)\vec{e}_k$, $\vec{d}_1 = \vec{e}_{j_1}, \ldots, \vec{d}_{D-2} = \vec{e}_{j_{D-2}}$ with $j_1, \ldots, j_{D-2} \neq h, k$ are linearly independent. Let us consider the hyperplane H_0 expressed in parametric form by the vectors $\vec{d}_0, \ldots, \vec{d}_{D-2}$. Now we show that if a vector $\vec{x} = t_0\vec{d}_0 + t_1\vec{d}_1 + \cdots + t_{D-2}\vec{d}_{D-2}$ belongs to $H_0 \cap \mathbb{Z}^D$, then $(t_0, t_1, \ldots, t_{D-2})^{\mathrm{T}} \in \mathbb{Z}^{D-1}$. Indeed for any $i \neq 0$ we have $t_i = x_{j_i} \in \mathbb{Z}$. On the other hand, the coefficient t_0 must be solution of both equations $x_h = t_0 \cdot z_h/m$ and $x_k = t_0 \cdot z_k/m$. Let us assume that $t_0 = n/d \in \mathbb{Q} \backslash \mathbb{Z}$, where $n \in \mathbb{Z}, d \in \mathbb{Z} \backslash \{0, 1, -1\}$. So d must divide both z_h/m and z_k/m, but $\gcd(z_h/m, z_k/m) = 1$, contradiction. Moreover let us show now that the vectors $\vec{u}$ and $\vec{v}$ stay on opposite sides of H_0. First of all, let us prove that both $\vec{u}, \vec{v} \notin H_0$. Indeed assuming $\vec{u} \in H_0$, we have $\vec{u} = r_0\vec{d}_0 + r_1\vec{d}_1 + \cdots + r_{D-2}\vec{d}_{D-2}$ for some $(r_0, r_1, \ldots, r_{D-2})^{\mathrm{T}} \in \mathbb{Z}^{D-1}$. This implies that r_0 must be solution of both equations $u_i = r_0((u_i + nv_i)/m)$, $i = h, k$, i.e., $((r_0 - m)/m)u_i + (r_0 n/m)v_i = 0$, $i = h, k$. From the linear independence of the pair $\vec{u}$ and $\vec{v}$, necessarily both conditions $r_0 = m$ and $r_0 = 0$ must be satisfied. This is a contradiction, hence $\vec{u} \notin H_0$. In a similar way it is possible to show that $\vec{v} \notin H_0$. Finally, since $\vec{u} + n\vec{v} \in H_0$ we can conclude that $\vec{u}$ and $\vec{v}$ stay on opposite sides of H_0.

- *Case* 2: Let $\vec{u} \neq \vec{0}$ be a vector of U (which certainly exists owing to the hypothesis). If $\vec{u}$ possesses a unique non null component $u_h \neq 0$, then the hyperplane H_0 expressed in parametric form by the vectors of the canonical basis $\vec{e}_h, \vec{e}_{j_1}, \ldots, \vec{e}_{j_{D-2}}$, for any choice of $D-2$ distinct indices $j_1, \ldots, j_{D-2} \neq h$, satisfies the required conditions.

  On the contrary, let $u_h \neq 0$ and $u_k \neq 0$ be two non null components of $\vec{u}$, then we can write $\vec{u}$ in the following way:

$$\vec{u} = \begin{pmatrix} \vdots \\ \\ u_h \\ \\ \vdots \\ \\ u_k \\ \\ \vdots \end{pmatrix} = m \begin{pmatrix} \vdots \\ 0 \\ u_h/m \\ 0 \\ \vdots \\ 0 \\ u_k/m \\ 0 \\ \vdots \end{pmatrix} + \sum_{j_i \neq h,k} u_{j_i} \vec{e}_{j_i},$$

  where $m = \gcd(u_h, u_k) \neq 0$. The hyperplane H_0 expressed in parametric form by the vectors $(z_h/m)\vec{e}_h + (z_k/m)\vec{e}_k$, $\vec{e}_{j_1}, \ldots, \vec{e}_{j_{D-2}}$ with $j_1, \ldots, j_{D-2} \neq h, k$, satisfies the required conditions. $\square$

Lemma 4.4. *Let F be a linear D-dimensional CA over $\mathcal{C}_{p^k}^D$ where p is a prime number. Then it is a factor of a one-dimensional CA F^* over $(\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$ which can be differently constructed on the basis of the CA neighborhood U in the two following mutually exclusive cases with the respective prescriptions*:

Case 1: *Let U contains two linearly independent vectors $\vec{u}, \vec{v} \in U$.*

Case 2: *All the vectors of U are pairwise linearly dependent.*

Moreover, denoting by f the local rule of the D-dimensional CA, the local rule f^* of the one-dimensional CA has the following properties:

Case 1: *If all the coefficients of f are prime with p, then f^* is permutive in each variable.*

Case 2: *f^* is the global transition mapping of a linear $(D-1)$-dimensional whose local rule coincides with f.*

Proof. In order to obtain the thesis we take the $\mathcal{C}_{p^k}^D$ and we split it (along a suitable $D-1$ dimensional hyperplane H_0 containing infinite points of integer coordinates) into "slices". Slicing takes place according to the neighbor structure of F as follows:

- *Case* 1: *There exists a pair $\vec{u}$, $\vec{v}$ of independent neighbor vectors.*

Thanks to the Lemma 4.3 we can construct a $D-1$ dimensional hyperplane H_0 expressed in a parametric form using the $D-1$ independent vectors $\vec{d}_0, \vec{d}_1, \ldots, \vec{d}_{D-2}$ of integer coordinates where for every $i \neq 0$ the vector $\vec{d}_i$ is an element of the canonical basis (see proof of Lemma 4.3). The construction is such that the set $H_0^* = H_0 \cap \mathbb{Z}^D$ contains vectors of the form $\vec{x}=t_0\vec{d}_0+t_1\vec{d}_1+\cdots+t_{D-2}\vec{d}_{D-2}$ where $\vec{t}=(t_0,t_1,\ldots,t_{D-2})\in\mathbb{Z}^{D-1}$. The mapping $\varphi: H_0\cap\mathbb{Z}^D\mapsto\mathbb{Z}^{D-1}$ associating to any $\vec{x}\in H_0\cap\mathbb{Z}^D$ the tuple $\varphi(\vec{x})=\vec{t}$ is a group isomorphism with respect to the standard operations. Moreover $\vec{u}$ and $\vec{v}$ stay on opposite sides of H_0. Let us remark that the inverse $\varphi^{-1}:\mathbb{Z}^{D-1}\mapsto H_0\cap\mathbb{Z}^D$ is defined by the law

$$\forall\vec{t}=(t_0,t_1,\ldots,t_{D-2})\in\mathbb{Z}^{D-1}\overset{\varphi^{-1}}{\to}\varphi^{-1}(\vec{t})=t_0\vec{d}_0+t_1\vec{d}_1+\cdots+t_{D-2}\vec{d}_{D-2}.$$

