We study the chaotic behavior of a particular class of dynamical systems: cellular automata. We specialize the definition of chaos given by Devaney for general dynamical systems to the case of cellular automata. A dynamical system \((X, F)\) is chaotic according to Devaney's definition of chaos if its transition map \(F\) is sensitive to the initial conditions, topologically transitive, and has dense periodic orbits on \(X\). Our main result is the proof that all the additive one-dimensional cellular automata defined on a finite alphabet of prime cardinality are chaotic in the sense of Devaney.

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 state of the CA, specified by the values of the variables at a given time, evolves in synchronous discrete time steps according to a given local rule.

CA have been widely used to model a variety of dynamical systems in physics, biology, chemistry, and computer science (see for example [1, 10–12, 18]). Despite their apparent simplicity, CA can display a rich and complex evolution. The exact determination of their temporal evolution is in general very hard, if not impossible. In particular, many properties of the temporal evolution of CA are undecidable [6, 8, 17].

In this paper we study the chaotic behavior of additive one-dimensional cellular automata. Informally, a deterministic dynamical system is chaotic if it is impossible to predict its future evolution, even for a short period of time, no matter how accurate...
is the description of the initial state. In this case, we will say that the system is *unpredictable*.

The existence of chaos for a discrete dynamical system whose temporal evolution obeys a deterministic rule is counterintuitive. Consider, for example, the case of CA. We are given a set of configurations and a deterministic map $F$ from a configuration to another one. Can such a dynamical system exhibit a chaotic evolution?

If we assume to be able to memorize each configuration and to compute $F$ with infinite precision, then the answer is no. If we make more realistic assumptions, e.g., we can memorize and use only a finite part of each configuration, then the answer is yes. In fact, the lack of infinite precision causes a loss of information which in turn is responsible of a transition from determinism to nondeterminism (unpredictability).

For discrete dynamical systems, such as CA, a formal definition of chaos does not exist. In the case of one-dimensional CA, there have been many attempts of classification according to their asymptotic behavior (see for example [7,15,20,22]), but none of them completely captures the notion of chaos. Existing classifications of CA are generally obtained as the outcome of experiments and do not rely on precise mathematical definitions. As an example, Wolfram [23] has suggested the following classification of CA into four classes. Class 1 contains CA that evolve to a unique homogeneous state after a finite transient (static CA). Class 2 contains CA whose evolution leads to a set of separated simple stable or periodic structures (space–time patterns) (periodic CA). Class 3 contains CA whose evolution leads to aperiodic (chaotic) space–time patterns (chaotic CA). Class 4 contains CA that evolve to complex patterns with propagative localized structures, sometimes long-lived (complex CA). This classification scheme is not based on a formal definition. It rather relies on empirical evidence gathered from a large number of experiments.

In the case of continuous dynamical systems, the theory of chaos is much more developed and it provides a number of elegant theoretical tools. Many formal definitions of chaos have been proposed during the last few years. Although a universally accepted definition of chaos does not exist, Devaney in [9] states one of the most used definitions.

Informally, a dynamical system consists of a space $X$ of configurations and of a transition map $F$, $F : X \to X$, which governs the temporal evolution of the system. A dynamical system $(X,F)$ is chaotic according to Devaney's definition of chaos if $F$ is sensitive to initial conditions, is transitive, and has dense periodic orbits. Sensitivity is recognized as a central notion in chaos theory because it captures the feature that in chaotic systems small errors in experimental readings lead to large scale divergence, i.e., the system is unpredictable. Note that if $f$ is sensitive to initial conditions, then for all practical purposes, its dynamics defies numerical computation. In fact, due to round-off errors, the finite-precision computation of an orbit, no matter how accurate, may be very different from the real orbit. Transitivity guarantees that the system cannot be decomposed into two or more subsystems which do not interact under $F$. Denseness of periodic orbits is an element of regularity for the system.

In this paper we consider additive one-dimensional CA defined on a finite alphabet of prime cardinality. Additive CA have been studied by several authors (see for
example [5, 14, 19]). Despite their simplicity that allows an algebraic analysis, additive CA exhibit many of the complex features of general CA. They have been used for modeling and approximating many physical phenomena (see for example [21]). We prove that they are chaotic according to the definition of chaos given by Devaney.

We show that the sensitivity of the local rule on which a CA is based plays a crucial role in determining its chaotic evolution. Informally, we say that a map $f$ is sensitive to one of its input variables if the output of $f$ strongly depends on that variable. As an example, consider the map $f$ which takes as input three bits and outputs the sum modulo 2 of the first and the third bit. This map is sensitive to the first and to the third variable and it is not sensitive to the second one (which never affects the output). We prove that a CA based on a local rule which is sensitive to its leftmost and/or rightmost variable is transitive.

