Discrete Comput Geom 1:277-288 (1986)

Discrete & Computational Geometry

Periodic Orbits for Additive Cellular Automata

Raul Cordovil*, Rui Dilão, and Ana Noronha da Costa

C.F.M.C., Av. Prof. Gama Pinto, 2, 1699 Lisboa Codex, Portugal

Abstract. We formulate and study a necessary and sufficient condition for a configuration of any type of infinite additive cellular automata to have periodic behavior in time. The number of orbits with period n is counted. Relations between spatial and temporal periods are discussed.

1. Introduction

Cellular automata (CA) are structures evolving on a (finite or infinite) lattice according to a definite deterministic local law. Each site on the lattice takes a value of some finite set, typically 0 or 1, and time evolution at each site is determined by the previous values at neighboring sites.

Cellular automata were first introduced by Von Neumann [8] and Ulam [6] as examples of simple structures presenting some of the features of life. Recently, they have been reintroduced by Wolfram in a series of remarkable papers [9]-[11], and inexpensive hardware has been implemented for the fast computation of any CA (Toffoli's CAM machine [5]). This has generated an increasing interest in the formulation of a large class of physical problems in terms of CA evolutionary laws (see De Pazzis *et al.* [1] and *Phys. D* **10** (1984), nos. 1 and 2, in particular Vichiniac [7]).

Some CA have a simplifying additivity property, i.e., they satisfy a superposition principle: given two configurations, the time evolution of their sum is given simply by the sum of their individual evolved configurations. A class of finite additive CA has been thoroughly investigated in a recent paper by Martin *et al.* [3]. In this paper we give necessary and sufficient conditions for a configuration to be periodic in time for any type of infinite additive CA. We further prove that configurations with temporal period n are generated by a linear map and have

* Supported in part by G.M.C.I., DEEE-LNETI (Portugal).

necessarily a spatial period $\alpha(n)$. Relations between temporal and spatial periods are also investigated.

2. Periodic Orbits

Let $\mathbb{Z}_2$ be the finite field with two elements $\{0, 1\}$. We denote by $\mathbb{Z}_2^{\mathbb{Z}}$ the vector space whose elements are the functions of the set $\mathbb{Z}$ of the integers in the field $\mathbb{Z}_2$: i.e., $x \in \mathbb{Z}_2^{\mathbb{Z}}$ if and only if $x = \{x_i\}_{i \in \mathbb{Z}}$ is a doubly infinite sequence of elements $x_i \in \mathbb{Z}_2$. Let $\sigma : \mathbb{Z}_2^{\mathbb{Z}} \leftrightarrows$ be the automorphism of $\mathbb{Z}_2^{\mathbb{Z}}$ such that, for every $x \in \mathbb{Z}_2^{\mathbb{Z}}$, $(\sigma x)_i = x_{i+1}$; thus σ shifts the entries one unit to the left. For every integer m let σ^m be the automorphism of $\mathbb{Z}_2^{\mathbb{Z}}$ defined by $(\sigma^m x)_i = x_{i+m}$. We denote by $\mathbb{V}$ the vector space over $\mathbb{Z}_2$ of the linear functions finitely generated by the automorphisms $\{\sigma^m\}_{m \in \mathbb{Z}}$:

$$\text{i.e.,} \quad \tau \in \mathbb{V} - \{0\} \quad \text{iff} \quad \tau = \sum_{i=m'}^{m''} \lambda_i \sigma^i, \qquad m' \leq m'', \quad \lambda_i \in \mathbb{Z}_2, \quad \lambda_{m'} = \lambda_{m''} = 1.$$

We may also view $\mathbb{V}$ as a $\mathbb{Z}_2$-algebra where the product of two linear functions τ, $\tau' \in \mathbb{V}$ is this composite:

$$\text{if} \quad \tau = \sum_i \lambda_i \sigma^i, \qquad \tau' = \sum_j \lambda'_j \sigma^j \quad \text{then} \quad \tau \cdot \tau' = \tau' \cdot \tau = \sum_{i,j} \lambda_i \lambda'_j \sigma^{i+j}.$$

For every $\tau \in \mathbb{V} - \{0\}$ we call the ordered pair $\mathcal{A} = (\mathbb{Z}_2^{\mathbb{Z}}, \tau)$ the *one-dimensional infinite CA over $\mathbb{Z}_2$ with additive time evolution rule τ*. In this paper we shall only consider this type of CA. For this reason, in the following, we call $\mathcal{A}$ simply a CA. If $x \in \mathbb{Z}_2^{\mathbb{Z}}$, we call x a *configuration* (of the CA, $\mathcal{A}$).

Example 2.1. We remark that in a CA, all entries x_i of a given configuration evolve in time according to a local law. This law can be given by specifying the outcome of an entry according to all possible values in a certain fixed neighborhood. One simple law, involving just nearest neighbors can be listed as follows:

time t:	111	110	101	100	011	010	001	000
time $t+1$:	0	1	0	1	1	0	1	0 .

It can easily be checked that the time evolution of an entry x_i is given by addition modulo 2 of the values at neighboring sites, i.e., $(\tau x)_i = x_{i-1} + x_{i+1} \pmod 2$ and so $\tau = \sigma^{-1} + \sigma$. This CA is usually referred to as *rule* 90 [9].

