Journal of Statistical Physics, Vol 43, Nos. 3/4, 1986

Exact Results for Deterministic Cellular Automata with Additive Rules

Pu-hua Guan[1] and Yu He[2]

Received June 6, 1985; final December 20, 1985

Deterministic cellular automata (CA) with additive rules are studied by exploiting the properties of circulant matrices on finite fields. Complete state transition diagrams for higher-order and multidimensional CA on finite lattices are analyzed. Conditions on the rules which make them reversible are obtained. It is shown that all state transition diagrams of the CA have identical trees rooted on cycles. General formulae for cycle lengths and multiplicities are given.

KEY WORDS: Cellular automata; discrete dynamical systems.

1. INTRODUCTION

Cellular automata (CA)[(1)] are dynamical systems which consist typically of a regular array of variables each of which can assume a finite number of discrete values. The state of the CA, specified by the values of each of the variables at a given time, evolves temporally in discrete steps according to a given rule. CA have been used to model a variety of systems in physics, biology, and computer science. Despite their apparent simplicity, CA display rich and complex behaviors usually studied numerically; the exact determination of the temporal behavior of CA is difficult, if not impossible. However, for a particular class of CA on finite lattices the time evolution can be studied analytically. This class of CA with additive rules (to be defined later) was studied by O. Martin *et. al.*[(2)] They gave an extensive analysis of the global behavior of such CA using properties of polynomials over finite fields.

In this paper we describe a new algorithm to analyze additive CA based on the properties of circulant matrices.[(3)] Several results about the structure of the state transition diagrams of multidimensional and higher-

[1] Department of Mathematics, Ohio State University, Columbus, Ohio 43210.
[2] Department of Physics, Ohio State University, Columbus, Ohio 43210.

0022-4715/86/0500-0463$05.00/0

order CA are established. In particular, we show how the behavior of a p^q-state (p is a prime, q any integer) additive CA in d dimensions on a *finite* lattice with periodic boundary conditions can be determined explicitly. Conditions on rules which determine whether they are reversible or not are derived. CA with irreversible rules exhibit transient behavior before settling into periodic attracting sets (cycles). Cycle lengths, lengths of transients, multiplicities of cycles, and other properties are shown to be calculable for finite additive CA.

This paper is organized as follows: In the following section we introduce our notation and prove some basic theorems. In Section 3, we analyze higher-order CA and illustrate the procedure of determining the state transition diagrams; higher-dimensional CA are treated in Section 4. Results for a CA in two dimensions for lattices of size up to 22×22 are also displayed.

2. NOTATION AND PRELIMINARIES

We begin by establishing notation and proving some basic theorems about circulant matrices employed frequently in the rest of the paper. For notational compactness, this section is restricted to one-dimensional CA.

Consider a finite one-dimensional lattice with N sites (called cells, conventionally) and periodic boundary conditions. At each of the N sites there is a variable that assumes one of p^q values belonging to a field K.[4] The state (configuration) of the CA at time t can be characterized by an N-component column vector $\boldsymbol{\sigma}(t)$, whose ith entry $\sigma_{i-1}(t)$ is the value the $i-1$ site takes at time t. The definition of the CA is completed by specifying the rule according to which the state evolves in discrete time. In this paper we consider additive rules which have the following general form

$$\sigma_i(t+1) = \sum_{j=0}^{N-1} a_j \sigma_{i+j}(t) \tag{2.1}$$

where the coefficients $\{a_j\}$ belong to the same field K as do the σ_is. [Periodic boundary conditions imply $\sigma_{i+N}(t) = \sigma_i(t)$]. Different choices for $\{a_j\}$ yield different rules. Additive CA are amenable to exact analysis because of the linearity of (2.1). It is useful to rewrite (2.1) as $\boldsymbol{\sigma}(t+1) = A\boldsymbol{\sigma}(t)$, where the transition matrix A is an $N \times N$ circulant matrix[3]

