Article

On One-Sided, D-Chaotic CA Without Fixed Points, Having Continuum of Periodic Points With Period 2 and Topological Entropy log(p) for Any Prime p

Wit Foryś [1],* and Janusz Matyja [2]

[1] Institute of Computer Science, Jagiellonian University, Łojasiewicza 6, 30-348 Kraków, Poland

[2] Department of Computer Science and Econometrics, Silesian Technical University, Roosevelta 26-28, 41-800 Zabrze, Poland; E-Mail: janusz.matyja@polsl.pl

* Author to whom correspondence should be addressed; E-Mail: forysw@ii.uj.edu.pl; Tel.: +48-12-664-66-33; Fax: +48-12-664-66-73.

External Editor: J. A. Tenreiro Machado

Abstract: A method is known by which any integer $n \geq 2$ in a metric Cantor space of right-infinite words $\tilde{A}_n^{\mathbb{N}}$ gives a construction of a non-injective cellular automaton $(\tilde{A}_n^{\mathbb{N}}, \tilde{F}_n)$, which is chaotic in Devaney sense, has a radius $r = 1$, continuum of fixed points and topological entropy $log(n)$. As a generalization of this method we present for any integer $n \geq 2$, a construction of a cellular automaton $(A_n^{\mathbb{N}}, F_n)$, which has the listed properties of $(\tilde{A}_n^{\mathbb{N}}, \tilde{F}_n)$, but has no fixed points and has continuum of periodic points with the period 2. The construction is based on properties of cellular automaton introduced here $(B^{\mathbb{N}}, F)$ with radius 1 defined for any prime number p. We prove that $(B^{\mathbb{N}}, F)$ is non-injective, chaotic in Devaney sense, has no fixed points, has continuum of periodic points with the period 2 and topological entropy $log(p)$.

Keywords: one-sided cellular automata; D-chaotic; E-chaotic; fixed points; topological entropy

MSC classifications: 37A35, 37B15, 37B40

1. Introduction

The dynamics of cellular automata have been investigated widely in mathematics, physics and theoretical computer science. Presently, there are many constructions of cellular automata in metric Cantor space of right infinite words $A^{\mathbb{N}}$, which are:

(1) positively expansive and topologically conjugated to a one-sided full shift or a one-sided subshift of finite type (SFT) [1,2]

(2) bijective, expansive and topologically conjugated to a two-sided full shift or a two-sided SFT [3–5]

(3) strongly transitive with non-zero memory [6].

The dynamics of transitive cellular automata in metric Cantor spaces $A^{\mathbb{N}}$ and $A^{\mathbb{Z}}$ has been intensively investigated [6–9]. It has been established that any positively expansive cellular automaton in $A^{\mathbb{N}}$ is topologically conjugated with a one-sided, topologically mixing SFT [1,2], is non-injective [1,10,11], E-chaotic [12] and has topological entropy $log(n), n \geq 2, n \in \mathbb{N}$ [1]. In particular, a one-sided full shift defined over $n-$elementary alphabet A is a positively expansive cellular automaton and has topological entropy $log(n)$.

In our papers [13–15], for any integer $n \geq 2$ we have presented a construction of non-injective, D-chaotic [16] cellular automaton $(\tilde{A}_n^{\mathbb{N}}, \tilde{F}_n)$, which has radius $r = 1$, continuum of fixed points and topological entropy equal to $log(n)$. This means that it can achieve the topological entropy of any fixed positively expansive cellular automaton in $A^{\mathbb{N}}$. Cardinality of the set of periodic points with the fixed period $m \geq 1$ is an invariant of topological conjugacy [17] which asserts that for any integer $n \geq 2$ an automaton $(\tilde{A}_n^{\mathbb{N}}, \tilde{F}_n)$, is not topologically conjugated to any positively expansive cellular automaton defined in $A^{\mathbb{N}}$ [1,2]. Additionally, a positively expansive cellular automaton defined in $A^{\mathbb{N}}$ need not be topologically conjugated to a one-sided full shift [2,18]. Hence in this context it is natural to ask whether there exists in $A^{\mathbb{N}}$ a non-injective, D-chaotic cellular automaton with continuum of periodic points with a fixed period $m \geq 1$ and topological entropy $log(n)$ for an integer $n \geq 2$ which is not topologically conjugated to $(\tilde{A}_n^{\mathbb{N}}, \tilde{F}_n)$.

In the paper we present a cellular automaton $(B^{\mathbb{N}}, F)$ with radius 1 defined for any prime number p. We prove that this automaton is not injective, is D-chaotic, has no fixed points, but has continuum of periodic points with the period 2 and topological entropy $log(p)$. Thus we obtain a positive answer for the above question and additionally for any integer $n \geq 2$, we are able to construct a cellular automaton $(A_n^{\mathbb{N}}, F_n)$, which has the listed properties of $(B^{\mathbb{N}}, F)$, but its topological entropy is equal to $log(n)$. In fact, if $n = p$, then $F_n = F$ and $A_n = B$. For a non-prime integer $n \geq 2$ and p any fixed prime from the factorization of n (for example the least one) we have $n = p \cdot k$. For this k a one-sided full shift σ, defined over $k-$elementary alphabet, is a topologically mixing cellular automaton with radius $r = 1$, which has topological entropy $log(k)$ and k fixed points. Now basing on the properties of F for a prime p, we conclude from Theorem 2 in [19] and Theorem 7.10 in [20] that the cartesian product $F \times \sigma$ is topologically conjugated to a cellular automaton $(A_n^{\mathbb{N}}, F_n)$, which has the expected properties.

The obtained results coincide with research directions pointed out by papers [1,2,6,7,11,13–15,18].

2. Preliminaries

This section contains all notions and notations to be used in the paper. We denote by $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ the sets of non-negative integers, integers and real numbers, respectively. $\#Y$ stands for the cardinality of a set Y. A finite (non-empty) word w over an alphabet B, that is a finite and non-empty set, is a function $w : [0, k] \longrightarrow B$ defined on a discrete interval $[0, k]$, where $k \geqslant 0$. The set of all such defined words with concatenation of words is a free semigroup $(B^+, \cdot)$. The length of a word w, denoted by $|w|$ is equal to the cardinality of its domain. The set of all words in B^+ with the length equal to n is denoted B^n. $(B^*, \cdot)$ stands for a free monoid of words after the empty word λ, the unit element of concatenation, is added. By the definition $|\lambda| = 0$ and $B^0 = \{\lambda\}$. A right infinite word is a function on $\mathbb{N}$ or equivalently on a discrete interval $[0, \infty)$ with values in B. The set of all right infinite words is denoted by $B^{\mathbb{N}}$. It is convenient to extend naturally concatenation to pairs of words in $B^* \times B^{\mathbb{N}}$ with values in $B^{\mathbb{N}}$. We will use also in the sequel words defined on finite discrete intervals of the form $I = [i, j]$, where $i \leq j$, are non-negative integers. If $i = j$, then we denote such degenerated interval by $[i, i]$, $[i]$ or $\{i\}$. For two discrete intervals I, J such that $J \subset I$ and for a word u defined on I we denote by u_J the restriction of u to J.

In the sequel we assume that $\#B \geq 2$.

We define metric $d : B^{\mathbb{N}} \times B^{\mathbb{N}} \to \mathbb{R}$ putting for any $x, y \in B^{\mathbb{N}}$

$$d(x, y) = \begin{cases} 2^{-i} & \text{if } x \neq y \\ 0 & \text{otherwise} \end{cases}$$

where $i = min\{j \geq 0 : x(j) \neq y(j)\}$.