According to another well-known CA, the time evolution of each entry x_i is given by $(\tau x)_i = x_{i-1} + x_i + x_{i+1} \pmod 2$ and so $\tau = \sigma^{-1} + \mathbb{1} + \sigma$ (*rule* 150 [9]).

Definition 2.2. Let $\mathcal{A} = (\mathbb{Z}_2^{\mathbb{Z}}, \tau)$ be a CA and let $n \geq 1$ be a natural number. We say that a *configuration x of $\mathcal{A}$ has temporal period n if and only if $\tau^n x = x$*. In this case we say also that x is a *periodic orbit of $\mathcal{A}$*. By definition the *spatial period $\alpha(x)$ of the configuration x is the smallest positive natural number p such that $x_{i+p} = x_i$ for every $i \in \mathbb{Z}$*. In case it does not exist, we say that $\alpha(x) = \infty$. *We denote by $\alpha(n)$ the largest $\alpha(x)$ from all the configurations x of $\mathcal{A}$ with temporal period n.*

Given the evolution rule $\tau = \sum_{i=m'}^{m''} \lambda_i \sigma^i$, with $m' \leq m''$ and $\lambda_{m'} = \lambda_{m''} = 1$, define $s(\tau) = m'' - m'$. *In this paper, we associate with each rule τ a natural number $\gamma(\tau)$, such that $\gamma(\tau) = s(\tau + \mathbb{1})$ if $\tau \neq \mathbb{1}$ and $\gamma(\mathbb{1}) = 0$, measuring its breadth.* The meaning of $\gamma(\tau)$ will be made clear in Theorem 2.3. Note that $\gamma(\tau) = 0$ iff $\tau = \mathbb{1} + \sigma^m$ $(m \in \mathbb{Z} - \{0\})$ or $\tau = \mathbb{1}$.

Theorem 2.3. *Let $\mathcal{A}$ be a CA with the time evolution rule $\tau = \sum_{i=m'}^{m''} \lambda_i \sigma^i$ and let $n \geq 1$ be a natural number. Then $x = \{x_i\}_{i \in \mathbb{Z}}$ is a configuration of $\mathcal{A}$ with temporal period n iff*

$$x_j = \sum_{i=nm'}^{nm''} \lambda_i^{(n)} x_{j+i} \qquad (j \in \mathbb{Z}), \tag{2.3.1}$$

where the scalars $\lambda_i^{(n)} \in \mathbb{Z}_2$ are determined by the equality $\tau^n = \sum_{i=nm'}^{nm''} \lambda_i^{(n)} \sigma^i$. On the other hand if $\gamma(\tau^n) \geq 1$ then the configuration x is uniquely determined if, for some $i_0 \in \mathbb{Z}$, we know the entries $x_{i_0}, x_{i_0+1}, \ldots, x_{i_0+\gamma(\tau^n)-1}$. Moreover, if $\tau \neq \mathbb{1}$, x has a spatial period $\alpha(x) < 2^{\gamma(\tau^n)}$.

Proof. Equality (2.3.1) is obvious. The second and third statements are proved below (see Remark 2.9). □

We remark that if x is a configuration with temporal period n for the CA $\mathcal{A} = (\mathbb{Z}_2^{\mathbb{Z}}, \tau)$, then x is the preimage of the zero configuration for the CA $\mathcal{A}'$ with the evolution rule $\tau' = \tau^n + \mathbb{1}$. In particular, as $(\tau^{2^n} + \mathbb{1}) = (\tau + \mathbb{1})^{2^n}$, if x has temporal period 2^n for the CA $\mathcal{A}$, then x is a preimage of the zero configuration of the CA with the evolution rule $\tau' = \tau + \mathbb{1}$ (see Examples 2.7 and 2.8 below).

The proposition below is simple but useful.

Proposition 2.4. *Let x be an initial configuration with spatial period n of the CA $\mathcal{A}$. Let τ be the time evolution rule of $\mathcal{A}$. Then $\tau(x)$ has spatial period d where d divides n, and either x is a periodic orbit of $\mathcal{A}$ or x is the preimage of a periodic orbit of $\mathcal{A}$.* □

We remark that Proposition 2.4 has the consequence that a configuration x of a CA, with only a finite number of entries equal to 1, is neither a periodic orbit nor a preimage of a periodic orbit if $\tau \neq \mathbb{1}$.

Let μ be the *Möbius function* of the partially ordered set $P = (\mathbb{N} - \{0\}, \leq)$ of the natural numbers which are different from zero, with the relation that $p \leq q$ iff p divides q (see [4]). More precisely, the Möbius function μ is defined as follows: for all $p, q \in \mathbb{N} - \{0\}$, $\mu(p, p) = 1$, $\mu(p, q) = 0$ if p does not divide q or q/p is divisible by the square of a prime, and $\mu(p, q) = (-1)^r$ if q/p is the product of r distinct primes.