In order to prove that additive CA have dense periodic orbits, we use a counting technique. We show that if the fraction of periodic configurations for a certain sequence $F_n$ of circular CA of suitable increasing size $n$ does not depend on $n$, then the corresponding infinite CA $F$ has dense periodic orbits. This technique allows us to establish a relation between the dynamics of an infinite sequence $(F_n)$ of finite circular CA and the dynamics of an infinite CA $(F)$. In the case of boolean additive CA based on local rules which depend on three input variables, we provide two ad hoc techniques which allow one to construct periodic orbits arbitrarily close to a given configuration.

The rest of this paper is organized as follows. In Section 2 we give some basic notations and definitions. In Section 3 we prove that additive one-dimensional CA are chaotic according to Devaney’s definition of chaos. In Section 4 we show how to construct periodic orbits which are arbitrarily close to any given configuration in the case of elementary CA. Section 5 contains conclusions and open problems.

### 2. Notations and definitions

Let $\mathcal{A} = \{0, 1, \ldots, m - 1\}$ be a finite alphabet and $f, f : \mathcal{A}^{2k+1} \to \mathcal{A}$, be any map. A one-dimensional CA based on the local rule $f$ is a pair $(\mathcal{A}^Z, F)$, where

$$F[c](i) = f(c(i - k), \ldots, c(i + k)), \quad c \in \mathcal{A}^Z, \quad i \in \mathbb{Z}.$$  

is the space of configurations and $F, F : \mathcal{A}^Z \to \mathcal{A}^Z$, is defined as follows.

$$f \text{ depends on } 2k + 1 \text{ variables which will be denoted by } x_{-k}, \ldots, x_k. $$ For this reason, we say that $k$ is the radius of $f$.

Throughout the paper, $F[c]$ will denote the result of the application of the map $F$ to the configuration $c$ and $c(i)$ will denote the $i$th element of the configuration $c$. We recursively define $F^n[c]$ by $F^n[c] = F[F^{n-1}[c]]$, where $F^1[c] = F[c]$. A configuration $c \in \mathcal{A}^Z$ is spatially periodic of period $n$ if and only if $c(i) = c(i + n), i \in \mathbb{Z}$. A finite
configuration \( c \in \mathcal{A}^n \) is a map from \( \{0, \ldots, n - 1\} \) to \( \mathcal{A} \). Let \( c \in \mathcal{A}^n \). We define \( c_\infty \in \mathcal{A}^Z \) as follows.

\[
c_\infty(nh + i) = c(i), \quad h \in \mathbb{Z}, \quad 0 \leq i < n.
\]

A configuration \( c \in \mathcal{A}^Z \) is of time period \( n \) for the map \( F \) if and only if \( F^n[c] = c \).

When no confusion arises, we will say that a configuration is of period \( n \) instead of time period \( n \).

One can easily verify that the temporal behavior of \( F \) over spatial periodic configurations of period \( n \) is isomorphic to the temporal behavior of the circular CA \( F_n \) defined by

\[
F_n[c](i) = f(c((i - k) \mod n), \ldots, c((i + k) \mod n)), \quad c \in \mathcal{A}^n, \quad 0 \leq i < n.
\]

Let \( f, f : \mathcal{A}^{2k+1} \to \mathcal{A} \), be a local rule, and \( m \) the cardinality of \( \mathcal{A} \). Note that if \( c \in \mathcal{A}^n \) is a periodic configuration for \( F_n \), then \( c_\infty \) is a periodic configuration for \( F \).

We now give the definitions of permutive and additive local rule.

**Definition 1** (Hedlund [16]). \( f \) is permutive in \( x_i, -k \leq i \leq k \), if and only if, for any given sequence \( x_{-k}, \ldots, x_i, \ldots, x_k \in \mathcal{A}^{2k} \), we have

\[
\{f(x_{-k}, \ldots, x_i, \ldots, x_k) : x_i \in \mathcal{A}\} = \mathcal{A}.
\]

**Definition 2.** \( f \) is leftmost [rightmost] permutive if and only if there exists an integer \( i, -k \leq i \leq k \), such that

- \( i < 0 \) [\( i > 0 \)],
- \( f \) is permutive in the \( i \)th variable,
- \( f \) does not depend on \( x_j, j < i, [j > i] \).