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{N-1} \\ a_{N-1} & a_0 & \cdots & a_{N-2} \\ \vdots & \vdots & & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix} \equiv \operatorname{circ}(a_0, a_1, \ldots, a_{N-1}) \equiv \sum_{i=0}^{N-1} a_i \Pi_N^i \tag{2.2}$$

where Π_N itself is an $N \times N$ circulant matrix defined as

$$\Pi_N \equiv \mathrm{circ}(0, 1, 0, \ldots, 0) \tag{2.3}$$

Theorem 2.1. Let K be a finite field of character p. $|K| = p^q$. If $(p, N) = 1$, Π_N can be diagonalized by F_N (with elements in the extension field of K)

$$F_N^{-1} \Pi_N F_N = \mathrm{diag}(\eta_0, \eta_1, \ldots, \eta_{N-1}) \tag{2.4}$$

where $\eta_j = \eta^j$, $(F_N)_{ij} = (1/N^{1/2})(\eta_{i-1})^{j-1}$ and η is an Nth primitive root of unity over K.[3]

Theorem 2.2. Let K and Π_N be as before. Suppose $N = rp^l$ with $(p, r) = 1$. Then Π_N is similar to a direct sum of r Jordan blocks, each of size $p^l \times p^l$. The eigenvalues of Π_N, each of which has multiplicity p^l, are $\xi_0, \xi_1, \ldots, \xi_{r-1}$ where $\xi_i = \xi^i$ and ξ is an rth primitive root of unity.

Proof. The minimum polynomial of Π_N is

$$m(\Pi_N) = x^N - 1 = (x^r - 1)^{p^l} = det(xI - \Pi_N) \tag{2.5}$$

Since $(p, r) = 1$, $x^r - 1$ is separable over K. Hence, the Jordan blocks are given by Theorem 2.2.

Observe that Theorem 2.1 is a special case of Theorem 2.2 when $l = 0$.

Theorem 2.3. Let N, p, l, r, and $\{\xi_i\}$ be as above. All $N \times N$ circulant matrices $A = \mathrm{circ}(a_0, a_1, \ldots, a_{N-1})$ are similar to a direct sum of r $p^l \times p^l$ blocks

$$A \sim \bigoplus_{k=0}^{r-1} A^{(k)}$$

where the $A^{(k)}$s are $p^l \times p^l$ matrices given by

$$A^{(k)} = \sum_{i=0}^{N-1} a_i(\xi_k I + C)^i \equiv \sum_{i=0}^{p^l - 1} b_i^{(k)} C^i \tag{2.6}$$

Here I is a $p^l \times p^l$ unit matrix and C is a $p^l \times p^l$ matrix given by

$$C \equiv \begin{pmatrix} 0 & 1 & & & \bigcirc \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & & 1 \\ & \bigcirc & & & 0 \end{pmatrix} \tag{2.7}$$

$$b_0^{(k)} = \sum_{i=0}^{N-1} a_i \xi_k^i \equiv \lambda_k \tag{2.8}$$

[3] Henceforth, a root of unity refers to a root of unity over K.

and $b_j^{(k)}$ can be written formally as

$$b_j^{(k)} = \frac{1}{j!}\frac{d^j}{d(\xi_k)^j} b_0^{(k)} \tag{2.9}$$

The proof follows directly from Theorem 2.2 and Eq. (2.2).

In particular, when $l=0$, i.e., when $(p, N)=1$, all circulant matrices A can be diagonalized.