Theorem 2.5. *Let $\mathcal{A} = (\mathbb{Z}_2^{\mathbb{Z}}, \tau)$ be a CA. Let $t(n)$ [resp. $t^*(n)$] be the number of configurations such that its temporal period [resp. smallest temporal period] is n.*

Then we have:

$$t(n) = 2^{\gamma(\tau^n)} \quad \text{if} \quad \tau \neq \mathbb{1} \quad \text{and} \quad t(n) = \infty \quad \text{if} \quad \tau = \mathbb{1}; \tag{2.5.1}$$

$$t^*(n) = \sum_{d=1}^{n} \mu(d, n) \cdot t(d). \tag{2.5.2}$$

Moreover, $\gamma(\tau^n)$ *has the following properties*:

$$\text{If} \quad \gamma(\tau) \geq 1 \quad \text{then} \quad \gamma(\tau^n) \geq 1. \tag{2.5.3}$$

$$\gamma(\tau^n) = n\gamma(\tau), \tag{2.5.4}$$

except in the case $\tau = \mathbb{1} + \sigma^{m_1} + \cdots + \sigma^{m_2}$ *with* $m_2 \geq m_1 > 0$ *or* $m_2 \leq m_1 < 0$. *In this case, we have*

$$\gamma(\tau^n) = n|m_2| - 2^{n'}|m_1|, \tag{2.5.5}$$

where n' *is the largest natural number such that* $2^{n'}$ *divides* n; *in particular if* $m_1 = m_2 = m'$

$$\gamma((\mathbb{1} + \sigma^{m'})^n) = |m'|(n - 2^{n'}).$$

Proof. We prove only the nontrivial cases of the second statement. Suppose $\tau = \mathbb{1} + \sigma^{m_1} + \cdots + \sigma^{m_2}$, with $m_2 \geq m_1 > 0$. Then $\tau^n = \mathbb{1} + \sum_{i=\nu}^{n} \binom{n}{i} (\sigma^{m_1} + \cdots + \sigma^{m_2})^i$ where ν is the least integer for which $\binom{n}{\nu} \neq 0 \pmod 2$. It is easy to see that for all natural numbers k, n, $2k \leq n$, if $n = 2^p + q$ with $0 \leq q < 2^p$, then $\binom{n}{k} = \binom{q}{k} \pmod 2$. But this implies $\nu = 2^{n'}$, where n' is the largest natural number such that $2^{n'}$ divides n, and $\gamma(\tau^n) = nm_2 - 2^{n'}m_1$. The case $m_2 \leq m_1 < 0$ is similar, and equation (2.5.5) follows. In particular, it is clear that if $m_1 = m_2 = m'$,

$$\gamma(\tau) = 0 \quad \text{and} \quad \gamma(\tau^n) = |m'|(n - 2^{n'}). \qquad \square$$

Remark 2.6. The reader may easily realize, in view of the above theorem, that some CA have a rather pathological behavior. More precisely, if $\tau = \mathbb{1} + \sigma^m$ ($m \in \mathbb{Z} - \{0\}$) for $n = 2^p$ ($p \in \mathbb{N}$), we have $\tau^n = \mathbb{1} + \sigma^{nm}$ and therefore $\gamma(\tau^n) = 0$. But then we have $t(2^n) = 1$, and consequently $\mathcal{A} = (\mathbb{Z}_2^{\mathbb{Z}}, \mathbb{1} + \sigma^m)$ is a dynamical system with no periodic orbits with period 2^n for every natural number $n \geq 1$ (see Table 1).

Table 1. Number of periodic points for the cellular automaton $\tau = \mathbb{1} + \sigma$ (Theorem 2.5).

	Number of periodic points of period n	Number of periodic points of smallest period n
1	1	1
2	1	0
3	4	3
4	1	0
5	16	15
6	16	12
7	64	63
8	1	0

Example 2.7. We now calculate explicitly some periodic configurations for rule 90, $\tau = \sigma^{-1} + \sigma$ (see Example 2.1). For every natural number $n \geq 1$, the time n evolution map, τ^n, is given by $(\sigma^{-1} + \sigma)^n = \sum_{i=0}^{n} \binom{n}{i} \sigma^{n-2i}$. Equation (2.3.1), giving the necessary and sufficient condition for a configuration x to have temporal period n, then becomes

$$x_j = \sum_{i=0}^{n} \binom{n}{i} x_{j+n-2i} \qquad (j \in \mathbb{Z}). \tag{2.7.1}$$

This is a recurrence relation of order $2n$ and, as asserted in Theorem 2.3, entry x_{n+j} is uniquely determined given entries $x_{j-n}, x_{j-n+1}, \ldots, x_{j+n-1}$. For example, for temporal period 3, $x_{j+3} = x_{j-3} + x_{j-1} + x_j + x_{j+1}$ $(j \in \mathbb{Z})$, which can be written in terms of the companion matrix,

$$(x_{j+1}, x_{j+2}, \ldots, x_{j+6}) = (x_j, x_{j+1}, \ldots, x_{j+5}) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.7.2}$$

Introducing as the "initial condition" the vector (000001) we successively obtain 15 different vectors. This means that the configuration having temporal period 3 generated by this "initial condition" is also periodic in space with period 15 (see Fig. 1(a)). Nevertheless, if we introduce into (2.7.2) the vector (000110), only five different vectors are generated and this configuration with temporal period 3 will only have spatial period 5 (see Fig. 1(b)). Notice that any configuration with temporal period 1 has, in particular, temporal period 3 and so satisfies equation (2.7.1). Introducing as initial conditions $x_0 = 1$, $x_1 = 1$, $x_2 = 0$, $x_3 = 1$, $x_4 = 1$, $x_5 = 0$, equation (2.7.1) generates the infinite configuration $\{\ldots 110110110 \ldots\}$, which can easily be seen to have temporal period 1. A spatial period associated with some temporal period is generally difficult to calculate explicitly. However, in the particular case $n = 2^m$ $(m \in \mathbb{N})$, equation (2.7.1) immediately yields spatial period $3n$: $x_{j+3n} = x_j$ $(j \in \mathbb{Z})$.