**Definition 3** (Martin et al. [19]). \( f \) is additive if and only if it can be written as

\[
f(x_{-k}, \ldots, x_k) = \left( \sum_{t=-k}^k \lambda_t x_t \right) \mod m,
\]

where \( \lambda_t \in \mathcal{A} \).

From now on, we will say that a CA is permutive or additive if the local rule on which it is based is permutive or additive.

Let \( g, g : \mathcal{A} \to \mathcal{A} \), be any map. We say that a local rule \( f, f : \mathcal{A}^{2k+1} \to \mathcal{A} \), is trivial if it satisfies \( f(x_{-k}, \ldots, x_k) = g(x_0) \). Trivial CA (CA based on a trivial local rule) exhibit a simple behavior, and they are not transitive.

Note that if \( \mathcal{A} \) is an alphabet of prime cardinality and \((\mathcal{A}^Z, F)\) is a non-trivial additive CA, then at least one of the following two properties hold:

- \((\mathcal{A}^Z, F)\) is leftmost permutive.
- \((\mathcal{A}^Z, F)\) is rightmost permutive.
2.1. The Devaney's definition of chaos

The popular book by Devaney [9] isolates three components as being the essential features of chaos. They are formulated for a continuous map $F, F : X \to X$, on some metric space $(X,d)$.

(1) $F$ is transitive, i.e., for all nonempty open subsets $U$ and $V$ of $X$ there exists a natural number $n$ such that $F^n(U) \cap V \neq \emptyset$.

(2) Let $P(F) = \{x \in X | \exists n > 0, F^n(x) = x\}$ be the set of periodic points of $F$. $P(F)$ is a dense subset of $X$, i.e., for any $x \in X$ and $\varepsilon > 0$, there exists a $y \in P(F)$ such that $d(x, y) < \varepsilon$.

(3) There exists a $\delta > 0$ such that for any $x \in X$ and for any neighborhood $N(x)$ of $x$, there is a point $y \in N(x)$ and a natural number $n$, such that $d(F^n(x), F^n(y)) > \delta$. $\delta$ is called sensitivity constant.

Condition (3) is known as sensitive dependence to initial conditions or simply sensitivity.

In [2] it has been proved that for general dynamical systems (1) and (2) imply (3). In [4] it has been proved that, for CA, transitivity alone implies sensitivity. Thus, for CA, the notion of transitivity becomes central to chaos theory.

In order to apply the Devaney's definition of chaos to CA we use the following definition of distance (Tychonoff distance) over the space of the configurations.

$$d(a, b) = \frac{1}{\sum_{i=-\infty}^{+\infty} m^{|a(i) - b(i)|}}, \quad a, b \in \mathcal{A}^\mathbb{Z},$$

where $m$ denotes the cardinality of $\mathcal{A}$. It is easy to verify that $d$ is a metric on $\mathcal{A}^\mathbb{Z}$ and that the metric topology induced by $d$ coincides with the product topology induced by the discrete topology of $\mathcal{A}$. With this topology, $\mathcal{A}^\mathbb{Z}$ is a compact and totally disconnected space and $F$ is a (uniformly) continuous map.

3. Additive CA are chaotic

In this section we prove the main result of the paper. More precisely, we show that additive one-dimensional CA defined on a finite alphabet of prime cardinality satisfy conditions (1) and (2) above and thus, by [2], are chaotic in the sense of Devaney.

We now prove that if a one-dimensional CA is leftmost or rightmost permutive then it is transitive.

**Theorem 1.** Let $f$ be any local rule. If $f$ is rightmost [leftmost] permutive then $F$ is transitive.

**Proof.** Assume, without loss of generality, that $f$ is rightmost permutive. Moreover, assume that $f$ is permutive in the $h$th variable $h > 0$ and it does not depend on the
variables $x_{h+1}, \ldots, x_k$. We have to show that for any two open sets $U, V \subseteq \mathcal{A}^Z$ there exists an integer $n$ such that $F^n[U] \cap V \neq \emptyset$. Let $u \in U$ and $v \in V$ be two configurations of $\mathcal{A}^Z$. Since $U$ and $V$ are open sets, there exists a ball $B(v, \varepsilon_1)$ centered in $v$ of radius $\varepsilon_1 > 0$ entirely contained in $V$ and a ball $B(u, \varepsilon_2)$ centered in $u$ of radius $\varepsilon_2 > 0$ entirely contained in $U$. Take $\varepsilon = \min\{\varepsilon_1, \varepsilon_2\}$. We prove that starting from a configuration $u' \in B(u, \varepsilon)$, after a certain number of steps, we reach a configuration $v' \in B(v, \varepsilon)$. Let $M_\varepsilon$ be the smallest integer which satisfies the two following properties:

(i) $\sum_{i=-\infty}^{-M_\varepsilon+1} (m-1)/m^{|i|} + \sum_{i=M_\varepsilon}^{+\infty} (m-1)/m^{|i|} < \varepsilon$,

(ii) $M_\varepsilon$ is a multiple of $h$.