Let us consider now the family $\mathcal{H}$ constituted by all the hyperplanes parallel to H_0 containing at least a point of integer coordinates (trivially for any vector $\vec{x}\in\mathbb{Z}^D$ there exists a hyperplane parallel to H_0 which contains this vector). We want to show that $\mathcal{H}$ is in a one-to-one correspondence to $\mathbb{Z}$. We remark that $\mathcal{H}$ induced a partition of $\mathbb{Z}^D$ by the equivalence relation $\sim$ over $\mathbb{Z}^D$ defined as follows: for every $\vec{x},\vec{y}\in\mathbb{Z}^D$, $\vec{x}\sim\vec{y}$ iff $\vec{x}$ and $\vec{y}$ belong to the same hyperplane parallel to H_0. Thus the cardinality of $\mathcal{H}$ cannot be greater than the cardinality of $\mathbb{Z}^D$ which trivially has the same cardinality of $\mathbb{Z}$, i.e., the cardinality of $\mathcal{H}$ must be either finite or numerable. Let us show that the cardinality of $\mathcal{H}$ cannot be finite. Indeed let us assume that $\mathcal{H}$ is constituted by the n hyperplanes $H_1,\ldots,H_n$. Let $l_a=[\vec{e}_a]$ be the one-dimensional subspace of $\mathbb{R}^D$ generated by a vector $\vec{e}_a$ of the canonical basis which is not contained in H_0. Let $\vec{x}_1,\ldots,\vec{x}_n\in\mathbb{R}^D$ be the points obtained by intersection of $H_1,\ldots,H_n$ with l_a. Denoting by $\xi\in\mathbb{Z}$ the first integer strictly greater than $\max_{1\leqslant i\leqslant n}\{(\vec{x}_i)_a\}$, there is no hyperplane belonging to $\mathcal{H}$ and passing for the point $\xi\vec{e}_a$, contradiction.

We adopt the numeration of the hyperplanes of $\mathcal{H}$ made in a such way that for every $i,j\in\mathbb{Z}$ the corresponding hyperplanes H_i and H_j satisfy the condition: $i<j$ iff $p_i<p_j$, where $\vec{p}_i=p_i\vec{e}_a$ and $\vec{p}_j=p_j\vec{e}_a$ are the intersection points between l_a and H_i and H_j, respectively. Let $\vec{p}_1=p_1\vec{e}_a$ be the intersection point between l_a and H_1 (this means that $p_1=\min_{i>0}\{p_i, \vec{p}_i=p_i\vec{e}_a\in l_a\cap H_i\}$). We want to show that if $\vec{x}\in\mathbb{Z}^D$ then there exists $i\in\mathbb{Z}$ such that $\vec{x}=ip_1\vec{e}_a+t_0\vec{d}_0+t_1\vec{d}_1+\cdots+t_{D-2}\vec{d}_{D-2}$ for some $t_0,\ldots,t_{D-2}\in\mathbb{R}$. Let H_x be the hyperplane passing for $\vec{x}$ and parallel to H_0 and let $p_x\vec{e}_a$, with $p_x\in\mathbb{R}$, be the intersection point between l_a and H_x. Points of the hyperplane H_x can be expressed by the expression $p_x\vec{e}_a+t_0\vec{d}_0+t_1\vec{d}_1+\cdots+t_{D-2}\vec{d}_{D-2}$. Let us assume that $\forall i\in\mathbb{Z}, p_x\neq ip_1$. Supposing $p_x>0$, let us consider now the hyperplane whose parametric form is $(p_x-i'p_1)\vec{e}_a+t_0\vec{d}_0+t_1\vec{d}_1+\cdots+t_{D-2}\vec{d}_{D-2}$, where i' is the integer such that $i'p_1<p_x<(i'+1)p_1$. This hyperplane contains at least one point of integer coordinates and its intersection point with l_a $(p_x-i'p_1)\vec{e}_a$ is such that $p_x-i'p_1<p_1$. Since this fact is contrary to the definition of p_x, we obtain a contradiction. (Analogously for $p_x<0$). Thus each $\vec{x}\in\mathbb{Z}^D$ can be expressed as $ip_1\vec{e}_a+t_0\vec{d}_0+t_1\vec{d}_1+\cdots+t_{D-2}\vec{d}_{D-2}$ for some $i\in\mathbb{Z}$ and some $t_0,\ldots,t_{D-2}\in\mathbb{R}$. Let us note that the integer $i\in\mathbb{Z}$ individuates just the hyperplane H_i since $ip_1\vec{e}_a$ represent the point of intersection between l_a and the hyperplane $\vec{x}$ belongs to. In particular we observe that

$$\forall i,j\in\mathbb{Z}\quad\text{if } \vec{x}\in H_i \quad\text{and}\quad \vec{y}\in H_j \quad\text{then } \vec{x}+\vec{y}\in H_{i+j}. \tag{$*$}$$

Let $\vec{y}_1\in\mathbb{Z}^D$ be an arbitrary but fixed vector belonging to H_1. For any $i\in\mathbb{Z}$, we define the vector $\vec{y}_i=i\vec{y}_1$ which, by ($\star$), belongs to $H_i\cap\mathbb{Z}^D$. In this way a bi-infinite sequence of vectors $\Sigma = \{\vec{y}_i \in H_i \cap \mathbb{Z}^D : i \in \mathbb{Z}\}$ is singled out. In the sequel each hyperplane H_i will be expressed in parametric form by the expression $\vec{y}_i + (t_0\vec{d}_0 + t_1\vec{d}_1 + \cdots + t_{D-2}\vec{d}_{D-2}) = \vec{y}_i + \vec{x}_0$, with $\vec{y}_i \in \Sigma$ and $\vec{x}_0 = t_0\vec{d}_0 + t_1\vec{d}_1 + \cdots + t_{D-2}\vec{d}_{D-2}$ running on H_0.

Let us summarize the situation. We have a numerable collection $\mathcal{H} = \{H_i : i \in \mathbb{Z}\}$ of hyperplanes parallel to H_0 inducing a partition of $\mathbb{Z}^D$. Let us define $H_i^* = H_i \cap \mathbb{Z}^D$, then $\mathbb{Z}^D = \bigcup_{i \in \mathbb{Z}} H_i^*$ (partition). Therefore, any configuration $c \in \mathcal{C}_{p^k}^D$, i.e., any mapping $c : \mathbb{Z}^D \mapsto \mathbb{Z}_{p^k}$, can be viewed as a mapping $c : \bigcup_{i \in \mathbb{Z}} H_i^* \mapsto \mathbb{Z}_{p^k}$. For every $i \in \mathbb{Z}$, the slice c_i over the hyperplane H_i of the configuration c is the mapping $c_i : H_i^* \mapsto \mathbb{Z}_{p^k}$, which is the restriction of c to the set $H_i^* \subset \mathbb{Z}^D$. In this way, a configuration $c \in \mathcal{C}_{p^k}^D$ can be expressed as the bi-infinite one-dimensional sequence $\prec c \succ = (\ldots, c_{-2}, c_{-1}, c_0, c_1, c_2, \ldots)$ of its slices $c_i \in \mathbb{Z}_{p^k}^{H_i^*}$ where the ith component of the sequence $\prec c \succ$ is $\prec c \succ_i = c_i$. Let us stress that each slice c_i is defined only over the set H_i^*. Moreover $\forall \vec{x} \in \mathbb{Z}^D, \exists! i \in \mathbb{Z} : \vec{x} \in H_i^*$ and in this case we identify $\prec c \succ (\vec{x}) \equiv \prec c \succ_i (\vec{x}) = c_i(\vec{x}) = c(\vec{x}) \in \mathbb{Z}_{p^k}$.