Example 2.8. For rule 150, $\tau = \sigma^{-1} + \mathbb{1} + \sigma$ (see Example 2.1), the time n evolution map, τ^n, is given by

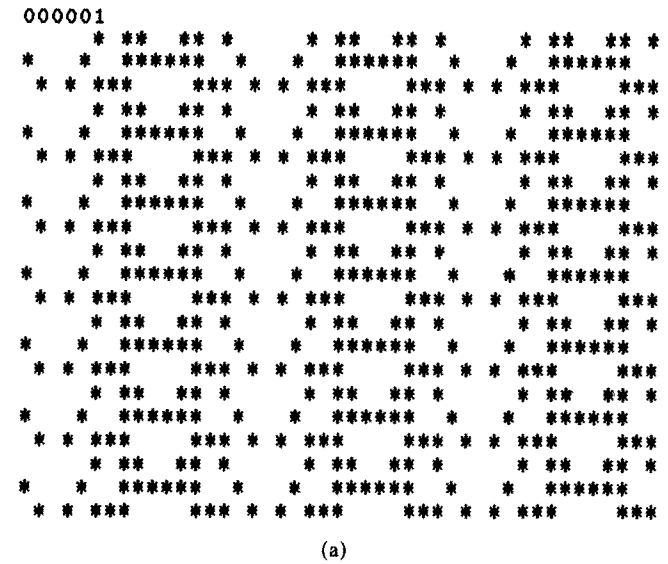
$$(\sigma^{-1} + \mathbb{1} + \sigma)^n = \sum_{i=-n}^{n} K_{i+n}^n \sigma^i, \qquad \text{where} \quad K_{i+n}^n = \sum_{j=0}^{n} \binom{n}{i+j} \binom{i+j}{n-j}.$$

Coefficients K_j^n, $0 \leq j \leq 2n$, are easily shown to verify the following properties:

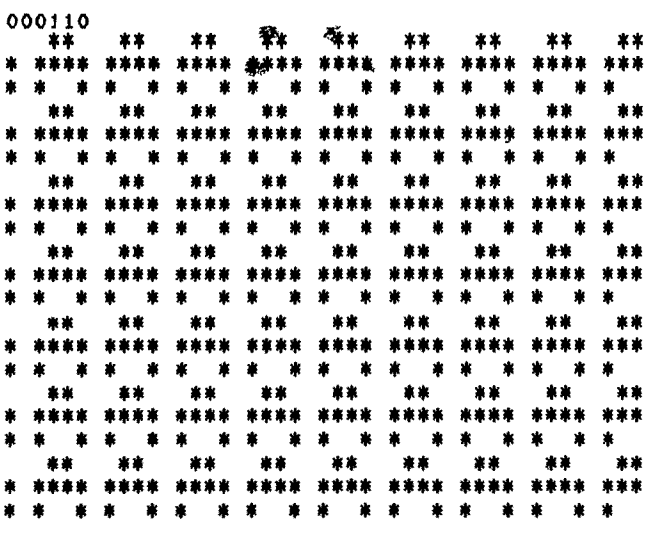
$$K_0^n = K_{2n}^n = 1, \tag{2.8.1}$$

$$K_j^n = K_{2n-j}^n, \tag{2.8.1'}$$

$$K_j^n = K_j^{n-1} + K_{j-1}^{n-1} + K_{j-2}^{n-1}. \tag{2.8.1''}$$



(a)



(b)

Fig. 1. Time evolution of two configurations of the cellular automaton $\tau = \sigma^{-1} + \sigma$ corresponding to temporal period 3: (a) configuration generated by the vector 000001, with maximal spatial period $\alpha(3) = 15$; (b) configuration generated by the vector 000110, with spatial period 5.

Equation (2.3.1) becomes,

$$x_j = \sum_{i=-n}^{n} K_{i+n}^{n} x_{j+i} \qquad (j \in \mathbb{Z}), \tag{2.8.2}$$

where the coefficients K_{i+n}^{n} are easily calculable from properties (2.8.1). Relation (2.8.2) has basically the same features as equation (2.7.1) for rule 90, generating a finite number of different vectors for each temporal period n. Notice again that spatial periods corresponding to temporal periods $n = 2^m$ ($m \in \mathbb{N}$) can be directly calculated from (2.8.1) and (2.8.2): $x_{j+2n} = x_j$ ($j \in \mathbb{Z}$).