The obtained topological space $B^{\mathbb{N}}$ is a Cantor space [6,10,21] and the family of balls $\beta = \{K(x, 2^{-n}) : x \in B^{\mathbb{N}}, n \in \mathbb{N}\}$ is its base. For $n \in \mathbb{N}$, every open ball in $B^{\mathbb{N}}$ with the radius 2^{-n}, is of the form $K(x, 2^{-n}) = wBBB...B... = w \cdot B^{\omega} = wB^{\omega}$, where $w = x_{[0,n]} \in B^{n+1}$. We denote by X^{ω} an infinite concatenation of a set of words X.

Let us fix $r \in \mathbb{N}$ and assume that there is given a mapping $F' : B^{r+1} \to B$. For any $x \in B^{\mathbb{N}}$, $i \in \mathbb{N}$ there exists $w \in B^{r+1}$ such that $w(j) = x(i + j)$ for any $j \in [0, r]$. We put in this case $F'(x_{[i, i+r]}) = F'(w)$. A mapping $F : B^{\mathbb{N}} \to B^{\mathbb{N}}$ such that $F(x)(i) = F'(x_{[i, i+r]})$ for any $x \in B^{\mathbb{N}}$ and $i \in \mathbb{N}$ is referred to as one-sided cellular automaton [1,22]. $F' : B^{r+1} \to B$ is called the local rule of F. Any cellular automaton F is continuous. If for $u \in B^+$, it holds $|u| > r$, then we define $F'(u)$ putting $F'(u)(i) = F'(u_{[i, i+r]})$ for any $i \in [0, |u| - r)$. If $r \in \mathbb{N} \setminus \{0\}$ and for any $w \in B^r$, $b \in B$ there exists exactly one $a \in B$ such that $F'(aw) = b$ ($F'(wa) = b$), then F is referred to as left (right) permutative [1,21]. If $F : B^{\mathbb{N}} \to B^{\mathbb{N}}$ is left (right) permutative then it is surjective [23]. A cellular automaton F is right-closing, if for any $x, y \in B^{\mathbb{N}}$ equalities: $F(x) = F(y)$, $x_{[0, i]} = y_{[0, i]}$ for some $i \geq r$, imply $x = y$ (compare [24]).

Assume, in what follows that S is a closed subset of $B^{\mathbb{N}}$. Let $\psi : S \to S$ be a continuous mapping. A pair (S, ψ) is referred to as a symbolic dynamical system, SDS in the abbreviated form [21]. A point $y \in S$ is periodic for ψ if and only if there exists $n \in \mathbb{N} \setminus \{0\}$ such that $\psi^n(y) = y$. The set of all periodic points of ψ is denoted $Per(\psi)$. If $\psi(y) = y$, then y is a fixed point of ψ. If there exists $\varepsilon > 0$ such that for any $x, y \in S$, $y \neq x$ there exists $n \in \mathbb{N}$ such that $d(\psi^n(x), \psi^n(y)) \geq \varepsilon$, then ψ is positively expansive. A mapping ψ is transitive, if it is surjective and for any not empty open sets

$U, V \subset S$ there exists an integer $n \in \mathbb{N} \setminus \{0\}$ such that $U \cap \psi^{-n}(V) \neq \emptyset$ [1,20]. If additionally S is infinite and $\psi : S \to S$ is surjective then SDS (S, ψ) is referred to as D-chaotic (or chaotic in the Devaney's sense) [16,21,25] if and only if

(1) the set $Per(\psi)$ is dense in S, that is for any $y \in S$, and $n \in \mathbb{N}$, $Per(\psi) \cap K(y, 2^{-n}) \neq \emptyset$ ($K(y, 2^{-n}) \subset S$),

(2) for any $n \in \mathbb{N}$, $K(y, 2^{-n}) \subset S$, and for any $K(x, 2^{-n}) \subset S$, there exists $m \in \mathbb{N} \setminus \{0\}$ such that $K(y, 2^{-n}) \cap \psi^{-m}(K(x, 2^{-n})) \neq \emptyset$, that is $\psi : S \to S$ is transitive.

If (S, ψ) is D-chaotic and additionally $\psi : S \to S$ is positively expansive, then (S, ψ) is referred to as E-chaotic [12]. In particular a cellular automaton $(B^{\mathbb{N}}, F)$ is SDS. A mapping $\pi : (B^{\mathbb{N}}, F) \to (S, \psi)$ is a surjective SDS morphism if it is surjective, continuous and $\pi \circ F = \psi \circ \pi$. In this case (S, ψ) is a factor of $(B^{\mathbb{N}}, F)$. If additionally π is a bijection, then it is a topological conjugacy. In this case SDS (S, ψ), $(B^{\mathbb{N}}, F)$ are topologically conjugated.

Assume that $\sigma(x)(i) = \sigma'(x_{[i, i+1]}) = x(i+1)$ for any $x \in B^{\mathbb{N}}$ and $i \in \mathbb{N}$. In such a case a cellular automaton $(B^{\mathbb{N}} \sigma)$ is called a one-sided full shift. If S is a closed subset of $B^{\mathbb{N}}$ and $\sigma(S) \subset S$, then a SDS (S, σ) is called a one-sided subshift [10,21].

Two objects are associated with a cellular automaton $F : B^{\mathbb{N}} \to B^{\mathbb{N}}$ defined by a local rule $F' : B^2 \to B$. The first, a one-sided subshift (S_F, σ) where $S_F = \{y \in B^{\mathbb{N}} : \exists x \in B^{\mathbb{N}}, F^k(x)(0) = y(k), k \in \mathbb{N}\}$ [6,26]. The second, a surjective SDS morphism $\chi : (B^{\mathbb{N}}, F) \ni x \to y = x(0)F(x)(0)F^2(x)(0)...F^k(x)(0)....\in (S_F, \sigma)$ [1]. In such a case topological entropy $h(B^{\mathbb{N}}, F)$ of SDS $(B^{\mathbb{N}}, F)$ is given by the equality $h(B^{\mathbb{N}}, F) = lim_{n\to\infty} \frac{1}{n+1} \log(\#\{y_{[0, n]} : y \in S_F\})$ [1,22,27].

3. Cellular Automaton F

This section starts from the introduction of a one-sided cellular automaton F, whose form depends on the chosen prime number p. The main objective of the section is to describe its basic properties.

In the sequel p is a fixed prime number. We use the following notation:

$$
\begin{aligned}
B &= \{0, 1, 2, ..., 2p-1\}, \\
A &= \{0, 2, 4, ..., 2(p-1)\} \subset B, \\
E &= \{0, 1\} \subset B.
\end{aligned}
$$

We introduce a mapping $\varphi' : B \to A$, defining $\varphi'(a) = 2\lfloor a/2 \rfloor$, where $\lfloor \ \rfloor$ denotes the floor function. Notice that $\varphi'(a)$ is the closest integer in A not greater than $a \in B$.

Define a function $f' : B^2 \to E$ such that $f'(a, b) = f'(a, \varphi'(b))$, $f'(a, b) \neq f'(\varphi'(a)+(a+1)mod\,2, b)$ for any $a, b \in B$. We define a cellular automaton $G : A^{\mathbb{N}} \to A^{\mathbb{N}}$ with a local rule $G' : A^2 \to A$ given by $G'(a, b) = 2((a/2 + b/2)\,mod\,p)$ for any $a, b \in A$.

The main object of our considerations in [13–15] are properties of some cellular automata $(B^{\mathbb{N}}, F)$ having a local rule $F' : B^2 \to B$ of the form $F'(a, b) = f'(a, b) + G'(\varphi'(a), \varphi'(b))$.

Notice that this form of $F' : B^2 \to B$ does not guarantee transitivity of $(B^{\mathbb{N}}, F)$ (see Example 1 in [15]). Observe that a cellular automaton $(A^{\mathbb{N}}, G)$ is right-permutative [21] and thus surjective and

positively expansive [1]. Additionally it is a factor of a linear and transitive cellular automaton defined on $\mathbb{Z}_p^{\mathbb{Z}}$ [26,28].