The identification of any configuration $c \in \mathcal{C}_{p^k}^D$ with the corresponding bi-infinite sequence of slices $c \equiv \prec c \succ = (\ldots, c_{-2}, c_{-1}, c_0, c_1, c_2, \ldots)$, allows one to introduce a new one-dimensional bi-infinite CA over the alphabet $\mathcal{C}_{p^k}^{D-1}$ expressed by a global transition mapping $F^* : (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}} \mapsto (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$ which associates to any configuration $a : \mathbb{Z} \mapsto \mathcal{C}_{p^k}^{D-1}$ a new configuration $F^*(a) : \mathbb{Z} \mapsto \mathcal{C}_{p^k}^{D-1}$. The local rule f^* of this new CA we are going to define will take a certain number of configurations of $\mathcal{C}_{p^k}^{D-1}$ as input and will produce a new configuration of $\mathcal{C}_{p^k}^{D-1}$ as output.

Precisely, let us consider the hyperplanes $H_{n_1}, H_{n_2}, \ldots, H_{n_l}$, with $n_1, \ldots, n_l \in \mathbb{Z}$, $n_1 < \cdots \leqslant 0 \leqslant \cdots < n_l$ and $2 \leqslant l \leqslant s$, parallel to H_0 and passing for the neighbor vectors ($l \leqslant s$ since different neighbor vectors can belong to the same hyperplane). For any positive integer $i \leqslant l$ we denote by $\vec{z}_{n_i,1}, \ldots, \vec{z}_{n_i,r_i} \in \{\vec{u}_1, \ldots, \vec{u}_s\}$ the neighbor vectors laying on the same hyperplane H_{n_i} (we have $\sum_{i=1}^{l} r_i = s$) and by $\lambda_{n_i,1}, \ldots, \lambda_{n_i,r_i}$ the corresponding coefficients of the local rule. Let us note that for any $t = 1, \ldots, s$, there exists a pair n_i, j such that $\vec{u}_t = \vec{z}_{n_i,j}$ and $\lambda_t = \lambda_{n_i,j}$ and vice versa. The set $\{n_1, n_2, \ldots, n_l\}$ is the neighborhood of the one-dimensional CA we are going to construct. In order to express formally the local rule of the new CA, we introduce some useful mappings.

Firstly, for each $h \in \mathbb{Z}$, we define the bijective mapping $T_h : \mathbb{Z}_{p^k}^{H_h^*} \mapsto \mathbb{Z}_{p^k}^{H_0^*}$ which associates to any slice c_h over the hyperplane H_h the slice $T_h(c_h)$

$$\left(c_h : H_h^* \mapsto \mathbb{Z}_{p^k}\right) \quad \overset{T_h}{\to} \quad (T_h(c_h) : H_0^* \mapsto \mathbb{Z}_{p^k})$$

defined as follows:

$$\forall \vec{x} \in H_0^*, \ \text{owing to } (*) \text{ we have } \vec{x} + \vec{y}_h \in H_h^* \text{ and } T_h(c_h)(\vec{x}) = c_h(\vec{x} + \vec{y}_h).$$

Let us note that the mapping $T_h^{-1} : \mathbb{Z}_{p^k}^{H_0^*} \mapsto \mathbb{Z}_{p^k}^{H_h^*}$ associates to any slice c_0 over the hyperplane H_0 the slice $T_h^{-1}(c_0)$ over the hyperplane H_h such that $\forall \vec{x} \in H_h^*$, $T_h^{-1}(c_h)(\vec{x}) = c_0(\vec{x} - \vec{y}_h)$.

We denote by $\Phi_0 : \mathbb{Z}_{p^k}^{H_0^*} \mapsto \mathcal{C}_{p^k}^{D-1}$ the bijective mapping putting in correspondence any $c_0 : H_0^* \mapsto \mathbb{Z}_{p^k}$ with the configuration $\Phi_0(c_0) \in \mathcal{C}_{p^k}^{D-1}$,

$$(c_0 : H_0^* \mapsto \mathbb{Z}_{p^k}) \quad \xrightarrow{\Phi_0} \quad (\Phi_0(c_0) : \mathbb{Z}^{D-1} \mapsto \mathbb{Z}_{p^k})$$

defined as follows:

$$\forall \vec{t} \in \mathbb{Z}^{D-1}, \quad \Phi_0(c_0)(\vec{t}) := c_0(\varphi^{-1}(\vec{t})) \in \mathbb{Z}_{p^k}$$

(equivalently we have that $\forall \vec{x} \in H_0^*, \quad \Phi_0(c_0)(\varphi(\vec{x})) = c_0(\vec{x})$).

Let us stress that the mapping $\Phi_0^{-1} : \mathcal{C}_{p^k}^{D-1} \mapsto \mathbb{Z}_{p^k}^{H_0^*}$ associates to any configuration $a \in \mathcal{C}_{p^k}^{D-1}$ the configuration $\Phi_0^{-1}(a) \in \mathbb{Z}_{p^k}^{H_0^*}$ in the following way:

$$\forall \vec{x} \in H_0^*, \quad \Phi_0^{-1}(a)(\vec{x}) = a(\varphi(\vec{x})).$$

For each $i = 1, \ldots, l$, we denote by $\Omega_i : \mathcal{C}_{p^k}^{D-1} \mapsto \mathcal{C}_{p^k}^{D-1}$ the bijective mapping associating to any configuration $a : \mathbb{Z}^{D-1} \mapsto \mathbb{Z}_{p^k}$ the configuration $\Omega_i(a) : \mathbb{Z}^{D-1} \mapsto \mathbb{Z}_{p^k}$

$$(a : \mathbb{Z}^{D-1} \mapsto \mathbb{Z}_{p^k}) \quad \xrightarrow{\Omega_i} \quad (\Omega_i(a) : \mathbb{Z}^{D-1} \mapsto \mathbb{Z}_{p^k})$$

defined as follows:

$$\forall \vec{t} \in \mathbb{Z}^{D-1}, \quad \Omega_i(a)(\vec{t}) := a(\vec{t} + \varphi(\vec{z}_{n_i,1} - \vec{y}_{n_i})).$$

For any $i \in \{1, \ldots, l\}$, we define $F_i : \mathcal{C}_{p^k}^{D-1} \mapsto \mathcal{C}_{p^k}^{D-1}$ the mapping such that:

$$F_i(a)(\vec{t}) = \left[\sum_{j=1}^{r_i} \lambda_{n_i,j} a(\vec{t} + \varphi(\vec{z}_{n_i,j} - \vec{z}_{n_i,1})) \right]_{p^k},$$

where $a \in \mathcal{C}_{p^k}^{D-1}$, $\vec{t} \in \mathbb{Z}^{D-1}$.