Remark 2.9. Let $\mathscr{A}$ be a CA with the time evolution rule $\tau = \sum_{i=m'}^{m''} \lambda_i \sigma^i$ such that $\gamma(\tau) \geq 1$. Let x be a configuration of $\mathscr{A}$ with temporal period n. Then, by Theorem 2.5, $\gamma(\tau^n) \geq 1$ and it results from equality (2.3.1) that its entries are uniquely determined given the $\gamma(\tau^n)$ entries $\{x_0, x_1, \ldots, x_{\gamma(\tau^n)-1}\}$. In fact, let $\mathbf{x}'$ be the vector of $\mathbb{Z}_2^{\gamma(\tau^n)}$ such that, for every $0 \leq i \leq \gamma(\tau^n) - 1$, $(x')_i = x_i$. Then there exists a linear application $L: \mathbb{Z}_2^{\gamma(\tau^n)} \leftrightarrows$ such that for every $m \in \mathbb{Z}$ and for every $0 \leq i \leq \gamma(\tau^n) - 1$, we have, in the canonical basis of $\mathbb{Z}_2^{\gamma(\tau^n)}$, $(L^m x')_i = x_i$. With respect to this basis, it is clear that the matrix A of the linear application L is of the following type:

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 & a_{\gamma(\tau^n)-1} \end{pmatrix},$$

where the a_i, $0 \leq i \leq \gamma(\tau^n) - 1$, are determined by equality (2.3.1). More precisely, in the particular case of a time evolution rule τ with $m' < 0 < m''$, we have

$$\begin{cases} a_i = \lambda_{nm'+i}^{(n)} & (0 \leq i \leq n(m'' - m') - 1,\ i \neq -nm'), \\ a_{-nm'} = \lambda_0^{(n)} + 1, \end{cases}$$

where the scalars $\lambda_i^{(n)} \in \mathbb{Z}_2$ are determined by the equality $\tau^n = \sum_{i=nm'}^{nm''} \lambda_i^{(n)} \sigma^i$. We remark that $a_0 = \lambda_{nm'}^{(n)} = \lambda_{m'} = 1$. More generally, it is seen that we always have $\det(A) = a_0 = 1$. *Hence any period n configuration x of $\mathscr{A}$ can be written in the form*

$$\{\ldots, x'A^{-2\gamma(\tau^n)}, x'A^{-\gamma(\tau^n)}, x', x'A^{\gamma(\tau^n)}, x'A^{2\gamma(\tau^n)}, \ldots\}.$$

Conversely, if x can be written in this form then it is clear that x is a configuration with temporal period n.

Note also that, as A determines an automorphism of $\mathbb{Z}_2^{\gamma(\tau^n)}$, $\alpha(x) < 2^{\gamma(\tau^n)}$.

The linear application $L: \mathbb{Z}_2^{\gamma(\tau^n)} \leftrightarrows$ and the matrix A constructed above are independent of the particular configuration with temporal period n of $\mathscr{A}$ that we have selected. *We say that A [resp. L] is the companion matrix [resp. linear application] of the configurations of $\mathscr{A}$ with temporal period n.*

Theorem 2.10. *Let $\mathcal{A} = (\mathbb{Z}_2^{\mathbb{Z}}, \tau)$ be a CA, and let n be a positive natural number. Suppose $\gamma(\tau^n) \geq 1$ and let A be the companion matrix of the configurations with temporal period n. Then $\alpha(n)$ is the smallest positive natural number such that $A^{\alpha(n)} = I$. In particular, for every configuration x with temporal period n, $\alpha(x)$ divides $\alpha(n)$.*

Corollary 2.11. *Let $\mathcal{A}$ be a CA, and let d and n be two positive natural numbers. Then if d divides n, $\alpha(d)$ also divides $\alpha(n)$. In particular, $\alpha(1)$ divides $\alpha(n)$.*

On the other hand, if $n = 2^r d$ and $\gamma(\tau) \geq 1$ [resp. $\tau = \mathbb{1} + \sigma^m$ $(m \in \mathbb{Z} - \{0\})$] then $\alpha(n) = 2^r \alpha(d)$ [resp. $\alpha(n) = 2^r \alpha(d)$ if $n \neq 2^p$ and $\alpha(2^p) = 1$].

The bulk of the proof of Theorem 2.10 rests in the following more technical result.

Lemma 2.12. *In the conditions of Theorem 2.10 let x' be a vector of $\mathbb{Z}_2^{\gamma(\tau^n)}$ such that $\{x', x'A, x'A^2, \ldots, x'A^{\gamma(\tau^n)-1}\}$ is a basis of $\mathbb{Z}_2^{\gamma(\tau^n)}$. Let $x = \{\ldots, x'A^{-\gamma(\tau^n)}, x', x'A^{\gamma(\tau^n)}, \ldots\}$. Then $\alpha(x) = \alpha(n)$ and $\alpha(n)$ is the smallest positive natural number such that $A^{\alpha(n)} = I$.*

Proof of Lemma 2.12. Let x' be a vector of $\mathbb{Z}_2^{(\tau^n)}$ such that $\{x', x'A, \ldots, x'A^{\gamma(\tau^n)-1}\}$ is a basis of $\mathbb{Z}_2^{\gamma(\tau^n)}$. Let y be a configuration with temporal period n of $\mathcal{A}$. From Remark 2.9, we know there is a vector $y' \in \mathbb{Z}_2^{\gamma(\tau^n)}$ such that $y = \{\ldots, y'A^{-\gamma(\tau^n)}, y', y'A^{\gamma(\tau^n)}, \ldots\}$. Then there are scalars $\xi_i \in \mathbb{Z}_2$, such that $y' = \sum \xi_i x'A^i$, $0 \leq i \leq \gamma(\tau^n) - 1$, implying that $\alpha(y)$ divides $\alpha(x)$ and necessarily $\alpha(x) = \alpha(n)$. Finally, if $A^\delta = I$ then $z'A^\delta = z'$ for every $z' \in \mathbb{Z}_2^{\gamma(\tau^n)}$, and the lemma follows. □