Now, consider $(A^{(k)})^{p^l}$. From (2.6), using the binomial expansion, we get

$$\begin{aligned}(A^{(k)})^{p^l} &= \left(\sum_{i=0}^{p^l-1} b_i^{(k)} C^i\right)^{p^l} = \sum_{i=0}^{p^l-1} (b_i^{(k)})^{p^l} (C^i)^{p^l} \\ &= \lambda_k^{p^l} I \end{aligned} \tag{2.10}$$

where we have used $C^{p^l}=0$ and $pB=0$ for all matrices B over the field of character p. Hence, A^{p^l} can be diagonalized as

$$A^{p^l} \sim \bigoplus_{i=0}^{r-1} \lambda_i^{p^l} I \tag{2.11}$$

Remark. From (2.8), we see that for each k, λ_k is an element of the extension field of K, $K(\xi)$. If $\lambda_k \neq 0$, λ_k has finite order $l_k \equiv \mathrm{ord}(\lambda_k)$, and $l_k \mid p^n - 1$, where $n = lcm\,(q, \mathrm{ord}_r\, p)$. $\mathrm{Ord}_r\, p$ is the least positive integer j such that $p^j = 1 \bmod(r)$. In particular, when $q=1$, $n = \mathrm{ord}_r\, p$.

Definition. The generating polynomial of $A = \mathrm{circ}(a_0, ..., a_{N-1})$ which defines an additive CA through (2.1), is

$$a(x) = \sum_{i=0}^{N-1} a_i x^i \tag{2.12}$$

Theorem 2.4. An additive CA (2.1) has zero eigenvalue if and only if $g(x) \equiv gcd[a(x), x^r - 1] \neq 1$. The dimension of the eigenspace of A with eigenvalue zero is $p^l \deg[g(x)]$.

Proof. Let $g(x) \neq 1$. Since $g(x) \mid x^r - 1$ and $x^r - 1$ is separable, all the roots of $g(x)$, $\xi_{k_i}\{i = 1, 2, ..., \deg[g(x)]\}$, are distinct and are roots of $x^r - 1$. Since $g(x) \mid a(x)$, $g(\xi_{k_i}) = 0$ implies $a(\xi_{k_i}) = 0$. Recall that the eigenvalue $\lambda_{k_i} = a(\xi_{k_i})$ by (2.8). Therefore, there are $\deg[g(x)]$ zero eigenvalues. The second part of Theorem 2.4 is a direct corollary of Theorem 2.3.

3. HIGHER-ORDER CA

In this section we consider N-site, p^q-state additive CA (with periodic boundary conditions) whose time-evolution is non-Markovian, i.e., the state of the CA at time t depends on the states at the $s(\geq 2)$ preceding time steps, $t-1$, $t-2$,..., $t-s$. For simplicity, we consider s-order CA in one dimension; the higher dimensional case is similar and can be treated analogously (see next section). We provide an algorithm for computing the state transition diagram explicitly. The conditions under which the class of CA rules are reversible, i.e., all states belong to cycles, are established: these depend on the influence of the state at time $t-s$ only. A general Theorem (3.2) regarding the topology of transition diagrams is proved. The fraction of the states on cycles is computed and explicit expressions for cycle lengths and multiplicities in terms of the orders of the nonzero eigenvalues of the transition matrix are given.

We discuss the CA in terms of the state vector[4] Σ, defined by

$$\Sigma^{\mathrm{Tr}}(t) = [\boldsymbol{\sigma}^{\mathrm{Tr}}(t-s+1), \boldsymbol{\sigma}^{\mathrm{Tr}}(t-s+2),..., \boldsymbol{\sigma}^{\mathrm{Tr}}(t)] \tag{3.1}$$

where $\boldsymbol{\sigma}$ is defined as before. The time evolution of Σ is given by $\Sigma(t+1) = A\Sigma(t)$. The transition matrix A has dimension sN and is given by

$$A = \begin{pmatrix} 0 & I & & & \bigcirc \\ & 0 & I & & \\ \bigcirc & & \ddots & \ddots & \\ & & & 0 & I \\ A_0 & A_1 & \cdots & & A_{s-1} \end{pmatrix} \tag{3.2}$$