Comparing with (3), each F_i can be viewed as the global transition mapping of a $D-1$-dimensional linear cellular automaton whose r_i neighborhood vectors are $\varphi(\vec{z}_{n_i,j} - \vec{z}_{n_i,1}) \in \mathbb{Z}^{D-1}$ with $j = 1, \ldots, r_i$. We introduce now the local rule $f^* : (\mathcal{C}_{p^k}^{D-1})^l \mapsto \mathcal{C}_{p^k}^{D-1}$ defined as follows:

$$\forall (a_1, \ldots, a_l) \in (\mathcal{C}_{p^k}^{D-1})^l, \quad f^*(a_1, \ldots, a_l) = \Omega_1(F_1(a_1)) \oplus \cdots \oplus \Omega_l(F_l(a_l)),$$

where $\forall b_1, b_2 \in \mathcal{C}_{p^k}^{D-1}, \vec{t} \in \mathbb{Z}^{D-1}$, $(b_1 \oplus b_2)(\vec{t}) = [b_1(\vec{t}) + b_2(\vec{t})]_{p^k}$. The one-dimensional CA we are going to construct is based on the neighborhood $\{n_1, \ldots, n_l\}$ and on the local rule f^*. The global transition mapping of this new CA is $F^* : (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}} \mapsto (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$ and the link between F^* and f^* is given as usual by $(F^*(a))_i = f^*(a_{i+n_1}, \ldots, a_{i+n_l})$ where $a = (\ldots, a_{-1}, a_0, a_1, \ldots) \in (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$ and $i \in \mathbb{Z}$. We now show that

(1) the DTDS $(\mathcal{C}_{p^k}^D, F)$ is conjugated to the DTDS $((\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}, F^*)$ by the bijective mapping $\Psi : \mathcal{C}_{p^k}^D \mapsto (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$ defined as follows:

$$\forall c \in \mathcal{C}_{p^k}^D, \quad \Psi(c) = (\ldots, \Phi_0(T_{-1}(c_{-1})), \Phi_0(T_0(c_0)), \Phi_0(T_1(c_1)), \ldots)$$

(2) the mapping $\Psi^{-1} : (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}} \mapsto \mathcal{C}_{p^k}^{D}$

$$\forall a \in (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}, \quad \Psi^{-1}(a) = (\ldots, T_{-1}^{-1}(\Phi_0^{-1}(a_{-1})),\ T_0^{-1}(\Phi_0^{-1}(a_0)),\ T_1^{-1}(\Phi_0^{-1}(a_1)), \ldots)$$

is continuous.

Let us prove claim 1, i.e., that the following diagram commutes:

$$\begin{array}{ccc} \mathcal{C}_{p^k}^{D} & \xrightarrow{F} & \mathcal{C}_{p^k}^{D} \\ \Psi \downarrow & & \downarrow \Psi \\ (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}} & \xrightarrow[F^*]{} & (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}} \end{array}$$

Let us show that $\Psi \circ F = F^* \circ \Psi$, i.e., that $\forall \vec{t} \in \mathbb{Z}^{D-1}, \forall i \in \mathbb{Z}, \forall c \in \mathcal{C}_{p^k}^{D}$, $(\Psi(F(c)))_i(\vec{t}) = (F^*(\Psi(c)))_i(\vec{t}) \in \mathbb{Z}_{p^k}$. Let us start to calculate $(\Psi(F(c)))_i(\vec{t})$:

$$\begin{aligned}(\Psi(F(c)))_i(\vec{t}) &= (F(c))_i(\varphi^{-1}(\vec{t}) + \vec{y}_i) \\ &= F(c)(\varphi^{-1}(\vec{t}) + \vec{y}_i) \\ &= \left[\sum_{\alpha=1}^{s} \lambda_\alpha c(\varphi^{-1}(\vec{t}) + \vec{y}_i + \vec{u}_\alpha)\right]_{p^k}.\end{aligned}$$

On the other hand

$$\begin{aligned}(F^*(\Psi(c)))_i(\vec{t}) &= f^*((\Psi(c))_{i+n_1}, \ldots, (\Psi(c))_{i+n_l})(\vec{t}) \\ &= \left[\sum_{h=1}^{l} \Omega_h(F_h(\Phi_0(T_{i+n_h}(c_{i+n_h}))))(\vec{t})\right]_{p^k} \\ &= \left[\sum_{h=1}^{l} \sum_{j=1}^{r_h} \lambda_{n_h,j} c_{i+n_h}(\varphi^{-1}(\vec{t}) + \vec{z}_{n_h,j} + \vec{y}_i)\right]_{p^k} \\ &= \left[\sum_{\alpha=1}^{s} \lambda_\alpha c(\varphi^{-1}(\vec{t}) + \vec{y}_i + \vec{u}_\alpha)\right]_{p^k}.\end{aligned}$$

We now prove the claim 2, i.e., that Ψ^{-1} is continuous mapping from the metric space $(\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$ to the metric space $\mathcal{C}_{p^k}^{D}$, both equipped with the suitable Tychonoff metric, which for the sake of simplicity is denoted by the same symbol d. It is easy to show the two following properties involving the Tychonoff metric.

For any pair of configurations $c, c' \in \mathcal{C}_m^D$, such that $\forall \vec{v} \in \mathbb{Z}^D\ c(\vec{v}) = c'(\vec{v})$, with $\|\vec{v}\|_\infty \leqslant n$, we have $d(c, c') < \sum_{i=n+1}^{+\infty} (2i+1)^D - (2i-1)^D/2^i$. On the other hand, if $d(c, c') < 1/2^n$ then $\forall \vec{v} \in \mathbb{Z}^D$, with $\|\vec{v}\|_\infty \leqslant n$, we have $c(\vec{v}) = c'(\vec{v})$.

Let $\mathcal{A}$ be a possibly infinite alphabet. For any pair of configurations $\underline{x}, \underline{y} \in \mathcal{A}^{\mathbb{Z}}$, if $x_i = y_i\ \forall i, |i| \leqslant n$ then we have $d(\underline{x}, \underline{y}) < 1/2^{n-1}$. On the other hand, if $d(\underline{x}, \underline{y}) < 1/2^n$ then we have $x_i = y_i\ \forall i, |i| \leqslant n$.