Let $n = 2M_\varepsilon/h$. We show that there exists a configuration $u' \in B(u, \varepsilon)$ such that $F^n[u'](i) \neq v(i)$ only for $|i| > M_\varepsilon$. We construct $u'$ as follows. We start from $u$ which trivially belongs to $B(u, \varepsilon)$. Then we find a sequence of configurations $\{u_i\}$, $0 < i < 2M_\varepsilon$, such that

1. $u_i \in B(u, \varepsilon)$, $0 < i < 2M_\varepsilon$,
2. $F^n[u_i](j) = v(j)$, $-M_\varepsilon < j \leq -M_\varepsilon + i$, $0 < i < 2M_\varepsilon$.

We construct $u_0$ as follows. For any $j \in Z$,

$u_0(j) = \begin{cases} 
u_0 & \text{if } j = M_\varepsilon + 1 \text{ and } v(-M_\varepsilon) \neq F^n[u](-M_\varepsilon), \\ u(j) & \text{otherwise.} \end{cases}$

Since $f$ is permutive in the rightmost variable, one can verify that there exists a unique $t_0 \in \mathcal{A}$ such that $v(-M_\varepsilon) = F^n[u_0](-M_\varepsilon)$. Since $u_0(j) = u(j)$ for $-M_\varepsilon \leq j \leq M_\varepsilon$, then $u_0(j)$ belongs to $B(u, \varepsilon)$.

We now show how to construct $u_{i+1}$ given $u_i$. For any $j \in Z$,

$u_{i+1}(j) = \begin{cases} u_{i+1} & \text{if } j = M_\varepsilon + i + 2 \text{ and } v(-M_\varepsilon + i + 1) \neq F^n[u](M_\varepsilon + i + 1), \\ u_{i}(j) & \text{otherwise.} \end{cases}$

Since $u_{i+1}(j) = u(j)$ for $-M_\varepsilon \leq j \leq M_\varepsilon$, then $u_{i+1}(j)$ belongs to $B(u, \varepsilon)$. Since $f$ is permutive in the rightmost variable, one can verify that there exists a unique element $t_{i+1} \in \mathcal{A}$ such that $v(-M_\varepsilon + i + 1) = F^n[u_{i+1}](M_\varepsilon + i + 1)$.

We now have $F^n[u'] \in B(v, \varepsilon)$, for $u' = u_{2M_\varepsilon}$. \hfill $\square$

As a consequence of Theorem 1 we have that all the nontrivial additive CA defined on any alphabet of prime cardinality are transitive.

Note that Theorem 1 holds for the class of leftmost and/or rightmost permutive CA which includes both additive and nonadditive CA. In [13] it has been shown that there exist transitive CA which are neither leftmost nor rightmost permutive.

The following lemmas allow us to prove that additive CA have dense periodic orbits.

Lemma 2 (Hedlund [16]). Let $b \in \mathcal{A}^i$ be a finite configuration of length $l$ defined on $\mathcal{A} = \{0, 1, \ldots, m-1\}$. Let $N(n)$ be the number of configurations of length $n$ which
contain $b$. Then

$$\lim_{n \to \infty} \frac{N(n)}{m^n} = 1.$$ 

Let $f$ be an additive local rule defined by

$$f(x_{-k}, \ldots, x_k) = \left( \sum_{j=-k}^{k} \lambda_j x_j \right) \mod m.$$ 

Let $T_f(x)$ be the dipolynomial associated to $f$ defined by

$$T_f(x) = \sum_{j=-k}^{k} \lambda_j x^{-j}.$$ 

The following lemma states a relation between $T_f(x)$ and the fraction of finite configurations of length $n$ which lie on a cycle of $F_n$.