As a continuation of our research we consider, in what follows, a cellular automaton $(B^{\mathbb{N}}, F)$ of the same type. Its local rule $F' : B^2 \to B$ is defined by a mapping $f' : B^2 \to E$ of the form: $f'(a, b) = (a + 1 + [\varphi'(a)/2 + q][\varphi'(b)/2 + 1 - q]) \, mod \, 2$ for $q = \lfloor (p+1)/2 \rfloor \, mod \, 2$ and $p \neq 3$, $f'(a, b) = (a + \rho(a)) \, mod \, 2$ for $\rho(a) = \frac{1}{2}(2 - \varphi'(a)/2)(1 - \varphi'(a)/2)$ and $p = 3$.

We extend $\varphi' : B \to A$ to a morphism $\varphi' : B^* \to A^*$. Additionally we introduce $\varphi : B^{\mathbb{N}} \to A^{\mathbb{N}}$ putting $\varphi(x) = y$ if and only if for any $x \in B^{\mathbb{N}}$ $y(i) = \varphi(x)(i) = \varphi'(x(i)) \in A$ for every $i \in \mathbb{N}$.

In a later part of this section we present basic properties of cellular automata $(B^{\mathbb{N}}, F)$, $(A^{\mathbb{N}}, G)$ and relationships between them. It follows just from the definition that the dynamics of $(B^{\mathbb{N}}, F)$ is closely related to the dynamics of $(A^{\mathbb{N}}, G)$. As a consequence of this dependance there are some generalized properties from [15] proved in the following lemma.

Lemma 1. *For the defined above mappings* F, G, φ', φ *it holds:*

(1) $\varphi' : B^* \to A^*$ *is surjective and* $|\varphi'(u)| = |u|$ *for any* $u \in B^*$.

(2) $\varphi : (B^{\mathbb{N}}, F) \to (A^{\mathbb{N}}, G)$ *is a surjective SDS morphism.*

(3) for any $a \in B$ *we have*

  (a) for any $b \in A$, *there exists a unique* $c \in B$ *such that for every* $b' \in \varphi'^{-1}(b)$, *it holds* $F'(a, b') = c$,
  (b) $\varphi'(\{F'(ab) : b \in A\}) = A$.

(4) if $n \geq 3, n \in \mathbb{N}, y \in B^{n+1}$ *and for any* $k \in [0, n)$ *there exists* $c \in A$ *such that* $F'(y(k)c) = y(k+1) \in B$ *then there exist* 2^n *words* $w \in B^n$ *and exactly one word* $\varphi'(w) \in A^n$ *such that* $y = y(0) \cdot F'(y(0)\varphi'(w))(0) \cdot F'^2(y(0)\varphi'(w))(0) \cdot ... \cdot F'^n(y(0)\varphi'(w))(0) = y(0) \cdot F'(y(0)w)(0) \cdot F'^2(y(0)w)(0) \cdot ... \cdot F'^n(y(0)w)(0)$.

Proof. Assertions of Points 1 and 2 are obvious.

From these assertions and the fact that $F'(a\varphi'(b)) = F'(ab)$ for any $a, b \in B$ follows directly Point 3.

We prove the statement 4. We start for $n = 3$. According to Point 3 there are two possibilities of $y_1(l) \in B$, one of $\varphi'(y_1(l)) \in A$ for $l = 0$, and then again one of $y_1(l) \in B$ for any $l \in (0, 2]$ such that

$$F'(y(l)y_1(l)) = y(l+1) \in B,$$
$$F'(y_1(l)c) = y_1(l+1) \in B, \quad \text{for} \quad l < 2, \text{ some } c \in A.$$

As the result we obtain a word $y_1 \in B^3$. Analogically we obtain a subsequent word $y_2 \in B^2$.

According to Point 3. there are two possibilities of $y_2(l) \in B$ and one of $\varphi'(y_2(l)) \in A$ for $l = 0$, and then again one for $y_2(l) \in B$ for any $l \in (0, 1]$ such that

$$F'(y_1(l)y_2(l)) = y_1(l+1) \in B,$$
$$F'(y_2(l)c) = y_2(l+1) \in B, \quad \text{for} \quad l < 1, \text{ some } c \in A.$$

Analogically we construct the last, in this case, word

$y_3 \in B$. According to Point 3, there are two possibilities of $y_3(0) \in B$ and one of $\varphi'(y_3(0)) \in A$ such that $F'(y_2(0)y_3(0)) = y_2(1) \in B$.

Finally we obtain exactly one word $\varphi'(w) \in A^3$ and 2^3 words $w = y_1(0)y_2(0)y_3(0) \in B^3$.

Now we assume that the assertion of the Point 4 is true for $n \geq 3$. Assume that $z \in B^{n+2}$ and for any $k \in [0, n]$ there exists $c \in A$ such that $F'(z(k)c) = z(k + 1) \in B$. Let us assume that $y = z_{[0, n]} \in B^{n+1}$. It follows from the assumption that the assertion of Point 4 is true for y.

Now, Point 3 implies that there is one possibility of $a_0 \in B$ such that

$$F'(y(n), a_0) = z(n + 1),$$
$$F'(F'^{n-1}(\varphi'(w))(0), c) = a_0, \quad \text{for some } c \in A$$

and then for any $k \in [1, \, n - 1]$ there is one possibility of $a_k \in B$ such that

$$F'(F'^{n-k}(\varphi'(w))(k - 1), a_k) = a_{k-1},$$
$$F'(F'^{n-k-1}(\varphi'(w))(k), c) = a_k, \quad \text{for some } c \in A.$$

Finally Point 3 implies that there are two possibilities of $a_n \in B$ and one possibility of $\varphi'(a_n) \in A$ such that

$$F'(F'^0(\varphi'(w))(n - 1), \, a_n) = a_{n-1} \, (F'^0(\varphi'(w)) = \varphi'(w))$$

Now, from the assumption there exist 2^{n+1} words $wa_n \in B^{n+1}$ and exactly one word $\varphi'(wa_n) \in A^{n+1}$ such that

$$
\begin{aligned}
z &= y(0) \cdot F'(y(0)\varphi'(wa_n))(0) \cdot F'^2(y(0)\varphi'(wa_n))(0) \cdots F'^n(y(0)\varphi'(wa_n))(0) \cdot F'^{n+1}(y(0)\varphi'(wa_n))(0) \\
&= y(0) \cdot F'(y(0)wa_n)(0) \cdot F'^2(y(0)wa_n)(0) \cdots F'^n(y(0)wa_n)(0) \cdot F'^{n+1}(y(0)wa_n)(0).
\end{aligned}
$$

$\square$

The following lemma simplifies the description of infinite words—elements of a one-sided subshift (S_F, σ).

Lemma 2. $S_F = \{y \in B^{\mathbb{N}} : \forall\, i \in \mathbb{N}, \ \exists c \in A, \ F'(y(i)c) = y(i + 1) \in B\}$.

Proof. Inclusion "$\subset$" is obvious. The inclusion in the opposite direction follows according to Point 4 of Lemma 1. $\square$

The obtained result simplifies the computation of a topological entropy $h(B^{\mathbb{N}}, F) = h(S_F, \sigma)$ [1,22] of a cellular automaton $(B^{\mathbb{N}}, F)$.

The following lemma presents basic properties of F. Notice that all properties listed in the below lemma except for left-permutativity, are invariants of a topological conjugacy.

Lemma 3. *Cellular automaton* F

(1) has topological entropy $h(B^{\mathbb{N}}, \, F) = \log(p)$,

(2) is left-permutative, surjective and not injective,

(3) has continuum of periodic points with the period 2,

(4) has no fixed points.