Let us choose an arbitrary configuration $a = (\ldots, a_{-1}, a_0, a_1, \ldots) \in (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$ and a real number $\varepsilon > 0$. Let n be a positive integer such that the condition $\sum_{i=n+1}^{+\infty} (2i+1)^D -$

$(2i-1)^D/2^i < \varepsilon$ holds. Consider the hyperplanes H_i, $\mu \leqslant i \leqslant \nu$ for some $\mu, \nu \in \mathbb{Z}$, which intersect the closed ball $K_n(\vec{0}) = \{\vec{x} \in \mathbb{R}^D : \|\vec{x}\|_\infty \leqslant n\}$. Setting $\delta = 1/2^{\max\{|\mu|,|\nu|\}}$, for any configuration $b \in (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$ such that $d(b,a) < \delta$, we have that $b_i = a_i$ for each $i \in \mathbb{Z}, \mu \leqslant i \leqslant \nu$. This fact implies that $(\Psi^{-1}(a))_i = (\Psi^{-1}(b))_i$, for $\mu \leqslant i \leqslant \nu$, and thus that $(\Psi^{-1}(a))_i(\vec{x}) = (\Psi^{-1}(b))_i(\vec{x})$, for $i \in \mathbb{Z}, \mu \leqslant i \leqslant \nu$ and for any $\vec{x} \in H_i^*$. Therefore we have that $(\Psi^{-1}(a))(\vec{x}) = (\Psi^{-1}(b))(\vec{x})$, for any $\vec{x} \in H_i^*$, with $\mu \leqslant i \leqslant \nu$ and in particular for any $\vec{x} \in K_n(\vec{0})$. So we have obtained that $d(\Psi^{-1}(b), \Psi^{-1}(a)) < \varepsilon$. In conclusion, Ψ^{-1} is continuous. This fact implies that in particular the DTDS $((\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}, F^*)$ is topologically semi-conjugated to the DTDS $(\mathcal{C}_{p^k}^{D}, F)$ by the surjective and continuous conjugation Ψ^{-1}.

Let us note that, if all the coefficients of F are prime with p, the local rule f^* is permutive in each variable a_i since both the mapping F_i and Ω_i are surjective. Indeed, for any i, chosen arbitrarily $a, a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_l \in \mathcal{C}_{p^k}^{D-1}$, thanks to the surjectivity of F_i and Ω_i, there exists a configuration $a_i \in \mathcal{C}_{p^k}^{D-1}$ such that $\Omega_i(F_i(a_i)) = a \ominus (\Omega_1(F_1(a_1)) \oplus \cdots \oplus \Omega_{i-1}(F_{i-1}(a_{i-1})) \oplus \Omega_{i+1}(F_{i+1}(a_{i+1})) \oplus \cdots \oplus \Omega_l(F_l(a_l)))$ where $\ominus$ is the inverse operation of $\oplus$. This fact means that $a = \Omega_1(F_1(a_1)) \oplus \cdots \oplus \Omega_l(F_l(a_l))$ and thus f^* is permutive in the variable a_i.

- *Case* 2: *All the neighbor vectors are pairwise linearly dependent*.

Thanks to the Lemma 4.3 we can choose a hyperplane H_0 containing all the neighbor vectors and having equation $\vec{x}(\vec{t}) = t_0\vec{d}_0 + t_1\vec{d}_1 + \cdots + t_{D-2}\vec{d}_{D-2}$ for suitable vectors $\vec{d}_0, \vec{d}_1, \ldots, \vec{d}_{D-2} \in \mathbb{Z}^D$, where $\vec{t} = (t_0, t_1, \ldots, t_{D-2}) \in \mathbb{Z}^{D-1}$. Slicing the space according to H_0 like in the case 1, the one-dimensional CA which is conjugated to the D-dimensional CA by Ψ is based on a neighborhood constituted by the null vector and on a local rule $f^* : \mathcal{C}_{p^k}^{D-1} \mapsto \mathcal{C}_{p^k}^{D-1}$ that depends on one variable and that associates to any configuration $d \in \mathcal{C}_{p^k}^{D-1}$ the configuration $f^*(d) \in \mathcal{C}_{p^k}^{D-1}$ defined as follows:

$$\forall \vec{t} \in \mathbb{Z}^{D-1}, \quad f^*(d)(\vec{t}) = \left[\sum_{i=1}^{s} \lambda_i d(\vec{t} + \varphi(\vec{u}_i))\right]_{p^k}.$$

Let us prove that $F^* \circ \Psi = \Psi \circ F$. For any $\vec{t} \in \mathbb{Z}^{D-1}$, for any $i \in \mathbb{Z}$ and for any $c \in \mathcal{C}_{p^k}^{D}$ we have

$$\begin{aligned}(F^*(\Psi(c)))_i(\vec{t}) &= f^*((\Psi(c))_i)(\vec{t}) \\ &= \left[\sum_{\alpha=1}^{s} \lambda_\alpha c_i(\varphi^{-1}(\vec{t}) + \vec{u}_\alpha + \vec{y}_i)\right]_{p^k} \\ &= \left[\sum_{\alpha=1}^{s} \lambda_\alpha c(\varphi^{-1}(\vec{t}) + \vec{u}_\alpha + \vec{y}_i)\right]_{p^k}\end{aligned}$$

and that

$$\begin{aligned}(\Psi(F(c)))_i(\vec{t}) &= (F(c))_i(\varphi^{-1}(\vec{t}) + \vec{y}_i) \\ &= (F(c))(\varphi^{-1}(\vec{t}) + \vec{y}_i) \\ &= \left[\sum_{\alpha=1}^{s} \lambda_\alpha c(\varphi^{-1}(\vec{t}) + \vec{y}_i + \vec{u}_\alpha)\right]_{p^k}.\end{aligned}$$

Thus $(\mathcal{C}_{p^k}^D, F)$ is conjugated to $((\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}, F^*)$ by Ψ and $(\mathcal{C}_{p^k}^D, F)$ is a factor of $((\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}, F^*)$.

Let us note that the action of F^* over any sequence $a = (\dots, a_{-1}, a_0, a_1, \dots) \in (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$ is such that each configuration $a_i \in \mathcal{C}_{p^k}^{D-1}$ evolves independently. Moreover, comparing with (3), f^* is the global transition mapping of a linear $(D-1)$-dimensional CA with local rule $f^{(D-1)} = f$ and neighborhood $\{\varphi(\vec{u}_1), \dots, \varphi(\vec{u}_s)\}$. □

Theorem 4.5. *Let F be a linear D-dimensional CA over $\mathcal{C}_{p^k}^D$, where p is a prime number. If F is strongly transitive then it has dense periodic points.*

Proof. Let $\hat{F}$ be the global transition map defined in Lemma 3.3 (we recall that $\hat{F}$ is based on the local rule $\hat{f}$ obtained from f by removing all the coefficients that are not prime with p). From Lemma 3.3 we have that if $\hat{F}$ has dense periodic points then F has dense periodic points. Furthermore from the strong transitivity of F it follows also that $\hat{F}$ is strongly transitive. Indeed, there exists a pair λ_i, λ_j, with $i, j \in \{1, \dots, s\}$, such that p divides neither of them. Since p is a prime number then $\gcd(p, \lambda_i) = 1$ and $\gcd(p, \lambda_j) = 1$, thus $i, j \in I$, where I has been introduced in Lemma 3.3. Therefore according to [15] $\hat{F}$ is also strongly transitive.