**Lemma 3** (Martin et al. [19]). Let $p$ be a prime number. Let $f$ be any additive local rule (different from the constant local rule) defined on $\mathcal{A} = \{0, 1, \ldots, p-1\}$. Let $D_p(n)$ be the maximum $p'$ such that $p'|n$ and $A_f(x) = \gcd(x^n - 1, T_f(x))$. Let $F_n$ be the circular CA of size $n$ based on $f$. Then the fraction $\frac{\text{frac}(n)}{\text{frac}(A_f(x))}$ of configurations which lie on a cycle of $F_n$ satisfies the following equation

$$\frac{\text{frac}(n)}{\text{frac}(A_f(x))} = \frac{1}{p^{\deg(A_f(x))}D_p(n)}.$$ 

By the definition of $T_f(x)$ and since $A_f(x) = \gcd(x^n - 1, T_f(x))$, we have that if $f$ is an additive local rule with radius $k$, then

$$\deg(A_f(x)) \leq 2k.$$ 

We are now ready to prove that additive CA have dense periodic orbits. Our proof is nonconstructive, and it rather follows from counting arguments. We will take advantage of the fact that the number of configurations which lie on a cycle in circular CA of suitable increasing size is a fraction of the total number of the configurations which is bounded from below by a constant.

**Theorem 4.** Let $p$ be a prime number. Let $f$ be any additive local rule (different from the constant local rule) defined on $\mathcal{A} = \{0, 1, \ldots, p-1\}$. Then $F$ has dense periodic orbits.

**Proof.** Let us assume that $F$ does not have dense periodic orbits. This means that there exist $\delta > 0$ and a configuration $c \in \mathcal{A}^2$ such that $B(c, \delta)$ does not contain periodic configurations. In other words, there exists a forbidden block $f \text{ block}$ of length
\[2\gamma + 1, \gamma > 0,\] such that \(f\) block = \(c(-\gamma), \ldots, c(\gamma)\). For any periodic configuration \(a \in \mathcal{A}^Z\), we have
\[a(-\gamma), \ldots, a(\gamma) \neq f\) block.\]

Since CA are shift commuting maps, one can easily verify that \(f\) block cannot occur in any position of \(a\), i.e.,
\[a(-\gamma + i), \ldots, a(\gamma + i) \neq f\) block, \quad i \in Z.\]

In particular \(f\) block cannot occur in any finite configuration of length \(n\) which is periodic for \(F_n\). In fact, assume that \(f\) block occur in a configuration \(a \in \mathcal{A}^n\) periodic for \(F_n\). Then, \(f\) block would occur in \(a_m\), which is periodic for \(F\).

Let \(n\) be such that \(\gcd(n, p) = 1\). Consider the circular CA \(F_n\). Let \(N(n)\) be the number of configurations of length \(n\) defined on \(\mathcal{A}\) which contain \(f\) block. Let \(\overline{N(n)} = p^n - N(n)\) be the number of configurations of length \(n\) defined on \(\mathcal{A}\) which do not contain \(f\) block. We have that the number \(P(n)\) of configurations which lie on a cycle of \(F_n\) satisfies the following inequality
\[P(n) \leq \overline{N(n)}.\]  

By inequality (1) and Lemma 2 we have that
\[
\lim_{n \to \infty} \frac{P(n)}{p^n} \leq \lim_{n \to \infty} \frac{\overline{N(n)}}{p^n} - 1 = 1 - \lim_{n \to \infty} \frac{N(n)}{p^n} = 0. \tag{2}
\]

Since \(D_p(n) = 1\), by Lemma 3 we have that the fraction \(\frac{P(n)}{p^n}\) of configurations which lie on a cycle of \(F_n\) satisfies the following inequality
\[
\frac{P(n)}{p^n} = \frac{1}{p^{\deg(a_i(x))}} \geq \frac{1}{p^k}. \tag{3}
\]

By inequalities (2) and (3) we have a contradiction. \(\square\)

Theorems 1 and 4 imply that nontrivial additive CA defined on any finite alphabet of prime cardinality are chaotic in the sense of Devaney.

If we remove the condition on the primality of the cardinality of the alphabet then we can find additive CA which are not surjective. Note that a nonsurjective CA is not transitive and it does not have dense periodic orbits. Consider the following example. Let \(\mathcal{A} = \{0, 1, 2, 3\}\), and \(f, f : \mathcal{A}^3 \to \mathcal{A}\) be defined by \(f(x_1, x_0, x_1) = (2x_1) \mod 4\). \(f\) is a rightmost additive but not rightmost permutive map. Since \(f\) never outputs 1, \(F\) is not surjective.

4. Construction of periodic orbits for elementary CA

In Section 3 we proved that additive CA defined on an alphabet with prime cardinality have dense periodic orbits. The proof of this result is nonconstructive. Assume
now that, given a CA \((\mathcal{A}^Z, F)\), a configuration \(a \in \mathcal{A}^Z\), and a real number \(\varepsilon > 0\), we aim at constructing a configuration \(b \in \mathcal{A}^Z\) such that \(d(a, b) < \varepsilon\), and \(b\) is periodic. We now show how to construct such a configuration in the case of elementary additive CA.