where I is an $N\times N$ unit matrix and A_is are $N\times N$ circulant matrices. $A_i = \mathrm{circ}[a_0^{(i)}, a_1^{(i)},..., a_{N-1}^{(i)}]$ describes the influence of $\boldsymbol{\sigma}(t-s+i)$ on $\boldsymbol{\sigma}(t)$. The time evolution of the CA according to the rule specified by A can be represented by a state transition diagram. Let us first recall a few definitions. A state transition diagram is a directed graph with the vertices of the graph corresponding to the states of the CA. The vertices are connected by directed edges which represent the transition between the CA states at each time step. (Note that the graph may be a union of disjoint subgraphs). Observe that since the CA rule is deterministic, each vertex has a unique successor. However, there may be zero, one, or more predecessors for each CA state. Since the number of CA states is finite the CA evolving from any initial state must eventually enter a cycle. Thus the transition diagram consists of cycles (which may be points!) with trees rooted on the

4 From now on in this section, Σ rather than $\boldsymbol{\sigma}$ is referred to as a state of the CA.

vertices in the cycle. The state at the top of a tree which does not have a predecessor will be referred to as a leaf.

We now explore the topology of the state transition diagram; one property of interest is clearly the occurrence of cycles. Since the state vector Σ at $t+1$ is $A\Sigma(t)$, Σ will be on a cycle if the projection of Σ on any invariant subspace of A with eigenvalue zero vanishes. We now proceed to determine the conditions under which A has no zero eigenvalues and thus all states are on cycles.

By Theorem 2.3, A_i is similar to a direct sum of upper triangular matrices

$$A_i \sim \Lambda_i = \bigoplus_{k=0}^{r-1} \Lambda_i^{(k)}$$

where $N = rp^l$ as before and $\Lambda_i^{(k)}$ is a $p^l \times p^l$ matrix given by Eqs. (2.6)–(2.9). Moreover, the matrix T which transforms A_i to Λ_i is the same for all i (it is the matrix that transforms Π_N to its Jordan form). Therefore, we have

$$\Lambda = \begin{pmatrix} T & & & \\ & T & & \\ & & \ddots & \\ & & & T \end{pmatrix}^{-1} A \begin{pmatrix} T & & & \\ & T & & \\ & & \ddots & \\ & & & T \end{pmatrix} = \begin{pmatrix} 0 & I & & & \\ & & I & & \\ & & & \ddots & \\ & & & & I \\ \Lambda_0 & \Lambda_1 & & \cdots & \Lambda_{s-1} \end{pmatrix} \tag{3.3}$$

The characteristic polynomial of A is obviously the same as that of Λ. Performing elementary operations on $xI - \Lambda \equiv B$, we obtain

$$B \sim \begin{pmatrix} I & & & & \\ & I & & 0 & \\ & & \ddots & & \\ & 0 & & I & \\ & & & & B_0 \end{pmatrix} \tag{3.4}$$

where B_0 is an $N \times N$ upper triangular matrix given by

$$B_0 = x^s I - \sum_{i=0}^{s-1} x^i \Lambda_i = x^s I - \bigoplus_{k=0}^{r-1} \sum_{i=0}^{s-1} x^i \Lambda_i^{(k)} \tag{3.5}$$

Since B is upper triangular, the characteristic polynomial of A is the product of the diagonal elements of B_0. The diagonal elements of the kth block of B_0 are all identical and they are simply

$$f_k(x) = x^s - \sum_{i=0}^{s-1} x^i \lambda_i^{(k)} \tag{3.6}$$

where $\lambda_i^{(k)}$, the kth eigenvalue of A_i, is given by

$$\lambda_i^{(k)} = \sum_{j=0}^{N-1} a_j^{(i)} \xi_k^j \tag{3.7}$$

as before.

If $\lambda_0^{(k)} \neq 0$ for every k none of the eigenvalues of A are zero. Hence, all possible states of CA will be on cycles. If, on the other hand, $\lambda_0^{(k)} = 0$ for some k, A will have zero eigenvalues. In this case, some states will not be on cycles and will appear only as vertices on trees.