As a consequence of these facts, we may now assume that all the coefficients of F (at least two of them are non-zero, otherwise F becomes a shift-like CA which is not strongly transitive) are prime with p. We prove the thesis by induction on D. In [5] it has been proved that thesis is true in the one-dimensional case. Let us assume the thesis in dimension $D-1$, then we prove it in dimension D. We treat the following two cases:

- *Case* 1: *There exists a pair $\vec{u}, \vec{v}$ of independent neighbor vectors.*
  Thanks to Lemma 4.4 the linear D-dimensional CA F over $\mathcal{C}_{p^k}^D$ is a factor of a one-dimensional linear CA F^* over $(\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$ whose local rule is permutive in each variable. The hypothesis of Lemma 4.1 are satisfied and then F^* has dense periodic points with respect to the Tychonoff distance over $(\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$. Since $((\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}, F^*)$ is topologically semi-conjugated to $(\mathcal{C}_{p^k}^D, F)$ we can conclude that also F has dense periodic orbits with respect to the Tychonoff distance over $\mathcal{C}_{p^k}^D$.
- *Case* 2: *All the neighbor vectors are pairwise linearly dependent.*
  Thanks to Lemma 4.4 the linear D-dimensional CA F over $\mathcal{C}_{p^k}^D$ is a factor of a one-dimensional linear CA F^* over $(\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$ whose local rule f^* is the global transition mapping of a strongly transitive CA over $\mathcal{C}_{p^k}^{D-1}$ which has dense periodic points by induction.

Let us show now that F has dense periodic points. We make use of the formalisms introduced in the proof of Lemma 4.4. Let us choose an arbitrary configuration $c \in \mathcal{C}_{p^k}^D$ and a real number $\varepsilon > 0$. Let n be a positive integer such that $\sum_{i=n+1}^{+\infty} (2i+1)^D - (2i-1)^D/2^i < \varepsilon$. Let us consider the hyperplanes H_i, $\mu \leqslant i \leqslant \nu$ for some $\mu, \nu \in \mathbb{Z}$, which intersect the closed ball $K_n(\vec{0})$. Denoting by S_i the subset of H_i^* contained in $K_n(\vec{0})$, owing to the regularity of f^*, for each i there exists a periodic (with respect to

f^*) configuration $p_i \in \mathcal{C}_{p^k}^{D-1}$ of period q_i such that $p_i(\vec{t}) = \Phi_0(T_i(c_i))(\vec{t}), \forall \vec{t} \in \{\varphi(\vec{x} - \vec{y}_i), \vec{x} \in S_i\}$. Let us construct now the configuration $p \in (\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}$ obtained repeating periodically the block $p_\mu \cdots p_v$, i.e., $p = (\ldots, p_\mu, \ldots, p_v, p_\mu, \ldots, p_v, p_\mu, \ldots, p_v, \ldots)$. The configuration p is a periodic point (of period equal to $lcm(q_1, \ldots, q_k)$) of $((\mathcal{C}_{p^k}^{D-1})^{\mathbb{Z}}, F^*)$ and so $\Psi^{-1}(p)$ is a periodic point of $(\mathcal{C}_{p^k}^D, F)$. Moreover $\forall \vec{x} \in S_i$, $(\Psi^{-1}(p))_i(\vec{x}) = c_i(\vec{x})$. Indeed

$$(\Psi^{-1}(p))_i(\vec{x}) = T_i^{-1}\Phi_0^{-1}(p_i)(\vec{x}) = p_i(\varphi(\vec{x} - \vec{y}_i)) = \Phi_0 T_i(c_i)(\varphi(\vec{x} - \vec{y}_i)) = c_i(\vec{x})$$

and this fact implies that $\forall \vec{x} \in K_n(\vec{0}), \Psi^{-1}(p)(\vec{x}) = c(\vec{x})$. Thus we have obtained $d(c, \Psi^{-1}(p)) < \varepsilon$ and we conclude that F has dense periodic points. □

Example 1. A linear CA over C_2^2.

We describe a two-dimensional binary CA whose evolution is governed by a local rule f which computes the sum modulo 2 of its 4 input values selected by the neighbor vectors. In this example the neighbor vectors select the cells to the north, west, east, and south of the cell we are considering. Let $D = 2$ and $s = 4$. Let $\vec{u}_1 = (0, 1)$, $\vec{u}_2 = (-1, 0)$, $\vec{u}_3 = (1, 0)$, $\vec{u}_4 = (0, -1)$. The local rule f is defined by $f(\xi_1, \xi_2, \xi_3, \xi_4) = (\xi_1 + \xi_2 + \xi_3 + \xi_4) \bmod 2$. The global transition map F is defined by $[F(c)](x_1, x_2) = (c(x_1, x_2 + 1) + c(x_1 - 1, x_2) + c(x_1 + 1, x_2) + c(x_1, x_2 - 1)) \bmod 2$.

In order to construct the one dimensional CA conjugated to the D-dimensional CA we can choose as hyperplane H_0 the axis of equation $x_1 = 0$ expressed in parametric form by the vector $\vec{e}_2 = (0, 1)$ and as vector $\vec{y}_1$ the vector $(1, 0)$. Therefore the hyperplanes containing the neighbor vectors are H_{-1}, H_0 and H_1.

In this way the two-dimensional CA is topologically conjugated by Ψ to a one-dimensional CA defined over the alphabet $\mathcal{C}_2^1$. The neighborhood of the new CA is the set $\{-1, 0, 1\}$. Let $\vec{z}_{0,1}$ be the neighbor vector $\vec{u}_4 = (0, -1)$. The local rule f^* is then defined as follows: $\forall (a_1, a_2, a_3) \in (\mathcal{C}_2^1)^3$, $f^*(a_1, a_2, a_3) = \Omega_1(F_1(a_1)) \oplus \Omega_2(F_2(a_2)) \oplus \Omega_3(F_3(a_3))$ where in this case the mappings Ω_1, Ω_3, F_1, F_3 are the identity and the mappings Ω_2 and F_2 are defined respectively as follows: $\forall t \in \mathbb{Z}, \forall a \in \mathcal{C}_2^1$, $\Omega_2(a)(\vec{t}) = a(t-1)$ and $\forall t \in \mathbb{Z}, \forall a \in \mathcal{C}_2^1$, $F_2(a)(\vec{t}) = [a(t) + a(t+2)]_2$.

It remains to be prove that surjective but not strongly transitive linear CA have dense periodic points.