A CA based on the local rule \(f, f : \mathcal{A}^{2k+1} + \mathcal{A},\) is an elementary CA (ECA) if \(k = 1\) and \(\mathcal{A} = \{0, 1\}\). A simple way for enumerating all ECA is the following. The ECA based on the local rule \(f\) is mapped onto the natural number \(n_f\), where

\[
n_f = f(0, 0, 0) \cdot 2^0 + f(0, 0, 1) \cdot 2^1 + \cdots + f(1, 1, 0) \cdot 2^6 + f(1, 1, 1) \cdot 2^7.
\]

From now on we will write “ECA \(n_f\)” instead of “ECA based on the local rule \(f\) whose enumeration number is \(n_f\).”

Each boolean additive local rule \(f\) with radius 1 has the following form.

\[
f(x_{-1}, x_0, x_1) = (ax_{-1} + bx_0 + cx_1) \mod 2,
\]

where the coefficients \(a, b, \) and \(c\) are boolean constants. In Table 1 we list all the elementary additive rules and their boolean coefficients.

We say that a configuration \(a \in \{0, 1\}^m\) contains a configuration \(b \in \{0, 1\}^n, m \geq n,\) if \(a(i) = b(i), 0 \leq i < n.\)

The problem of constructing a periodic configuration which is arbitrarily close to a given configuration \(a\) can be reduced to the following problem. Let \((\{0, 1\}^Z, F)\) be a nontrivial additive ECA and \(c \in \{0, 1\}^n\) be a finite configuration. Construct another finite configuration \(c' \in \{0, 1\}^{n'}, n' \geq n,\) such that \(c'\) contains \(c,\) and \(c'\) is periodic.

Assume that for any given configuration \(c\) of length \(n,\) we are able to construct a periodic configuration \(c'\) of length \(n', n' \geq n,\) which contains \(c.\) Then, \(c'_\infty\) is a periodic configuration for \(F\) which contains \(c\) infinitely many times. Since CA are shift commuting map and since \(c\) is an arbitrary configuration of finite length, we are able, modulo a suitable shift operation, to construct a sequence of periodic configurations for \(F\) whose limit is the target configuration \(a.\)

4.1. Rules 150, 170, 240

We recall the following simple result (see for example [19]).

<table>
<thead>
<tr>
<th>Rule</th>
<th>Coefficients (a, b, c)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0,0,0</td>
</tr>
<tr>
<td>204</td>
<td>0,1,0</td>
</tr>
<tr>
<td>170</td>
<td>0,0,1</td>
</tr>
<tr>
<td>240</td>
<td>1,0,0</td>
</tr>
<tr>
<td>60</td>
<td>1,1,0</td>
</tr>
<tr>
<td>102</td>
<td>0,1,1</td>
</tr>
<tr>
<td>90</td>
<td>1,0,1</td>
</tr>
<tr>
<td>150</td>
<td>1,1,1</td>
</tr>
</tbody>
</table>
Let \( f \) be an additive local rule defined by \( f(x_{-1}, x_0, x_1) = (ax_{-1} + bx_0 + cx_1) \mod 2. \)

Consider the \( n \times n \) transition matrix

\[
M_n = \begin{pmatrix}
    b & c & a \\
    a & . & . \\
    . & . & . \\
    . & . & . \\
    c & a & b \\
\end{pmatrix}
\]

If \( \text{Det}(M_n) \neq 0 \), then each configuration \( c \in \{0,1\}^n \) is a periodic configuration of \( F_n \).

In fact, since \( F[c] = M_n \cdot c \), then for each configuration \( b \) there exists a configuration \( c \) such that \( F_n[c] = b \). As a consequence, any configuration \( c \in \{0,1\}^n \) is on a cycle.

One can easily verify that the transition matrices of ECA 240 and 170 (shifts) are permutation matrices and thus they are nonsingular for any value of \( n \). We conclude that any configuration of finite length stays on a cycle.

The transition matrix of ECA 150 has a more complicated structure than the transition matrices of ECA 240 and 170. We now show that there are arbitrarily large values of \( n \), for which the transition matrix of rule 150 is nonsingular.