Combining (3.6) and Theorem 2.4 we have:

Theorem 3.1. For additive CA of order s, each state Σ is on a cycle (i.e., the rule is reversible) if and only if $gcd[a_0(x), x^r - 1] = 1$, where $a_0(x)$ is the generating polynomial of A_0.

When $gcd[a_0(x), x^r - 1] \equiv g(x) \neq 1$, there will be states Σ which belong to trees rooted on cycles. We now establish a general property of trees.

Theorem 3.2. The trees rooted at all vertices on all cycles of the state transition diagram of the CA defined by (3.2) are identical.

Proof. There exists a transformation matrix Q, such that $Q^{-1}AQ = J$. J is a Jordan matrix. A state vector Σ is on a cycle if Σ belongs to an invariant subspace of A with nonzero eigenvalue. Consider the largest invariant space V^1 of A with eigenvalue zero. Within V^1 there can still be invariant subspaces $J_1, J_2, \ldots, J_k$, each one of which corresponds to a block in J with zero diagonal elements. For each subspace J_i there exists a generator $\mathbf{u}_i$, such that, if the dimension of J_i is d_i, then $\mathbf{u}_i$, $A\mathbf{u}_i$, $A^2\mathbf{u}_i, \ldots, A^{d_i - 1}\mathbf{u}_i \neq 0$ form a basis of the subspace J_i and $A^{d_i}\mathbf{u}_i = 0$. Thus all the elements in V^1 form one tree with the root $\Sigma = 0$ and leaves

$$\sum_{i=1}^{k} \sum_{j=0}^{d_i - 1} a_{ji} A^j \mathbf{u}_i \qquad \text{where } a_{ji} \in K(\xi) \text{ and } a_{0i} \neq 0 \text{ for some } i$$

Now, in the Jordanized basis, the transition matrix can be written as $A = A_0 \oplus A_1$, where A_1 is a direct sum of all the Jordan blocks which have nonzero diagonal elements. Correspondingly, $\mathbf{\Sigma} = \mathbf{\Sigma}_0 \oplus \mathbf{\Sigma}_1$, and hence, the time evolution is given by $\mathbf{\Sigma}(t+1) = (A_0\mathbf{\Sigma}_0) \oplus (A_1\mathbf{\Sigma}_1)$. For each $\mathbf{\Sigma}$ on a cycle, i.e., $\mathbf{\Sigma}_0 \equiv 0$, construct the set

$$S_1 = \left\{ \mathbf{\Sigma}_0 \oplus (A_1^{-1}\mathbf{\Sigma}_1) + \sum_{i=1}^{k} a_{d_i-1,i} A^{d_i-1} \mathbf{u}_i \,|\, a_{d_i-1,i} \in K(\xi), \right.$$

$$\vdots \qquad \left. a_{d_i-1,i} \neq 0 \text{ for some } i \right\}, \tag{3.8}$$

$$S_d = \left\{ \mathbf{\Sigma}_0 \oplus (A_1^{-d}\mathbf{\Sigma}_1) + \sum_{i=1}^{k} \sum_{j=d_i-d}^{d_i-1} a_{j,i} A^j \mathbf{u}_i \,|\, a_{j,i} \in K(\xi), \right.$$

$$\ldots \qquad \left. a_{d_i-d,i} \neq 0 \text{ for some } i \right\}, \tag{3.9}$$

Then, $\bigcup_{t=1}^{\max\{d_i\}} S_t$ is a tree rooted on $\mathbf{\Sigma}$ and is isomorphic to the tree rooted on $\mathbf{\Sigma} = 0$. Q.E.D.

Note that the above proof does not depend on the A_is being circulant matrices. In fact, Theorem 3.2 is valid for arbitrary (including inhomogenous) additive CA irrespective of dimensionality, order, or nature of boundary conditions.