Proof. Lemma 2 assures that $y \in S_F$ if and only if for any $i \in \mathbb{N}$ there exists $c \in A$ such that $F'(y(i)c) = y(i+1)$. Now from Lemma 1 we have for any $a \in B$, $\#\{F'(ac) : c \in A\} = p$. Hence starting from these $\#B$ words of the length 1, in the subsequent steps from 1 to n it is possible to construct exactly $\#B \cdot p^n$ words $z \in B^{n+1}$ fulfilling the following condition: for any $i \in [0, n-1]$ there exists $c \in A$ such that $F'(z(i)c) = z(i+1)$. According to the above remarks and the definition of topological entropy of SDS $(B^{\mathbb{N}}, F)$ the equality of point 1. holds.

For the proof of Point 2, notice that just from the definition of $F' : B^2 \to B$, for any fixed $b, c \in B$, there exists exactly one $a = \varphi'(a) + a \bmod 2 \in B$ such that $F'(ab) = c$. Hence $(B^{\mathbb{N}}, F)$ is left-permutative [21] and surjective [23].

To prove that F is not injective observe that for $p = 2$, we have $F(1111 \cdots) = F(3333 \cdots) = 000 \cdots$, for $p = 3$, we have $F(242424 \cdots) = F(424242 \cdots) = 00000 \cdots$.

Now consider $p \geq 5$ and assume that $a = p - 1$ and $b = p + 2$. Thus

$$
\begin{aligned}
& F'(ab) \\
= \; & (p + [\lfloor (p-1)/2 \rfloor + q][\lfloor (p+2)/2 \rfloor + 1 - q]) \bmod 2 + 2((\lfloor (p-1)/2 \rfloor + \lfloor (p+2)/2 \rfloor) \bmod p) \\
= \; & (p + [(p-1)/2 + q][(p+1)/2 + 1 - q]) \bmod 2 + 2(((p-1)/2 + (p+1)/2) \bmod p) \\
= \; & (p + [(p-1)/2 + q][(p+1)/2 + 1 - q]) \bmod 2.
\end{aligned}
$$

Notice that $p \bmod 2 = 1$ and $[(p+1)/2 + 1 - q] \bmod 2 = 1$. If $q = 0$, then $((p-1)/2) \bmod 2 = 1$ and consequently $F'(ab) = 0$. If $q = 1$, then $((p-1)/2) \bmod 2 = 0$ and consequently $F'(ab) = 0$.

Similarly for $a = p + 2$, $b = p - 1$, we obtain $F'(ab) = 0$ for $q = 0$ or $q = 1$.

Finally, if $x, x' \in B^{\mathbb{N}}$, $x'(2i+1) = x(2i) = p - 1$, $x'(2i) = x(2i+1) = p + 2$ for any $i \in \mathbb{N}$, then $F(x) = F(x') = 00000... \in B^{\mathbb{N}}$.

Thus in these three cases F is not injective for any prime number p.

For Point 3 observe that $F'(ac) = 1 - a$ for any $a, c \in E$. Hence, if $x \in E^{\mathbb{N}}$, then $F^2(x) = x$. Observe that the cardinality of the set $E^{\mathbb{N}}$ is equal to continuum.

Finally for the assertion number 4. let us assume that there exist $a, b, c \in B$, $x = abc... \in B^{\mathbb{N}}$ such that $F(x) = x$. Hence $F'(ab) = a$. From Points 1 and 2 in Lemma 1, we have $G'(\varphi'(ab)) = \varphi'(a)$ and $(\varphi'(a) + \varphi'(b)) \bmod 2p = \varphi'(a)$. Thus $\varphi'(b) = 0$ and $b \in E$. Analogically $F'(bc) = b$ and $G'(\varphi'(bc)) = \varphi'(b)$, $(\varphi'(b) + \varphi'(c)) \bmod 2p = \varphi'(b)$.

Hence $\varphi'(c) = 0$ and consequently $b, c \in E$.

Just from the definition of a local rule we have $F'(bc) = 1 - b$ for any $b, c \in E$ which creates the contradiction. $\square$

If $a \in B$, $w \in B^+$, then $F'(aw) = F'(a\varphi'(w))$. Additionally, if $a, a' \in B$, $a \neq a'$, $w \in B^+$, $\varphi'(a) = \varphi'(a')$ ($\varphi'(a) \neq \varphi'(a')$), $c = F'(aw)(0)$, $c' = F'(a'w)(0)$, then $c \neq c'$, $\varphi'(c) = \varphi'(c')$ ($\varphi'(c) \neq \varphi'(c')$).

These properties are generalized in the lemma below, which can be proved exactly in the same way as its counterparts in [14,15].

Lemma 4. *(1) if $a \in B, w \in B^+, |w| = n \in \mathbb{N} \setminus \{0\}, a_0 = a, a_i = F'(a_{i-1}G''^{i-1}(\varphi'(w)))(0)$ for*
$i \in [1, n]$, then $a_k = F'^k(aw)(0)$ for any $k \in [0, n]$,

(2) if $w \in B^+$, $|w| = n \in \mathbb{N} \setminus \{0\}$, $a, a' \in B$ and for any $k \in [0, n]$:

   (a) $a' \neq a$, $\varphi'(a) = \varphi'(a')$, $F'^k(aw)(0) = c \in B$, $F'^k(a'w)(0) = c' \in B$, then $c' \neq c$,
   $\varphi'(c) = \varphi'(c')$,

   (b) $\varphi'(a) \neq \varphi'(a')$, $F'^k(aw)(0) = c \in B$, $F'^k(a'w)(0) = c' \in B$, then $\varphi'(c) \neq \varphi'(c')$.

Similarly as in [14] the above result could be used in the proofs of Lemmas 7, 8, 10, 11 and 13.

It is not difficult to show that for any $a, b \in A$, $n \in \mathbb{N}$, $w \in A^*$, $|w| = p^n - 1$ the formula $G''^{p^n}(awb)$ takes values $G'(ab)$. This implies hat the value $G''^{p^n}(awb)$ does not depend on a chosen word $w \in A^{p^n-1}$.

Exactly such a case is presented in the following lemma and its easy, inductive proof is left to the reader.

Lemma 5. *If $a, b, c \in A$, $G'(ab) = c$, then $G''^{p^n}(awb) = c$ for any $n \in \mathbb{N}$, $w \in A^*$, $|w| = p^n - 1$.*

Similarly as in [14] the above result could be used in the proofs of Lemmas 7, 8, 10 and 11.

The greatest difficulty in the proof of transitivity of $(B^{\mathbb{N}}, F)$ (see Theorem 5.1) is the case $p \geq 5$. Possibility of defining a local rule $F' : B^2 \to B$ without applying a function $\lfloor \rfloor$ is the first step to overcome this difficulty. An alternative possibility of defining $F' : B^2 \to B$ is presented in the lemma below.

Lemma 6. *(compare [14]) For $p \geq 5$ and any $j, k \in [0, p-1]$ and $\alpha_k, \gamma \in [0,1]$,*
$F'(2k + ((j+1-q)(q+k)+1+\alpha_k)mod\,2, 2j+\gamma) = 2((j+k)mod\,p) + \alpha_k$.

Proof. Let
$$a = 2k + ((j+1-q)(q+k)+1+\alpha_k)\,mod\,2,$$
$$b = 2j + \gamma.$$

We have
$$2((\lfloor a/2 \rfloor + \lfloor b/2 \rfloor)\,mod\,p) = 2((k+j)\,mod\,p).$$

Additionally
$$(a + 1 + \lfloor \lfloor a/2 \rfloor + q \rfloor \lfloor \lfloor b/2 \rfloor + 1 - q \rfloor)\,mod\,2$$
$$= (2k + (j+1-q)(q+k)+1+\alpha_k+1+(k+q)(j+1-q))mod\,2$$
$$= (2(k + (j+1-q)(q+k)+1)+\alpha_k)mod\,2$$
$$= \alpha_k.$$

$\square$

4. Transitivity of F for $p \geq 5$

The main goal of this section is to prove transitivity of the cellular automaton $(B^{\mathbb{N}}, F)$ for $p \geq 5$. We present also lemmas and some properties that lead to the justification of Corollary 14. All along this section it is assumed that $p \geq 5$.