Proof of Theorem 2.10. Let x' be the vector of $\mathbb{Z}_2^{\gamma(\tau^n)}$ such that, in the canonical basis of $\mathbb{Z}_2^{\gamma(\tau^n)}$, $x_i = 0$ if $0 \leq i \leq \gamma(\tau^n) - 2$ and $x_{\gamma(\tau^n)-1} = 1$. Then $\{x', x'A, \ldots, x'A^{\gamma(\tau^n)-1}\}$ is a basis of $\mathbb{Z}_2^{\gamma(\tau^n)}$ and Theorem 2.10 follows from Lemma 2.12. □

Proof of Corollary 2.11. We prove the first statement. If $\tau = \mathbb{1}$, then $\alpha(n) = \infty$, $n \geq 1$. Suppose $\tau \neq \mathbb{1}$. If $\tau = \mathbb{1} + \sigma^m$ $(m \in \mathbb{Z} - \{0\})$ and $n = 2^p$ we have, by Theorem 2.5, $\alpha(d) = \alpha(n) = 1$. Suppose now $\gamma(\tau^n) \geq 1$. Then, by Theorem 2.5, $\gamma(\tau^d) \geq 1$ and from the proof of Theorem 2.10 there is a configuration x, with temporal period d, such that $\alpha(x) = \alpha(d)$. But x also has temporal period n, because d divides n. Then, from Theorem 2.10, $\alpha(d)$ divides $\alpha(n)$.

To prove the second statement of the corollary we need the following lemma. (We recall that $P_A(X)$, the *minimal polynomial* of a $n \times n$ matrix A over the field K, is the monic polynomial of least degree in $K[X]$ such that $P_A(A) = 0$.)

Lemma 2.13. *Let $\mathcal{A}$ be a CA with $\tau \neq \mathbb{1}$ and let n be a natural number such that $\gamma(\tau^n) \geq 1$. Let A_n [resp. A_{2n}] be the companion matrix of the configurations with temporal period n [resp. $2n$] of $\mathcal{A}$. Let $P_{A_n}(X)$ [resp. $P_{A_{2n}}(X)$] be the minimal polynomial of A_n [resp. A_{2n}]. Then $P_{A_n}(X) = (P_{A_{2n}}(X))^2$.*

Proof. Let $(a_0, a_1, \ldots, a_{\gamma(\tau^n)-1})^T$ [resp. $(b_0, b_1, \ldots, b_{\gamma(\tau^n)-1})^T$] be the last column of the matrix A_n [resp. A_{2n}]. If $\tau^n = \sum_{i=nm'}^{nm''} \lambda_i^{(n)} \sigma^i$, we have $\tau^{2n} = (\tau^n)^2 = \sum_{i=nm'}^{nm''} \lambda_i^{(n)} \sigma^{2i}$. From the definition of the companion matrix, it is easily checked that $b_{2i} = a_i$ and $b_{2i+1} = 0$ for $0 \le i \le \gamma(\tau^n) - 1$. So

$$P_{A_{2n}}(X) = \sum_{i=0}^{\gamma(\tau^n)-1} a_i X^{2i} + X^{2\gamma(\tau^n)} = \left(\sum_{i=0}^{\gamma(\tau^n)-1} a_i X^i + X^{\gamma(\tau^n)} \right)^2$$

$$= (P_{A_n}(X))^2.$$

Proof of Corollary 2.11 (*sequel*). Let A_n [resp. A_{2n}] be the companion matrix of the configurations with temporal period n [resp. $2n$] of $\mathscr{A}$. Let $P_{A_n}(X)$ [resp. $P_{A_{2n}}(X)$] be the minimal polynomial of A_n [resp. A_{2n}]. From the definitions and Galois' Theorem (see [2]), $\alpha(n)$ [resp. $\alpha(2n)$] is the least positive integer such that $P_{A_n}(X)$ divides $X^{\alpha(n)} + 1$ [resp. $P_{A_{2n}}(X)$ divides $X^{\alpha(2n)} + 1$]. By the preceding results, we know that $\alpha(n)$ divides $\alpha(2n)$. By Lemma 2.13, $P_{A_{2n}}(X) = (P_{A_n}(X))^2$ divides $(X^{\alpha(n)} + 1)^2 = X^{2\alpha(n)} + 1$. So $\alpha(2n) = \alpha(n)$ or $\alpha(2n) = 2\alpha(n)$. Suppose $\alpha(2n) = \alpha(n)$. If $\alpha(n) = 2k$, then $(P_{A_n}(X))^2$ divides $X^{2k} + 1 = (X^k + 1)^2$, and we get the contradiction that $\alpha(n) \le k$. If $\alpha(n) = 2k+1$, then $(P_{A_n}(X))^2$ divides $X^{2k+1} + 1$, so that $X^{2k+1} + 1$ has multiple roots in some extension field, contradicting the fact that its derivative X^{2k} has no roots in common with it. Hence $\alpha(2n) = 2\alpha(n)$ and the second statement of the corollary follows. □

We risk the conjecture that there are no further properties for $\alpha(n)$ in any of the classes of the one-dimensional infinite CA over $\mathbb{Z}_2$ with additive evolution rules, other than those made explicit by Theorem 2.10 and Corollary 2.11. The evaluation of $\alpha(n)$ is very time consuming. Some of the calculations of $\alpha(n)$ for rules 90, 150 and $\tau = \mathbb{1} + \sigma$ are given in Table 2.