Corollary. Let k be the number of Jordan blocks with zero diagonal elements in A, and d_m be the dimension of the largest of those k blocks. The height of the tree rooted at each vertex of a cycle is d_m. In particular, if all the k blocks have the same size d_m, the tree is balanced and has in-degree $|K|^k$. [A tree is said to be balanced if the number of predecessors (in-degree) is the same for all vertices on the tree and the distance from each leaf to the root is also the same. The height of a tree is defined to be the largest distance from the leaf to the root.]

Let us define

$$g_1(x) = gcd[a_1(x), g(x)] \tag{3.10}$$

$$g_i(x) = gcd[a_i(x), g_{i-1}(x)] \qquad \text{for} \quad i = 2, 3, \ldots, s-1 \tag{3.11}$$

$$n_i' = \deg[g_i(x)] \qquad n_s' = 0 \quad \text{and} \quad n_0' = \deg[g(x)] \tag{3.12}$$

Clearly, $n_i = n_{i-1}' - n_i'$ is the number of f_js which have zero roots of multiplicity i. So the total number of zeros on the diagonal of the Jordan form of A is

$$\lambda = p^l \sum_{i=1}^{s} i n_i \tag{3.13}$$

From the proof of Theorem 3.2, we have:

Theorem 3.3. The fraction of the configurations of a CA defined by (3.2) that are on cycles is $|K|^{-\lambda}$.

Remark. All the states of the CA are in K^{Ns} while the Jordan forms and generating vectors we have been discussing belong to $K(\xi)^{Ns}$. Since K^{Ns} is a full lattice in $K(\xi)^{Ns}$, the intersection of K^{Ns} with any subspace V of $K(\xi)^{Ns}$, which has dimension n, is also a subspace of K^{Ns} with dimension n.

We now obtain the multiplicities and the lengths of the cycles in terms of the order of the nonzero eigenvalues of the transition matrix A. By solving (3.6) for each k, we get all eigenvalues ζ_i of A. Then $A \sim J = \bigoplus_i(\zeta_i I + C_{d_i})$, where C_{d_i} is a $d_i \times d_i$ matrix of the form in (2.7). Let $\bar{l}$ be the smallest integer such that $p^{\bar{l}} \geqslant \bar{d}$, where $\bar{d}$ is the dimension of the largest Jordan block of J; we then have

$$A^{p^{\bar{l}}} \sim \bigoplus_i (\zeta_i I + C_{d_i})^{p^{\bar{l}}} = \bigoplus_i \zeta_i^{p^{\bar{l}}} I$$

That is, $A^{p^{\bar{l}}}$ is similar to a diagonal matrix. Denote the nonzero eigenvalues of A by $\zeta_i (i = 0, 1,..., r')$. We have thus shown:

Theorem 3.4. The possible cycle lengths of a CA defined by (3.2) are $\mathrm{ord}(\zeta_i)$, $p\,\mathrm{ord}(\zeta_i)$,..., $p^{l_i}\,\mathrm{ord}(\zeta_i)$ and their least common multiples, $p^i \times lcm[\mathrm{ord}(\zeta_{i_1}), \mathrm{ord}(\zeta_{i_2}),..., \mathrm{ord}(\zeta_{i_m})] (i_j = 0, 1, 2,..., r', m = 2, 3,..., r'$ and $i \leqslant (\bar{l})$, where l_i is the smallest integer such that $p^{l_i} \geqslant d_i$ (d_i is the dimension of the Jordan block corresponding to the nonzero eigenvalue ζ_i).

The maximum cycle length L is

$$L = p^{\bar{l}} \times lcm[\mathrm{ord}(\zeta_0), \mathrm{ord}(\zeta_1),..., \mathrm{ord}(\zeta_{r'})]$$

So we see that all possible cycle lengths are divisors of the maximum cycle length L and, in turn, L is a divisor of $p^{\bar{l}}(p^n - 1)$. (See the remark in Sect. 2.)