The lemma presented below can be considered as a counterpart of Lemma 5 but it is formulated for $(B^{\mathbb{N}}, F)$.

In contrast to the formula for G'^{p^n} in Lemma 5 the formula presented below for F'^{p^n} depends on a chosen word $\varphi'(w) \in A^{p^n - 1}$. The choice of $\varphi'(w) \in A^{p^n - 1}$ determines values of coefficients $i \in [0, p-1]$ and $i_k \in [0, 1]$ which occur in the formula for any $k \in [0, p-1]$.

The lemma could be proved exactly in the way as its counterpart in [14] making use of Lemmas 1 and 4–6.

Lemma 7. *Let us assume that $n \in \mathbb{N}$, $w \in B^*$, $|w| = p^n - 1$. For any $j, k \in [0, p-1]$, $\alpha_k \in [0, 1]$, and some fixed $i \in [0, p-1]$, $i_k \in [0, 1]$,*

$$F'^{p^n}(2((k+i) \bmod p) + ((j+1-q)(q+k) + i_k + 1 + \alpha_k) \bmod 2, \varphi'(w), 2((j+p-i) \bmod p))$$
$$= 2((j+k) \bmod p) + \alpha_k$$

The following conclusions can be derived from Lemma 7 for any fixed $m \in [1, p-1]$.

Under the assumptions of the lemma, if $j = (i+m) \bmod p$, $b = 2(m \bmod p)$, $a = 2((k+i) \bmod p) + (i_k + 1 + \alpha_k) \bmod 2$ for $k = q$ and some $\alpha_q \in [0, 1]$, then for the following equalities $a_0 = a$, $a_l = F'^{p^n}(a_{l-1}, \varphi'(w), b)$ for any $l \in [1, p]$, we obtain $a_l = 2((lm + q + i) \bmod p) + \alpha_{((l-1)m+q) \bmod p}$ for $k = ((l-1)m + q) \bmod p$ and for any $l \in [1, p]$, $\alpha_{((l-1)m+q) \bmod p} = ((j+1-q)[q+k] + i_k + 1 + \alpha_k) \bmod 2$ for $k = (lm+q) \bmod p$ and for any $l \in [1, p-1]$. Notice that in view of Point 1 in Lemma 4 and Lemma 5 to calculate a_l for any $l \in [1, p]$, we can apply F'^{lp^n} to a word $a\varphi'(w)b \cdot 0^{(l-1)p^n} \in B^{lp^n+1}$.

A generalization of this observation leads to the lemma formulated below. The formulation is preceded by the introduction of some denotations.

We will use in the sequel the following notations: $e_\infty(a) = a000... = a0^\omega$, $e_0(a) = a$, $e_k(a) = a0^k$ for any $a \in A$, $k \in \mathbb{N} \setminus \{0\}$, $\theta(d) = d \bmod 2$ for any $d \in B$. Assume now that $n \in \mathbb{N}$, $w \in B^*$, $|w| = p^n - 1$. Lemma 7 implies that for any $j, k \in [0, p-1]$, $\alpha_k \in [0, 1]$,

$$F'^{p^n}(2((k+i) \bmod p) + ((j+1-q)(q+k) + i_k + 1 + \alpha_k) \bmod 2, \varphi'(w), 2((j+p-i) \bmod p))$$
$$= 2((j+k) \bmod p) + \alpha_k$$

for some fixed $i \in [0, p-1]$, $i_k \in [0, 1]$.

Now, let us fix $m \in [1, p-1]$ and $j = (i+m) \bmod p$, $b = 2((j+p-i) \bmod p)$, $a = 2((q+i) \bmod p) + (i_q + 1 + \alpha_q) \bmod 2$ for $\alpha_q \in [0, 1]$. Additionally let $\Delta_{\alpha_q} = \{F'^{l2p^n}(a, \varphi'(we_{(2l-1)p^n}(b)))\}_{l \in [1, p]}$, $s = (j + 2 - q + \sum_{l=0}^{p-1} i_l) \bmod 2$.

Lemma 8. *The following statements are true:*

(1) $\{\varphi'(F'^{2lp^n}(a\varphi'(we_{(2l-1)p^n}(b))))\}_{l \in [1, p]} = A$,

(2)

$$F'^{p^{n+1}}(a\varphi'(we_{(p-1)p^n}(b)))$$
$$= \; 2((q+i) \bmod p) + \alpha_{((p-1)m+q) \bmod p}, \alpha_{((p-1)m+q) \bmod p}$$
$$= \; (i_q + 1 + o) \bmod 2, o$$
$$= \; (s + \alpha_q) \bmod 2,$$

(3) $F'^{2p^{n+1}}(a\varphi'(we_{(2p-1)p^n}(b))) = a, \; \Delta_0 \cap \Delta_1 = \emptyset, \; \Delta_0 \cup \Delta_1 = B,$

$$F'^{lp^n}(a\varphi'(we_{(l-1)p^n}(b)))\}_{l \in [1, 2p]} = \begin{cases} \Delta_{\alpha_q}, & \text{if } s = 0 \\ B, & \text{if } s = 1. \end{cases}$$

(4) if $s = 0$, *then* $\theta(F'^{2lp^n}(a\varphi'(we_{(2l-1)p^n}(b)))) = \alpha_{((2l-1)m+q) \bmod p}$ *for* $l \in [1, p]$,

(5) if $s = 1$, *then:*

$$\theta(F'^{2lp^n}(a\varphi'(we_{(2l-1)p^n}(b)))) = \begin{cases} \alpha_{((2l-1)m+q) \bmod p}, & \text{for } l \in [1, (p-1)/2], \\ (1 + \alpha_{((2l-1)m+q) \bmod p}) \bmod 2, & \text{for } l \in [(p+1)/2, p]. \end{cases}$$

Proof. The first statement is left to the reader.

From Point 1 in Lemma 4 and Lemma 5 follows that for any $l \in [0, p-2]$,

$$\alpha_{(lm+q) \bmod p}$$
$$= \; (i_{((l+1)m+q) \bmod p} + 1 + \alpha_{((l+1)m+q) \bmod p} + (j + 1 - q)[q + (((l+1)m + q) \bmod p)]) \bmod 2,$$

$$\begin{aligned} F'^{p^n}(a\varphi'(we_0(b))) &= 2((m+q+i) \bmod p) + (i_{(m+q) \bmod p} + 1 + \alpha_{(m+q) \bmod p} \\ &\quad + (j+1-q)[q + (m+q) \bmod p]) \bmod 2, &\text{(1)} \\ F'^{2p^n}(a\varphi'(we_{p^n}(b))) &= 2((2m+q+i) \bmod p) + (i_{(2m+q) \bmod p} + 1 + \alpha_{(2m+q) \bmod p} \\ &\quad + (j+1-q)[q + (2m+q) \bmod p]) \bmod 2, &\text{(2)} \\ F'^{3p^n}(a\varphi'(we_{2p^n}(b))) &= 2((3m+q+i) \bmod p) + (i_{(3m+q) \bmod p} + 1 + \alpha_{(3m+q) \bmod p} \\ &\quad + (j+1-q)[q + (3m+q) \bmod p]) \bmod 2, &\text{(3)} \\ &\quad\quad \vdots \\ F'^{(p-1)p^n}(a\varphi'(we_{(p-2)p^n}(b))) &= 2(((p-1)m+q+i) \bmod p) + (i_{((p-1)m+q) \bmod p} + 1 + \alpha_{((p-1)m+q) \bmod p} \\ &\quad + (j+1-q)[q + ((p-1)m+q) \bmod p]) \bmod 2, &\text{(4)} \\ F'^{p^{n+1}}(a\varphi'(we_{p^n(p-1)}(b))) &= 2((pm+q+i) \bmod p) + \alpha_{((p-1)m+q) \bmod p} \\ &= 2((i+q) \bmod p) + (i_q + 1 + o) \bmod 2 \text{ for some } o \in [0, 1]. &\text{(5)} \end{aligned}$$