**Theorem 5.** The matrix of ECA 150 is nonsingular if and only if \( n \) is not a multiple of 3.

**Proof.** The matrix of ECA 150 has the following form.

\[
M_n = \begin{pmatrix}
    1 & 1 & 1 & 1 \\
    1 & . & . & . \\
    . & . & . & . \\
    . & . & . & . \\
    1 & . & . & . \\
\end{pmatrix}
\]

Let \( T_n \) be the \( n \times n \) tridiagonal matrix with entries:

\[
t_{ij} = \begin{cases} 
    1 & \text{if } |i-j| \leq 1, \\
    0 & \text{otherwise}.
\end{cases}
\]

Over the field \( GF(2) \), we have that

\[
\text{Det}(M_n) = \text{Det}(T_{n-1}), \quad \text{and} \quad \text{Det}(T_n) = \text{Det}(T_{n-3}).
\]

Since \( \text{Det}(T_1) = \text{Det}(T_3) = 1 \) and \( \text{Det}(T_2) = 0 \), then the thesis follows. \( \square \)

**4.2. Rules 60, 90, 102**

The technique we used to construct periodic orbits for rules 240, 170, and 150 cannot be used for rules 90, 60, and 102. In fact, the transition matrices of these rules are
always singular. In the next two theorems we show how to construct a set of dense periodic orbits for rules 90, 60, and 102 by using an ad hoc technique.

We proceed as follows. We first construct a particular sequence \( \{e_n\}_{n \in I} \) (\( I \subseteq \mathbb{N} \)) of periodic configurations of length \( n \) such that each \( e_n \) contains an isolated 1, i.e., a 1 surrounded by a number of 0's increasing with \( n \). Then we use this particular sequence of configurations as a basis to construct periodic configurations of finite length which contain any given configuration of finite size.

Formally, let \( F \) be an additive ECA and \( I \) be an infinite subset of \( \mathbb{N} \). Let \( g, g: I \to \mathbb{N} \), be an increasing integer function such that \( g(n) < |n/2| \). Let \( \{e_n\}_{n \in I} \) be a sequence of configurations of length \( n \) which satisfies the following two properties.

(i) For any \( n \in I \), there exists an integer \( p, 0 \leq p < n \), such that \( e_n(p) = 1 \) and \( e_n((p + i) \mod n) = e_n((p - i) \mod n) = 0 \), \( i \neq 0 \), \( |i| \leq g(n) \).

(ii) For any \( n \in I \), \( e_n \) lies on a cycle of \( F_n \).

Let \( \sigma_i, j \in \mathbb{Z} \), be the shift CA defined by \( \sigma^i[a](i) = a(i - j), i \in \mathbb{Z} \). Let \( c \) be any given configuration of length \( h \) and \( n \in I \) be such that \( g(n) > h \). Then, starting from \( e_n \), one can construct a periodic configuration \( c' \) which contains \( c \) as follows.

\[
c' = \left( \sum_{i=1}^{h} c(i) \cdot \sigma^i_n[e_n] \right) \mod 2,\]

where

\[
c(j) \cdot \sigma^i_n[e_n] = \begin{cases} 
\sigma^i_n[e_n] & \text{if } c(j) = 1, \\
\text{null configuration} & \text{otherwise}.
\end{cases}
\]

Let \( l \) be the period length of \( e_n \). One can easily verify that each configuration \( c(j) \cdot \sigma^i_n[e_n] \) is periodic with period length \( l \). Since \( F \) is additive, we have that \( c' \) is periodic with period \( l \). Moreover, \( c' \) contains \( c \) starting from the position \( p + 1 \).

In the following two theorems we show how to construct a sequence of configurations which satisfies properties (i) and (ii) for rule 60 and 90, respectively.

**Theorem 6.** Let \( n = 3 \cdot 2^j, j \geq 0 \). Let \( f \) be the local rule 90. Let \( e_n \) be the following finite configuration of length \( n \).

\[
e_n(i) = \begin{cases} 
1 & \text{if } i = 2^j - 1 \text{ or } i = 2^{j+1} - 1, \\
0 & \text{otherwise}.
\end{cases}
\]

Then \( e_n \) is periodic of period \( 2^j \) for \( F_n \).

**Proof.** Let \( e'_n \) and \( e''_n \) be two finite configurations of length \( n \) defined as follows.

\[
e'_n(i) = \begin{cases} 
1 & \text{if } i = 2^j - 1, \\
0 & \text{otherwise},
\end{cases}
\]

and

\[
e''_n(i) = \begin{cases} 
1 & \text{if } i = 2^{j+1} - 1, \\
0 & \text{otherwise}.
\end{cases}
\]
It is easy to verify that \( e_n = (e'_n + e''_n) \mod 2 \). Since rule 90 is additive, the configuration we reach starting from \( e_n \) is the sum modulo 2 of the two configurations we reach starting from \( e'_n \) and \( e''_n \), i.e., \( F_n[(e'_n + e''_n) \mod 2] = (F_n[e'_n] + F_n[e''_n]) \mod 2 \). \( F_n \) can be written as follows

\[
F_n[e_n] = (\sigma_n^{-1} + \sigma_n^0)[e_n] \mod 2.
\]