Knowing the cycle length $L(i)$, its multiplicity $m[L(i)]$ can be computed. Let $K^{Ns} = V_0 \oplus V$ where V_0 and V are subspaces corresponding to zero and nonzero eigenvalues, respectively. Let D_i be the dimension of the largest subspace S_i of V such that the maximum cycle length in S_i is $L(i)$. Two cases must be distinguished. If no other cycles with length different from $L(i)$ are present in S_i, then $m[L(i)]$ is given by (not including the trivial one-cycle $\mathbf{O}$)

$$m[L(i)] = [(p^q)^{D_i} - 1]/L(i) \tag{3.14}$$

where the numerator is the total number of states (excluding the zero state) in the D_i-dimensional subspace. If, on the other hand, S_i contains several distinct cycles with length denoted by $L(j_1), L(j_2),..., L(j_n)$ then the multiplicity is

$$m[L(i)] = \left\{(p^q)^{D_i} - \sum_{k=1}^{n} L(j_k)\, m[L(j_k)] - 1\right\} \Big/ L(i) \qquad (3.15)$$

4. CA IN HIGHER DIMENSIONS

The methods described in previous sections can be applied to arbitrary integer dimensions. As an illustrative example, we present the results for two-dimensional CA when the state at time t depends only on the state at time $t-1$. Results for one-dimensional CA can be recovered as a special case by setting the number of rows equal to 1 while the higher-dimensional cases can be treated inductively. The extension to higher-order CA in higher dimensions is tedious but straightforward.

Consider a p^q-state CA on a two-dimensional lattice of M rows and N columns with periodic boundary conditions. We can represent the state of CA by an MN-component column vector $\boldsymbol{\sigma}(t)$ with the elements representing the state of N sites in each of the M rows successively. Because of the periodicity in both directions, the transition matrix A is a circulant of circulant matrices

$$A = \mathrm{circ}(A_0, A_1,..., A_{M-1}) \qquad (4.1)$$

Here, each A_i is an $N \times N$ circulant matrix[5] which describes the influence of the ith row on the future

$$A_i = \mathrm{circ}[a_0^{(i)}, a_1^{(i)},..., a_{N-1}^{(i)}] \qquad (4.2)$$

A can be written in terms of the $M \times M$ matrix Π_M (defined before) as

$$A = \sum_{i=0}^{M-1} \Pi_M^i \otimes A_i \qquad (4.3)$$

First we discuss the simple case $(M, p) = 1$ and $(N, p) = 1$. Recall that Π_M and A_i can both be diagonalized by F_M and F_N, respectively (Theorems 2.1 and 2.3)

$$\begin{aligned} \Pi_M &\sim \Omega = \mathrm{diag}(\xi_0, \xi_1,..., \xi_{M-1}) \\ A_i &\sim \Lambda_i = \mathrm{diag}[\lambda_0^{(i)}, \lambda_1^{(i)},..., \lambda_{N-1}^{(i)}] \end{aligned} \qquad (4.4)$$

[5] Note that A itself is not necessarily an $NM \times NM$ circulant matrix. In three dimensions, the transition matrix will be a circulant of circulant of circulant matrices, and so on.

where

$$\xi_i = \xi^i, \ \xi \text{ is an } M\text{th primitive root of unity and} \tag{4.5}$$

$$\lambda_j^{(i)} = \sum_{l=0}^{N-1} a_l^{(i)} \eta_j^l, \ \eta_j = \eta^j \tag{4.6}$$

η is an Nth primitive root of unity. Therefore

$$\begin{aligned} \Pi_M^i \otimes A_i &= (F_M \Omega^i F_M^{-1}) \otimes (F_N \Lambda_i F_N^{-1}) \\ &= (F_M \otimes F_N)(\Omega^i \otimes \Lambda_i)(F_M \otimes F_N)^{-1} \end{aligned} \tag{4.7}$$

and

$$A = (F_M \otimes F_N) \sum_{i=0}^{M-1} (\Omega^i \otimes \Lambda_i)(F_M \otimes F_N)^{-1} \tag{4.8}$$