To finish the proof of Point 2, observe that the following equation holds:

$$(i_q + 1 + \alpha_q) \bmod 2$$
$$= \; (j + 1 - q + p + \sum_{l=0}^{p-1} i_l + \alpha_{((p-1)m+q) \bmod p}) \bmod 2$$
$$= \; (j + 2 - q + \sum_{l=0}^{p-1} i_l + i_q + 1 + o) \bmod 2.$$

Thus

$$o = (s + \alpha_q) \bmod 2.$$

The Point 3 follows according to Point 2, Lemmas 4, 5 and Equations (1)–(4). We have for $l \in [1, (p-1)/2]$,

$$\theta(F'^{2lp^n}(a\varphi'(we_{(2l-1)p^n}(b)))) = \alpha_{((2l-1)m+q) \bmod p}$$

For Point 4 observe that putting $o = \alpha_q$, the Equation (5) gives

$$F'^{pp^n}(a\varphi'(we_{(p-1)p^n}(b))) = 2((i+q) \bmod p) + (i_q + 1 + \alpha_q) \bmod 2 = a.$$

Thus from the Equations (1)–(4), we obtain

$$
\begin{aligned}
F'^{(p+1)p^n}(a\varphi'(we_{pp^n}(b))) &= F'^{p^n}(a\varphi'(we_0(b))) \\
F'^{2lp^n}(a\varphi'(we_{(2l-1)p^n}(b))) &= F'^{(2l-p)p^n}(a\varphi'(we_{(2l-(p+1))p^n}(b)))
\end{aligned}
$$

for $l \in [(p+1)/2, p]$. Consequently $\theta(F'^{2lp^n}(a\varphi'(we_{(2l-1)p^n}(b)))) = \alpha_{((2l-1)m+q) \bmod p}$ for $l \in [1, p]$.

Point 5 could be proved as above putting $o = (1 + \alpha_q) \bmod 2$ in the Equation (5). $\square$

The results proved above can be applied in the proofs of Lemmas 9, 10, 11, 13.

For a, b which fulfills exactly the assumptions introduced before Lemma 8 and for a fixed word $w \in B^*$, such that $|w| = p^n - 1$, $n \in \mathbb{N}$, let us consider the following set

$$\{F'^{l2p^n}(a, \varphi'(we_{(2l-1)p^n}(b))) : l \in [1, p]\}$$

If the set is independent of choosing and fixing $m \in [1, p-1]$ (remind that in fact b depends on m) we put $\{F'^{l2p^n}(a, \varphi'(we_{(2l-1)p^n}(b)))\}_{l \in [1, p]} = \Omega$ and say, that the Condition (*) is fulfilled for any $m \in [1, p-1]$.

In a similar way as in [14] the properties established in Lemma 8 give reason for an indirect proof of the lemma presented below. A contradiction is obtained by considering a system of linear equations formulated over $\mathbb{Z}_2$ assuming that the Condition (*) is fulfilled for any $m \in [1, p-1]$.

Lemma 9. *If $n \in \mathbb{N}$, $w \in B^*$, $|w| = p^n - 1$, then Condition (*) does not hold.*

The statement of the lemma means that there exist $m_1, m_2 \in [1, p-1]$, $m_1 \neq m_2$, $b_{m_1} \neq b_{m_2}$ such that

$$
\begin{aligned}
\Omega_{m_1} &:= \{F'^{l2p^n}(a, \varphi'(we_{(2l-1)p^n}(b = b_{m_1})))\}_{l \in [1, p]}, \\
\Omega_{m_2} &:= \{F'^{l2p^n}(a, \varphi'(we_{(2l-1)p^n}(b = b_{m_2})))\}_{l \in [1, p]} \\
\Omega_{m_1} &\neq \Omega_{m_2}
\end{aligned}
$$

Consequently,

(1) there exist $a' \in \Omega_{m_2} \setminus \Omega_{m_1}$, $l_2 \in [1, p]$ such that $F'^{l_2 2p^n}(a, \varphi'(we_{(2l_2-1)p^n}(b_{m_2}))) = a'$,

(2) $\{F'^{l2p^n}(a, \varphi'(we_{(2l-1)p^n}(b_{m_1})))\}_{l \in [1, p]} = \Omega_{m_1}$,

(3) $\{F'^{l2p^n}(a', \varphi'(we_{(2l-1)p^n}(b_{m_1})))\}_{l \in [1, p]} = B \setminus \Omega_{m_1}$ (Lemma 8, point 3)

Similarly as in [14] the above property and Lemma 11 play a key role in the proof of transitivity of $(B^{\mathbb{N}}, F)$ (see Lemma 13).

A subsequent lemma, rather a technical one, can be proved exactly as its counterpart in [14] and in the proof Lemma 4, 5 and 8 are used.

Lemma 10.

(1) If $a \in B$, $w \in B^+$, $p^n - 1 > |w| \geq p^{n-1}$, $n \in \mathbb{N} \setminus \{0\}$, then $F'^{2p^n}(awe_{2p^n-1-|w|}(p-1)) = a$,

(2) If $w \in B^+$, $|w| = p^n - 1$, $n \in \mathbb{N} \setminus \{0\}$, then

    (a) if $a \in B$, then $F'^{2p^{n+1}}(awe_{p^n(2p-1)}(p-1)) = a$,

    (b) if $a \in B$, $F'^{l_1 2p^n+k}(awe_{p^n(2p-1)}(p-1))(0) = c \in B$, $F'^{l_2 2p^n+k}(awe_{p^n(2p-1)}(p-1))(0) = c' \in B$ for any $l_1 \neq l_2$, $l_1, l_2 \in [0, p-1]$, $k \in [0, 2p^n - 1]$, then $\varphi'(c) \neq \varphi'(c')$.

It is easy to notice that for any fixed $b \in A \setminus \{0\}$, any expression of the form $e_k(p - 1)$ for some $k \in \mathbb{N}$, which occurs in the assertion of the above Lemma could be replaced by $e_k(b)$.

The same observation is true for Lemma 11.

Let us denote $R_{p^n} = EB^{p^{n-1}(p-1)-1}...EB^{p^3(p-1)-1}EB^{p^2(p-1)-1}EB^{p(p-1)-1}EB^{(p-1)-1}\{0\}$ for any $n \in \mathbb{N} \setminus \{0\}$. Notice that, if $n \in \mathbb{N} \setminus \{0\}$, $w \in R_{p^n}$ then $|w| = p^n$.

Lemmas 4, 8 and 10 play a key role in an inductive proof of the following lemma. The proof is left to the reader.

Lemma 11. *For any* $n \in \mathbb{N} \setminus \{0\}$ *the following assertions are true:*

(1) $F'^{2p^n}(q_n e_{2p^n-1}(p-1)) = q_n$,
    $F'^{2p^{n+1}}(t_n e_{2p^{n+1}-1}(p-1)) = t_n$,
    $\#\{F'^k(t_n e_{2p^{n+1}-1}(p-1))_{[0,\,p^n)} : k \in [0,\, 2p^{n+1} - 1]\} = 2p^{n+1}$,
    $\#(\{F'^k(t_n e_{2p^{n+1}-1}(p-1))_{[0,\,p^n)} : k \in [0,\, 2p^{n+1} - 1]\} \cap R_{p^n}) = 1$
    for every $t_n \in Eq_n \subset R_{p^n}$,

(2) $\bigcup_{t_n \in R_{p^n}}\{F'^k(t_n e_{2p^{n+1}-1}(p-1))_{[0,\,p^n)} : k \in [0,\, 2p^{n+1} - 1]\} = B^{p^n}$.