However, more information concerning the minimal polynomial of companion matrices can be obtained from the following result.

Proposition 2.14. *Let $\mathscr{A}$ be a CA, and let d and n be positive natural numbers. Suppose d divides n, $\gamma(\tau^d) \ge 1$ and $\gamma(\tau^d)$ divides $\gamma(\tau^n)$. Denote by $P_A(X)$ the minimal polynomial of the matrix A and let A_d [resp. A_n] be the companion matrix of the configurations with temporal period d [resp. n]. Then $P_{A_d}(X)$ divides $P_{A_n}(X)$.*

Proof. Let x'' be the vector of $\mathbb{Z}_2^{\gamma(\tau^d)}$ such that, in the canonical basis of $\mathbb{Z}_2^{\gamma(\tau^d)}$, $(x'')_i = 0$ if $0 \le i \le \gamma(\tau^d) - 2$ and $(x'')_{\gamma(\tau^d)-1} = 1$. From Remark 2.9 $x = \{\ldots, x'' A_d^{-\gamma(\tau^d)}, x'', x'' A_d^{\gamma(\tau^d)}, \ldots\}$ is a configuration of $\mathscr{A}$ with temporal period d. Since x is also a configuration with temporal period n (because d divides n) and $\gamma(\tau^d)$ divides $\gamma(\tau^n)$ we must also have $x = \{\ldots, x' A_n^{-\gamma(\tau^n)}, x', x' A_n^{\gamma(\tau^n)}, \ldots\}$, where $x' = [x'', x'' A_d^{\gamma(\tau^d)}, \ldots, x'' A_d^{(r-1)\gamma(\tau^d)}]$. Let y'' [resp. y'] a vector of $\mathbb{Z}_2^{\gamma(\tau^d)}$ [resp. $\mathbb{Z}_2^{\gamma(\tau^n)}$] such that, for some $j \in \mathbb{Z}$, $(y'')_i = x_{i+j}$, $0 \le i \le \gamma(\tau^d) - 1$, [resp. $(y')_i = x_{i+j}$, $0 \le i \le \gamma(\tau^n) - 1$]. From the definitions, $(y'' A_d)_i = x_{i+j+1}$, $0 \le i \le \gamma(\tau^d) - 1$, and

Table 2. $\alpha(n)$ for rules $\tau=\sigma^{-1}+\sigma$, $\tau=\sigma^{-1}+\mathbb{1}+\sigma$ and $\tau=\mathbb{1}+\sigma$.

	$\alpha(n)$		
n	$\tau=\sigma^{-1}+\sigma$	$\tau=\sigma^{-1}+\mathbb{1}+\sigma$	$\tau=\mathbb{1}+\sigma$
1	3	2	1
2	6	4	1
3	15	10	3
4	12	8	1
5	51	30	15
6	30	20	6
7	63	126	7
8	24	16	1
9	315	130	63
10	102	60	30
11	3 075	2 050	341
12	60	40	12
13	12 291	8 190	819
14	126	252	14
15	255	510	15
16	48	32	1
17	65 535	510	255
18	630	260	126
19	786 435	524 290	21 483
20	204	120	60
21	4 095	8 190	63
22	6 150	4 100	682
23	4 194 303	2 796 202	4 185 601
24	120	80	24
25	17 825 775	209 715	25 575
26	24 582	16 380	1 638
27	436 905	524 290	13 797

$(y'A_n)_i = x_{i+j+1}$, $0 \le i \le \gamma(\tau^n)-1$. Then we have $(x''A_d^j)_i = x_{i+j}$, $0 \le i \le \gamma(\tau^d)-1$, and $(x'A_n^j)_i = x_{i+j}$, $0 \le i \le \gamma(\tau^n)-1$, and it follows that

$$x'A_n^j = [x''A_d^j, x''A_d^{\gamma(\tau^d)+j}, \ldots, x''A_d^{(r-1)\gamma(\tau^d)+j}]. \tag{2.14.1}$$

We now show that given any polynomial $P(X)$ in $\mathbb{Z}_2[X]$ we have $x'P(A_n)=0$ if and only if $x''P(A_d)=0$. Indeed, consider the projection $\pi: \mathbb{Z}_2^{\gamma(\tau^n)} \to \mathbb{Z}_2^{\gamma(\tau^d)}$ defined in the canonical basis of $\mathbb{Z}_2^{\gamma(\tau^n)}$ and $\mathbb{Z}_2^{\gamma(\tau^d)}$ as $(\pi(x))_i = x_i$. From the definitions $\pi(x') = x''$ and, using (2.14.1), $\pi(x'P(A_n)) = x''P(A_d)$. Then if $x'P(A_n)=0$ we have $\pi(x'P(A_n) = x''P(A_d) = 0$. Conversely, if $x''P(A_d)=0$, then $x''P(A_d)A_d^{i\gamma(\tau^d)} = x''A_d^{i\gamma(\tau^d)}P(A_d) = 0$, $0 \le i \le r-1$. Using again (2.14.1) we have $x'P(A_n)=0$ as asserted.