Theorem 4.6. *Surjective linear D-dimensional CA over $\mathcal{C}_m^D$ have dense periodic points.*

Proof. Let $m = p_1^{q_1} \ldots p_n^{q_n}$ be the prime factor decomposition of m. Let $m_i = p_i^{q_i}$, $1 \leqslant i \leqslant n$. From a repeated application of Lemma 3.2 we have that F has dense periodic points if and only if $[F]_{m_i}$ has dense periodic points for every $1 \leqslant i \leqslant n$. If $[F]_{m_i}$ is strongly transitive then in view of Theorem 4.5 it has dense periodic points. Assume now that $[F]_{m_i}$ is not strongly transitive. Since F is surjective, $[F]_{m_i}$ must be surjective and in view of Lemma 3.4 we conclude that there exists a positive integer h such that $[F]_{m_i}^h$ is a shift-like CA. Since shift-like CA have dense periodic points we obtain the thesis. □

5. Periodic points for non-surjective linear CA

In this section we study the distribution of periodic points of non-surjective linear CA with the aim of understanding which points of $\mathcal{C}_m^D$ can be approximated with arbitrary precision by periodic points. To this extent, we take advantage of the theory of attractors applied to linear CA developed in [16]. In [16], the authors prove that for any non-surjective linear CA F, there exists a subspace Y_F such that, for any configuration x, $F^k(x) \in Y_F$ for all $k \geqslant \lfloor \log_2 m \rfloor$. That is, after a transient phase of length at most $\lfloor \log_2 m \rfloor$, the evolution of the system takes place completely within the subspace Y_F. This result indicates that, in order to study periodic points of non-surjective linear CA, one should analyze the behavior of the map F over the subspace Y_F. In addition, they prove that the behavior of F over Y_F is *identical* to the behavior of a linear surjective map F^* defined over a configuration space isomorphic to Y_F.

Let F denote the global transition map of a non-surjective linear D-dimensional CA over $\mathbb{Z}_m$ defined by

$$(F(c))(\vec{v}) = \left[\sum_{i=1}^{s} \lambda_i c(\vec{v} + \vec{u}_i)\right]_m . \tag{5}$$

Let $d = \gcd(m, \lambda_1, \ldots, \lambda_s)$. Since F is not surjective we know that $d > 1$. Let $m = p_1^{q_1} p_2^{q_2} \cdots p_n^{q_n}$. Without loss of generality we can assume that $d = p_1^{v_1} p_2^{v_2} \cdots p_l^{v_l}$ with $1 \leqslant v_i \leqslant q_i$ and $l \leqslant n$. Let

$$q = p_1^{q_1} \cdots p_l^{q_l}, \tag{6}$$

and define

$$Y_F = \{c \in \mathcal{C}_m^D \mid [c(\vec{v})]_q = 0, \ \forall \vec{v} \in \mathbb{Z}^D\} \quad \text{and} \quad m^* = \frac{m}{q}. \tag{7}$$

We have the following theorem (which is the combination of Theorems 3.1 and 3.2 of [16]).

Theorem 5.1 (Manzini and Margara [16]). *Let $(\mathcal{C}_m^D, F)$ denote a non-surjective linear CA. Let Y_F and m^* be defined as in (7). Then*
(a) *for any $c \in \mathcal{C}_m^D$ and $k \geqslant \lfloor \log_2 m \rfloor$, we have $F^k(c) \in Y_F$ and*
(b) *the subsystem (Y_F, F) is topologically conjugated to the surjective linear CA $(\mathcal{C}_{m^*}^D, [F]_{m^*})$.*

Taking advantage of Theorem 5.1 we can prove the main result of this section.

Corollary 5.2. *Let $(\mathcal{C}_m^D, F)$ denote a non-surjective linear CA. Let Y_F be defined as in (7). Then*
(c) *the periodic points of F are dense over Y_F and*
(d) *Y_F is the largest subset of $\mathcal{C}_m^D$ where F has dense periodic points.*

Proof. From Theorem 5.1 we know that after at most $\lfloor \log_2 m \rfloor$ steps the evolution of $(\mathcal{C}_m^D, F)$ takes place completely within the subspace Y_F. This implies that all periodic points belong to Y_F. In addition, the subsystem (Y_F, F) is topologically conjugated to a surjective linear CA $(\mathcal{C}^D_{m^*}, [F]_{m^*})$ which, in view of Theorem 4.6, has dense periodic points over the entire $\mathcal{C}^D_{m^*}$. Since topological conjugation preserves denseness of periodic orbits, we conclude that F has dense periodic points over Y_F.

Let $x \in \mathcal{C}^D_m$ be any configuration which does not belong to Y_F. Then there exists a vector $\vec{v} \in \mathbb{Z}^D$ such that for every $y \in Y_F$ we have $x(\vec{v}) \neq y(\vec{v})$ and then $d(x, y) \geqslant 1/2^{\|v\|_\infty}$. We conclude that Y_F is the largest subset of $\mathcal{C}^D_m$ where F has dense periodic points. □

6. Topological mixing for linear CA

In this section we prove that topological mixing and transitivity are equivalent properties as far as linear CA are concerned.

Theorem 6.1. *Let F be a linear D-dimensional CA over $\mathcal{C}^D_m$. If F is strongly transitive then it is topologically mixing.*

Proof. Let $C \subseteq \mathcal{C}^D_m$ be any cylinder and t_C be the positive integer defined in Lemma 3.1. We have that $F^{t_C}(C) = \mathcal{C}^D_m$. Since F is surjective, we have

$$\forall n \geqslant t_C : \quad F^n(C) = \mathcal{C}^D_m,$$

that is, F is topologically mixing as claimed. □

Theorem 6.2. *Transitive linear D-dimensional CA over $\mathcal{C}^D_m$ are topologically mixing.*

Proof. Let $m = p_1^{q_1} \cdots p_n^{q_n}$ be the prime factor decomposition of m. Let $m_i = p_i^{q_i}$, $1 \leqslant i \leqslant n$. From (a repeated application of) Lemma 3.2 we have that F is topologically mixing if and only if $[F]_{m_i}$ is topologically mixing for every $1 \leqslant i \leqslant n$. Assume now that $[F]_{m_i}$ is not topologically mixing. Since F is transitive, $[F]_{m_i}$ must be transitive (and then surjective). By a combination of Theorem 6.1 and Lemma 3.4 there exists a positive integer h such that $[F]^h_{m_i}$ is a shift-like CA with radius r. Since $[F]_{m_i}$ is transitive r must be greater than zero. The thesis follows from the fact that shift-like CA with radius greater than zero are topologically mixing. □

Since topologically mixing CA are transitive by definition, we conclude that for linear CA transitivity and topological mixing are equivalent properties.

7. Chaotic behavior of linear cellular automata

In this section we classify linear D-dimensional CA over $\mathbb{Z}_m$ $(D \geqslant 1,\ m \geqslant 2)$ according to the Devaney's definition of chaos.