Since \( \sigma_n^i[\sigma_n^j[e_n]] = \sigma_n^{i+j}[e_n] \) and

\[
\begin{pmatrix} 2^j \\ j \end{pmatrix} \mod 2 = \begin{cases} 0 & \text{if } 0 < i < 2^j, \\ 1 & \text{if } i = 0 \text{ or } i = 2^j, \end{cases}
\]

we have that

\[
F_n^{2^j}[e_n] = (\sigma_n^{-1} + \sigma_n^{2^j})[e_n] \mod 2 = \left( \sum_{h=0}^{2^j} \binom{2^j}{h} \sigma_n^{-h}[\sigma_n^{2^j-h}[e_n]] \right) \mod 2 = (\sigma_n^{-2^j} + \sigma_n^{2^j})[e_n] \mod 2.
\]

Thus,

\[
F_n^{2^j}(e'_n) = \begin{cases} 1 & \text{if } i = 2^j + 1 - 1 \text{ or } i = 3 \cdot 2^j - 1, \\ 0 & \text{otherwise,} \end{cases}
\]

and

\[
F_n^{2^j}(e''_n) = \begin{cases} 1 & \text{if } i = 2^j - 1 \text{ or } i = 3 \cdot 2^j - 1, \\ 0 & \text{otherwise.} \end{cases}
\]

Summarizing, we have

\[
F_n^{2^j}[e_n] = F_n^{2^j}[(e'_n + e''_n) \mod 2] = (F_n[e'_n] + F_n[e''_n]) \mod 2 = e_n.
\]

\[\square\]

**Theorem 7.** Let \( n = 2^j - 1 \), \( j > 0 \). Let \( f \) be the local rule 60. Let \( e_n \) be the following finite configuration of length \( n \).

\[
e_n(i) = \begin{cases} 1 & \text{if } i = 0 \text{ or } i = 2^j - 1, \\ 0 & \text{otherwise.} \end{cases}
\]

Then \( e_n \) is periodic of period \( 2^j - 1 \) for \( F_n \).

**Proof.** Since rule 60 is additive, the configuration we reach starting from \( e_n \) is the sum modulo 2 of the two configurations we reach from

\[
e'_n(i) = \begin{cases} 1 & \text{if } i = 0, \\ 0 & \text{otherwise}, \end{cases} \quad \text{and} \quad e''_n(i) = \begin{cases} 1 & \text{if } i = 2^j - 1, \\ 0 & \text{otherwise.} \end{cases}
\]

\( F_n \) can be written as follows

\[
F_n[e_n] = (\sigma_n^{-1} + \sigma_n^0)[e_n] \mod 2.
\]
Since $\sigma_n^i[\sigma_n^j[e_n]] = \sigma_n^{i+j}[e_n]$ and
\[
\binom{2^j - 1}{i} \mod 2 = 1, \quad 0 \leq i \leq 2^j - 1,
\]
we have that
\[
F_n^{2^j-1}[e_n] = \left(\sum_{h=0}^{2^j-1} \sigma_n^{-h}\right)[e_n] \mod 2.
\]
Let $\bar{a}$ be the configuration defined by $\bar{a}(i) = 1 - a(i), \quad i \in Z$. One can easily verify that
\[
F_n^{2^j-1}(e_n') = \bar{e}_n', \quad \text{and} \quad F_n^{2^j-1}(e_n'') = \bar{e}_n'',
\]
where $(\bar{e}_n' + \bar{e}_n'') \mod 2 = e_n$. \hfill \Box

Let $f$ and $g$ denote local rules 60 and 102, respectively. Since $f(x_{-1},x_0,x_1) = g(x_1,x_0,x_{-1})$, one can easily verify that ECA 102 enjoys the same topological properties of ECA 60.

Note that the technique we used to construct a set of dense periodic orbits in the case of additive ECA can be easily extended to the case of general additive CA.

5. Conclusions and further work

We proved that additive one-dimensional CA defined on a finite alphabet of prime cardinality are chaotic according to Devaney's definition of chaos. This definition, which is based on topological notions, is imported from the theory of discrete dynamical systems. This is the first step towards a complete formal classification of CA. Further work includes the extension of the results presented in this paper to CA defined on alphabets of composite cardinality, to nonadditive CA, and to multidimensional CA.

Acknowledgements

We wish to thank Bruno Codenotti and Giovanni Manzini for many interesting discussions and helpful suggestions.

References