The result of the above lemma is used later when we prove that $(B^{\mathbb{N}}, F)$ is D-chaotic.

For $n \in \mathbb{N} \setminus \{0\}$ and $w \in R_{p^n}$, let us denote:

$Q_{p^n,\,w} = \{F^k(we_\infty(p-1)) \in B^{\mathbb{N}} : k \in [0,\, 2p^{n+1} - 1]\}$, $\quad Q_{p^n} = \bigcup_{w \in R_{p^n}} Q_{p^n,\,w}$.

From Lemma 11 for any $n \in \mathbb{N} \setminus \{0\}$ we have $F^{2p^{n+1}}(x) = x$ for any $x \in Q_{p^n}$ and $\bigcup_{x \in Q_{p^n}}\{x_{[0,\,p^n)}\} = B^{p^n}$. Since the family $\{tB^\omega\}_{n \in \mathbb{N}\setminus\{0\},\,t \in B^{p^n}}$ is a base of $B^{\mathbb{N}}$ then we obtain the following corollary.

Corollary 12. $Per(F)$ *is dense in* $B^{\mathbb{N}}$.

For $n \in \mathbb{N}\setminus\{0\}$, $w \in B^{p^n}$, $c \in B$, $i \in [0, p^n)$ define a word $w[i, c] \in B^{p^n}$ putting for $j \in [0, p^n)$

$$w[i,\, c](j) = \begin{cases} w(j) & \text{if } j > i, \\ c & \text{if } i = j \end{cases}$$

and $w[i, c](j) \in B$ for $j < i$.

The above denotation facilities presentation of the following observations.

According to Lemma 9 Condition (*) does not hold. Thus Point 1 of Lemma 4 implies that for $i \in [1, p^n)$, there exist $m_1, m_2 \in [1, p-1]$, $m_1 \neq m_2$, $b_{m_1} \neq b_{m_2}$ such that

$$\{F'^{k2p^n}(w[i,c]e_{i-1}(p-1)e_{k2p^n-i-1}(b_{m_1}))(i)\}_{k\in[1,p]} = \Omega_{m_1},$$
$$\{F'^{k2p^n}(w[i,c]e_{i-1}(p-1)e_{k2p^n-i-1}(b_{m_2}))(i)\}_{k\in[1,p]} = \Omega_{m_2}, \quad \text{where } \Omega_{m_1} \neq \Omega_{m_2}.$$

Additionally, from Lemma 11 we have

$$F'^{k2p^n}(w[i,c]e_{i-1}(p-1)e_{k2p^n-i-1}(b_m)) = w[i,d], \text{for } m = m_1 \text{ or } m = m_2 \text{ and for } k \in \mathbb{N} \setminus \{0\}.$$

Observations made above, the possibility of choosing $b_m \in \{b_{m_1}, b_{m_2}\}$ and the fact that i varies in the range from $i = p^n - 1$ to $i = 0$ play an essential role in the proof of the subsequent lemma. This proof, based also on Lemmas 4, 8, 9 and 11 is analogical to the proof of its counterpart in [14].

Lemma 13. *Let us assume that*

$$n \in \mathbb{N} \setminus \{0\}, \quad x, y \in Q_{p^n}, \quad t = x_{[0,p^n)}, \quad t' = y_{[0,p^n)} \in B^{p^n}.$$

There exists

$$l \in \mathbb{N} \setminus \{0\}$$

such that

$$tB^\omega \cap F^{-l2p^n}(t'B^\omega) \neq \emptyset.$$

Lemma 3 implies that $F : B^{\mathbb{N}} \to B^{\mathbb{N}}$ is surjective. Observe that the family $\{tB^\omega\}_{n\in\mathbb{N}\setminus\{0\}, t\in B^{p^n}}$ is a base of $(B^{\mathbb{N}}, \tau_d)$ and thus it is enough to prove that for any $n \in \mathbb{N} \setminus \{0\}$, $t, t' \in B^{p^n}$ there exists $m \in \mathbb{N} \setminus \{0\}$ such that $tB^\omega \cap F^{-m}(t'B^\omega) \neq \emptyset$. From Lemma 11 we have $\bigcup_{x\in Q_{p^n}}\{x_{[0,p^n)}\} = B^{p^n}$ for any $n \in \mathbb{N} \setminus \{0\}$. Thus Lemma 13 implies the following corollary.

Corollary 14. *Cellular automaton $F : B^{\mathbb{N}} \to B^{\mathbb{N}}$ is transitive.*

5. Main Result

This section contains the main result concerning the cellular automaton $(B^{\mathbb{N}}, F)$, that is a theorem presented below. It exposes these properties of F, which are invariants of a topological conjugacy.

Theorem 15. *For any prime number p the considered automaton $F : B^{\mathbb{N}} \to B^{\mathbb{N}}$ defined over an alphabet B of $2p$ elements has the following properties:*

(1) is not injective,

(2) has no fixed points,

(3) has continuum of periodic points with period equal to 2,

(4) has topological entropy $h(B^{\mathbb{N}}, F) = \log(p) > 0$,

(5) is D-chaotic.

Proof. From Lemma 3 follows that F is not injective, is surjective and has no fixed points, has continuum of periodic points with period 2 and finally its topological entropy is equal to $\log(p) > 0$.

The last assertion is proved considering two subcases.

For the first subcase assume that $p \leq 3$. A form of the local rule $F' : B^2 \to B$ allows for a construction of oriented graphs having properties exactly as required in [13,15]. Arguing analogically as in [13,15] we finally obtain density of $Per(F)$ in $B^{\mathbb{N}}$, and transitivity of F.

For the second subcase assume that $p \geq 5$. From Corollary 12 $Per(F)$ is dense in $B^{\mathbb{N}}$ and Corollary 14 implies that F is transitive. Hence in any case F is D-chaotic. $\square$

The following conclusions points out some possibilities of classification of the cellular automaton $(B^{\mathbb{N}}, F)$ in Cantor metric space $A^{\mathbb{N}}$.

A positively expansive cellular automaton defined in $B^{\mathbb{N}}$ is topologically conjugated with a one-sided subshift of finite type (SFT) [1,2], which has no infinite set of periodic points with the period 2. Cardinality of the set of periodic points with the period 2 is an invariant of a topological conjugacy. Hence basing on Point 3 of Theorem 15 the following corollary could be derived.

Corollary 16. *Cellular automaton F is not positively expansive.*

Defined for any prime p, and presented in [13–15] a one-sided cellular automaton associated to F has continuum of fixed points and topological entropy $\log(p)$. Cardinality of the set of fixed points is an invariant of a topological conjugacy. Thus Point 2 of Theorem 15 leads to the following corollary.

Corollary 17. *For any fixed prime number p, the cellular automaton F is not topologically conjugated with an associated one-sided, D-chaotic cellular automaton presented in [13–15] having continuum of fixed points and topological entropy $\log(p)$.*

Below we present an example of a cellular automaton $(B^{\mathbb{N}}, F)$ which is not transitive. It is defined in $B^{\mathbb{N}}$, by a local rule $F' : B^2 \to B$ over an alphabet $B = \{0, 1, 2, ..., 2p-1\}$ for which a mapping $\varphi : (B^{\mathbb{N}}, F) \to (A^{\mathbb{N}}, G)$ defined in Section 3 is a surjective morphism SDS, $F'(a\varphi'(b)) = F'(ab)$ for any $a, b \in B$, and has the following properties:

(1) is left permutative,

(2) is right-closing,

(3) is surjective and non-injective,

(4) has no fixed points,

(5) has continuum of periodic points with the period 2,

(6) is non transitive.