Let $Q(X)$ be the nonnull polynomial in $\mathbb{Z}_2[X]$ of least degree such that $x''Q(A_d)=0$. As $\{x'', x''A_d, \ldots, x''A_d^{\gamma(\tau^d)-1}\}$ is a basis of $\mathbb{Z}_2^{\gamma(\tau^d)}$, we have $z'P_{A_d}(A_d)=0$ for every vector $z' \in \mathbb{Z}_2^{\gamma(\tau^d)}$. Hence, $Q(X)$ is the nonnull polynomial of least degree such that $Q(A_d)=0$ and, from the definitions, $Q(X) = P_{A_d}(X)$.

From the above results, $P_{A_d}(X)$ is also the nonnull polynomial of least degree such that $x'P_{A_d}(A_n)=0$. Hence degree $P_{A_n}(X) \geq$ degree $P_{A_d}(X)$. Suppose that $P_{A_d}(X)$ does not divide $P_{A_n}(X)$. Then there is a nonnull polynomial $R(X)$ such that degree $R(X) <$ degree $P_{A_d}(X)$ and $x''R(A_d)=0$. It follows from the last equality, as above, that $R(A_d)=0$, a contradiction with the definition of $P_{A_d}(X)$. Hence $P_{A_d}(X)$ divides $P_{A_n}(X)$. □

In order to finish this section we (re)consider the following fundamental problem.

Problem 2.15. *Let $\mathcal{A}$ be a CA, and let x be a configuration with temporal period n of $\mathcal{A}$. What is the space period of x?*

If $\tau=\mathbb{1}$ there is no information to evaluate $\alpha(x)$. If $\tau=\mathbb{1}+\sigma^m$ $(m\in\mathbb{Z}_2-\{0\})$ and $n=2^p$ $(p\in\mathbb{N})$, only the zero configuration has temporal period n. Suppose now $\gamma(\tau^n)\geq 1$. Let A_n be the companion matrix of the configurations with temporal period n of $\mathcal{A}$. Let $\mathbf{x}'$ be the vector of $\mathbb{Z}_2^{\gamma(\tau^n)}$ such that $(x')_i=x_i$, $0\leq i\leq \gamma(\tau^n)-1$. Let $n(x')$ be the smallest integer such that the vectors $\{x', x'A_n, \ldots, x'A_n^{n(x')}\}$ are linearly dependent. Suppose $\sum_{i=0}^{n(x')}\xi_i x'A_n^i=0$ such that $\{x'A_n^i\colon \xi_i=1\}$ is a minimal dependent set. Let $Q(X)=\sum_{i=0}^{n(x')}\xi_i X^i$. (Then $Q(X)$ is the nonnull polynomial in $\mathbb{Z}_2[X]$ of least degree such that $x'Q(A_m)=0$.) Now let $m(x')$ be the smallest integer such that $Q(X)$ divides $X^{m(x')}+1$. *We claim that* $m(x')=\alpha(x)$. Since $x'A_n^{m(x')}+x'=0$ we have, from the definition of $\alpha(x)$, $\alpha(x)\leq m(x')$. If $Q(X)$ divides $X^{\alpha(x)}+1$, then we must also have $m(x')\leq\alpha(x)$ and $\alpha(x)=m(x')$. Suppose that $Q(X)$ does not divide $X^{\alpha(x)}+1$. From the definitions we have degree $Q(X)\leq\alpha(x)$. Then there is a nonnull polynomial $R(X)$ such that degree $R(X)<$ degree $Q(X)$ and $x'R(A_n)=0$, a contradiction. Hence $Q(X)$ divides $X^{\alpha(x)}+1$ and $\alpha(x)=m(x')$.

Acknowledgments

We wish to acknowledge our indebtedness to a referee for several remarks on an earlier version of this paper.

References

1. O. De Pazzis, J. Hardy, and Y. Pomeau, Molecular dynamics of a classical lattice gas: transport properties and time correlation functions, *Phys. Rev. A* **13** (1976), 1949–1961.
2. S. Lang, *Algebra*, Addison-Wesley, Reading, MA, 1967.
3. O. Martin, A. A. Odlyzko, and S. Wolfram, Algebraic properties of cellular automata, *Commun. Math. Phys.* **93** (1984), 219–258.
4. G.-C. Rota, On the foundations of combinatorial theory I: theory of Möbius functions, *Z. Wahrsch. Verw. Gebiete* **2** (1964), 340–368.
5. T. Toffoli, CAM: a high-performance cellular automaton machine, *Phys. D* **10** (1984), 195–204.
6. S. Ulam, Some ideas and prospects in biomathematics, *Ann. Rev. Biomath.* **255** 1974.

7. G. Y. Vichniac, Simulating physics with cellular automata, *Phys. D* **10** (1984), 96–116.
8. J. Von Neumann, in *Theory of Self-reproducing Automata*, (A. W. Burks ed.), University of Illinois Press, Urbana, IL, 1966.
9. S. Wolfram, Statistical mechanics of cellular automata, *Rev. Modern Phys.* **55** (1983), 601–644.
10. S. Wolfram, Universality and complexity in cellular automata, *Phys. D* **10** (1984), 1–35.
11. S. Wolfram, Computation theory of cellular automata, *Commun. Math. Phys.* **96** (1984), 15–57.

Received May 29, 1985, and in revised form December 16, 1985.