Definition 7.1 (Devaney's Chaos). A dynamical system is chaotic according to Devaney's definition of chaos if and only if it is topologically transitive, it is sensitive to the initial conditions, and it has dense periodic points.

Let us recall that, in [1], it was proved that transitivity and denseness of periodic points together imply sensitivity to the initial condition.

Let $(\mathcal{C}_m^D, F)$ be a D-dimensional linear CA over $\mathbb{Z}_m$ defined by

$$(F(c))(\vec{v}) = \left[\sum_{i=1}^{s} \lambda_i c(\vec{v} + \vec{u}_i)\right]_m, \tag{8}$$

where $c \in \mathcal{C}_m^D, \vec{v} \in \mathbb{Z}_d$, where, as usual, we assume $\|\vec{u}_1\|_\infty = 0$ and $\|\vec{u}_i\|_\infty > 0$ for every $2 \leqslant i \leqslant s$. Let $\mathcal{P}$ be the set of prime factors of m. We have the following results:

(a) $(\mathcal{C}_m^D, F)$ is topologically transitive if and only if $\gcd(\lambda_2, \ldots, \lambda s, m) = 1$ (see [4]).

(b) $(\mathcal{C}_m^D, F)$ is sensitive to initial conditions if and only if there exists $p \in \mathcal{P}$ which does not divide $\gcd(\lambda_2, \ldots, \lambda_s)$ (see [15]).

(c) $(\mathcal{C}_m^D, F)$ is surjective if and only if $\gcd(\lambda_1, \ldots, \lambda s, m) = 1$ (see [13]).

(d) $(\mathcal{C}_m^D, F)$ has dense periodic points if and only if it is surjective (this paper).

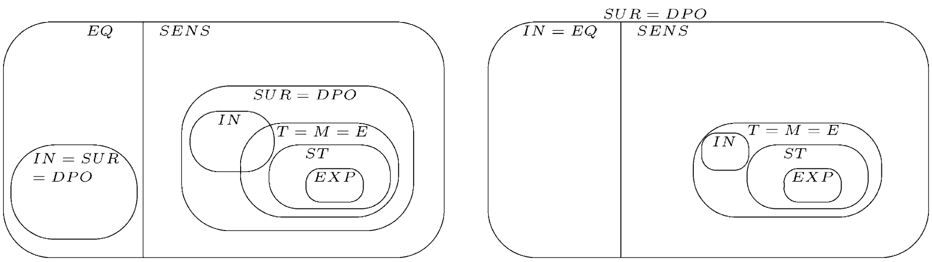
As a consequence of $(a) - (d)$ we have the following corollary.

Corollary 7.2. *Let $(\mathcal{C}_m^D, F)$ be any D-dimensional linear CA over $\mathbb{Z}_m$. Let $\lambda_1, \ldots, \lambda_s$ be the coefficients of its local rule. The following statements are equivalent.*

- $(\mathcal{C}_m^D, F)$ *is chaotic according to the Devaney's definition of chaos*,
- $(\mathcal{C}_m^D, F)$ *is topologically transitive*,
- $\gcd(\lambda_2, \ldots, \lambda s, m) = 1$.

8. Concluding remarks and open problems

This paper extends the topological classification of linear CA over $\mathbb{Z}_m$ given in [4,5,15] by exactly characterizing topological mixing and denseness of periodic orbits. In the following diagram we show inclusions among properties of D-dimensional linear CA over $\mathbb{Z}_m$ for m composite (left) and m prime (right). All inclusions are proper. Note that the class of expansive CA is empty in any dimension greater than 1.



In the picture IN = Injectivity, T = Transitivity, ST = Strong Transitivity, EXP = Expansivity, E = Ergodicity, M = Topological Mixing, $SENS$ = Sensitivity to Initial

Conditions, SUR = Surjectivity, DPO = Denseness of Periodic Orbits, EQ = Equicontinuity.

Some of the inclusions pictured in the above diagram hold also for general (i.e., non-linear) CA. For example, expansivity implies strong transitivity and transitivity implies sensitivity. On the other hand, some of the properties which hold for linear CA do not hold for general CA. For example there exist CA which are not equicontinuous nor sensitive to initial conditions.

The following questions have a positive answer in the case of linear CA but, to our knowledge, are still unanswered in the case of general CA.

(1) Transitivity implies ergodicity (with respect to the Haar measure)?
(2) Strong transitivity implies topological mixing?
(3) Surjectivity implies denseness of periodic points?

References

[1] J. Banks, et al., On Devaney's definition of chaos, Amer. Math. Monthly 99 (1992) 332–334.

[2] G. Cattaneo, A. Dennunzio, L. Margara, Chaotic subshifts and related languages, application to one dimensional cellular automata, Fund. Inform. 52 (2002) 39–80.

[4] G. Cattaneo, E. Formenti, G. Manzini, L. Margara, On ergodic linear cellular automata over Z_m, in: 14th Annual Symp. on Theoretical Aspects of Computer Science (STACS '97), LNCS n. 1200, Springer, Berlin, 1997, pp. 427–438.

[5] G. Cattaneo, E. Formenti, G. Manzini, L. Margara, Ergodicity, transitivity, and regularity for linear cellular automata over Z_m, Theoret. Comput. Sci. 233 (1–2) (2000) 147–164.

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

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

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

[9] M. D'amico, G. Manzini, L. Margara, On computing the entropy of cellular automata, in: 25th Internat. Colloq. on Automata Languages and Programming (ICALP '98), Springer, Berlin, 1998.

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

[11] P. Favati, G. Lotti, L. Margara, One dimensional additive cellular automata are chaotic according to Devaney's definition of chaos, Theoret. Comput. Sci. 174 (1997) 157–170.

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

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

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

[15] G. Manzini, L. Margara, A complete and efficiently computable topological classification of D-dimensional linear cellular automata over Z_m, A Preliminary Version of this Paper has been Presented to the 24th International Colloquium on Automata Languages and Programming (ICALP '97), LNCS n. 1256, Springer, Berlin, 1997. Theoret. Comput. Sci. 221(1–2) (1999) 157–177.

[16] G. Manzini, L. Margara, Attractors of D-dimensional linear cellular automata, A Preliminary Version of this Paper has been Presented to the 15th Annual Symposium on Theoretical Aspects of Computer Science (STACS '98), LNCS n. 1373, Springer, Berlin, 1998, pp. 128–138. J. Comput. Syst. Sci. 58(3) (1999) 597–610.

[17] G. Manzini, L. Margara, Invertible linear cellular automata over Z_m: algorithmic and dynamical aspects, J. Comput. Syst. Sci. 1 (1998) 60–67.

[18] L. Margara, On some topological properties of linear cellular automata, in: 24th Internat. Symp. on Mathematical Foundations of Computer Science (MFCS '99), LNCS n. 1672, Springer, Berlin, 1999, pp. 209–219.

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