Example 1. *Let us consider*

$$F : B^{\mathbb{N}} \to B^{\mathbb{N}},$$

$$F' : B^2 \to B,$$

$$F'(a, b) = f'(a, b) + G'(\varphi'(a), \varphi'(b)),$$

$$f'(ab) = (a + 1) \, mod \, 2, \quad \forall a, b \in B.$$

Just from the definition of F', for any fixed $b, c \in B$ there exists exactly one symbol $a = \varphi'(a) + a \bmod 2 \in B$ such that $F'(ab) = c$. Hence $(B^{\mathbb{N}}, F)$ is left-permutative [21] and so surjective [23].

Additionally, if $F'(da) = F'(db)$ for some $d, a, b \in B$ and $a \neq b$, then $\varphi'(a) = \varphi'(b)$ and $F'(ac) \neq F'(bc)$ for any $c \in B$. Thus $(B^{\mathbb{N}}, F)$ is right-closing and has a dense set of jointly periodic points [24].

For $p \geq 3$, if we take $x, x' \in B^{\mathbb{N}}$, such that

$$x'(2i+1) = x(2i) = p$$
$$x'(2i) = x(2i+1) = p+2, \forall i \in \mathbb{N},$$

then

$$F(x) = F(x') = 00000... \in B^{\mathbb{N}}.$$

For $p = 2$ we have

$$F(1111....) = F(3333....) = 000....$$

Additionally $F'(ac) \neq a$ for any $a, c \in B$. Consequently $(B^{\mathbb{N}}, F)$ is not injective and has no fixed points. Notice that $F'(ac) = 1 - a$ for any $a, c \in E$. Hence, if $x \in E^{\mathbb{N}}$, then $F^2(x) = x$ and cardinality of the set $E^{\mathbb{N}}$ is continuum.

Just from the definition of $F' : B^2 \to B$ follows that

$$F'(aAA) = (B \setminus A)^2, \quad \forall a \in A,$$
$$F'(b(B \setminus A)A) = A^2, \quad \forall b \in B \setminus A.$$

Hence, for any $t \in C = A^2 \cup (B \setminus A)^2$ and $t' \in B^2 \setminus C$ we have $F'(ts) \neq t'$ for every $s \in B$. It means, that for any $t \in C$, $t' \in B^2 \setminus C$ and any integer $m \in \mathbb{N} \setminus \{0\}$ it holds $tB^{\omega} \cap F^{-m}(t'B^{\omega}) = \emptyset$. It excludes transitivity of $(B^{\mathbb{N}}, F)$.

Acknowledgments

Author contributions

The paper was written by Wit Foryś and Janusz Matyja. The authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Blanchard, F.; Maass, A. Dynamical Properties of Expansive Cellular Automata. *Isr. J. Math.* **1997**, *99*, 149–174.
2. Boyle, M.; Fiebig, D.; Fiebig, U. A Dimension Group for Local Homeomorphisms and Endomorphisms of One-sided Shifts of Finite Type. *J. Reine Angew. Math.* **1997**, *487*, 27–59.
3. Boyle, M.; Maass, A. Expansive Invertible One-sided Cellular Automata. *J. Math. Soc. Jpn.* **2000**, *52*, 725–740.
4. Dartnell, P.; Maass, A.; Schwartz, F. Combinatorial Constructions Associated to the Dynamics of One-sided Cellular Automata. *Theor. Comput. Sci.* **2003**, *304*, 485–497.
5. Nasu, M. The Dynamics of Expansive Invertible One-sided Cellular Automata. *Trans. Am. Math. Soc.* **2002**, *354*, 4067–4084.
6. Acerbi, L.; Dennunzio, A.; Formenti, E. Conservation of Some Dynamical Properties for Operations on Cellular Automata. *Theor. Comput. Sci.* **2009**, *410*, 3685–3693.
7. Dennunzio, A.; Di Lena, P.; Margara, L. Strictly Temporally Periodic Points in Cellular Automata. **2012**, arXiv:1208.2770.
8. Dennunzio, A.; Di Lena, P.; Formenti, E.; Margara, L. Periodic Orbits and Dynamical Complexity in Cellular Automata. *Fund. Inform.* **2013**, *126*, 183–199.
9. Kari, J.; Zhang, K. Two Transitive Cellular Automata and Their Strictly Temporally Periodic Points. In Proceedings of AUTOMATA 2013—19th International Workshop on Cellular Automata and Discrete Complex Systems, Gieβen, Germany, 17–19 September 2013.
10. Kitchens, B.P. *Symbolic Dynamics: One-sided, Two-sided and Countable State Markov Shifts*; Springer-Verlag: Berlin, Germany, 1998.
11. Blanchard, F.; Cervelle, J.; Formenti, E. Some Results About the Chaotic Behavior of Cellular Automata. *Theor. Comput. Sci.* **2005**, *349*, 318–336.
12. Delorme, M.; Mazoyer, J. *Cellular Automata: A Parallel Model*; Kluwer Academic Publishers: Dordrecht, The Netherlands, 1999.
13. Foryś, W.; Matyja, J. An Example of One-sided, D-chaotic CA over Four Elementary Alphabet, which is not E-chaotic and not Injective. *J. Cell. Auto.* **2011**, *6*, 231–243.
14. Foryś, W.; Matyja, J. On One-sided, D-chaotic Cellular Automata, having Continuum of Fixed Points and Topological Entropy log(p) for any Prime $p > 3$. *J. Cell. Auto.* **2012**, *7*, 303–319.
15. Foryś, W.; Matyja, J. On One-sided, D-chaotic Cellular Automaton, having Continuum of Fixed Points and Topological Entropy log(3). *J. Cell. Auto.* **2013**, *8*, 131–146.
16. Banks, J.; Brooks, J.; Cairns, G.; Davis, G.; Stacey, P. On Devaney's Definition of Chaos. *Am. Math. Mon.* **1992**, *99*, 332–334.
17. Lind, D.; Marcus, B. *An Introduction to Symbolic Dynamics and Coding*; Cambridge University Press: Cambridge, UK, 1995.
18. Nasu, M. Expansive Automorphisms and Expansive Endomorphisms of the Shift. *Dyn. Compl. Syst.* **2004**, *1404*, 68–82.
19. Degirmenci, N.; Kocak, S. Chaos in Product Maps. *Turk. J. Math.* **2010**, *34*, 593–600.
20. Walters, P. *An Introduction to Ergodic Theory*; Springer-Verlag: New York, NY, USA, 1982.

21. Kurka, P. *Topological Dynamics of One-dimensional Cellular Automata, Encyclopedia of Complexity and System Sciences*; Springer-Verlag: Berlin, Germany, 2008.

22. Di Lena, P. On Computing the Topological Entropy of One-sided Cellular Automata. *J. Cell. Auto.* **2007**, *2*, 121–130.

23. Kurka, P. *Topological and Symbolic Dynamics*; SMF, Cours Specialises: Paris, France, 2003.

24. Boyle, M.; Kitchens, B. Periodic Points for Onto Cellular Automata. *Indagat. Math.* **1999**, *10*, 483–493.

25. Codenotti, B.; Margara, L. Transitive Cellular Automata are Sensitive. *Am. Math. Mon.* **1996**, *103*, 58–62.

26. Dennunzio, A.; Di Lena, P.; Formenti, E.; Margara, L. On the Directional Dynamics of Additive Cellular Automata. *Theor. Comput. Sci.* **2009**, *410*, 4823–4833.

27. Di Lena, P.; Margara, L. Row Subshifts and Topological Entropy of Cellular Automata. *J. Cell. Auto.* **2007**, *2*, 131–140.

28. Subrahmonian Moothathu, T.K. Set of Periods of Additive Cellular Automata. *Theor. Comput. Sci.* **2006**, *352*, 226–231.