Hence, the eigenvalues of A are given by

$$\begin{aligned} \rho_{kj} &= \sum_{i=0}^{M-1} \xi_k^i \lambda_j^{(i)} = \sum_{l=0}^{N-1} \left[\sum_{i=0}^{M-1} a_l^{(i)} \xi_k^i \right] \eta_j^l \\ &\equiv \sum_{l=0}^{N-1} b_{lk} \eta_j^l \qquad \begin{pmatrix} k = 0, 1, \ldots, M-1 \\ j = 0, 1, \ldots, N-1 \end{pmatrix} \end{aligned} \tag{4.9}$$

where

$$b_{lk} = \sum_{i=0}^{M-1} a_l^{(i)} \xi_k^i \tag{4.10}$$

Theorem 4.1. Let

$$b_k(x) = \sum_{l=0}^{N-1} b_{lk} x^l \tag{4.11}$$

All configurations of the CA evolving under the rule specified by (4.1) for $(p, M) = 1$ and $(p, N) = 1$ are on cycles if and only if for $k = 0, 1, \ldots, M-1$

$$gcd[b_k(x), x^N - 1] \equiv g_k(x) = 1 \tag{4.12}$$

Proof. By (4.9), $\rho_{kj} = b_k(\eta_j)$. If (4.12) holds, then $b_k(\eta_j) \neq 0$ for all j. Therefore, $\rho_{kj} \neq 0$. Since ρ_{kj} is in a finite extension of a finite field, $A^h = I$ for $h = lcm_{k,j}[\mathrm{ord}(\rho_{kj})]$. Therefore, all configurations are on cycles.

Corollary 4.1. The fraction of configurations that are on cycles for the CA evolving under the rules specified by (4.1) for $(p, M) = 1$ and $(p, N) = 1$ is

$$|K|^{-\sum_{i=0}^{M-1} \deg[g_i(x)]}$$

Now, consider the case $(p, N) \neq 1$, $(p, M) \neq 1$. Let[6] $M = sp^k$, $N = rp^l$, and $(s, p) = (r, p) = 1$. By Theorem 2.3, all A_i can be simultaneously transformed to a direct sum of r blocks $A_i^{(j)}$ each of size $p^l \times p^l$ by a nonsingular matrix T, and Π_M^i can be transformed to a direct sum of s blocks P_j^i each of size $p^k \times p^k$ by S, where $A_i^{(j)}$ and p_j^i are given by

$$A_i^{(j)} = \sum_{m=0}^{N-1} a_m^{(i)} (\eta_j I + C)^m \tag{4.13}$$

and

$$P_j^i = (I\xi_j + C)^i \tag{4.14}$$

($\eta_i = \eta^i$, $\xi_j = \xi^j$, and η and ξ are the rth and sth primitive roots of unity, respectively).

Hence

$$\begin{aligned} A &= \sum_{i=0}^{M-1} (SP^iS^{-1}) \otimes (TA_iT^{-1}) \\ &= (S \otimes T) \sum_{i=0}^{M-1} \left[\left(\bigoplus_{j=0}^{s-1} P_j^i \right) \otimes \left(\bigoplus_{m=0}^{r-1} A_i^{(m)} \right) \right] (S \otimes T)^{-1} \end{aligned} \tag{4.15}$$

The diagonal elements have the same form as (4.9), and so we have:

Corollary 4.2. All configurations of the CA evolving under the rule specified by (4.1) are on cycles if and only if for $k = 0, 1, \ldots, s-1$

$$gcd[b_k(x), x^r - 1] \equiv g_k(x) = 1$$

Obviously, the number of ρ_{ij} which are zero is given by $\sum_{i=0}^{s-1} \deg[g_i(x)]$ and each zero has degeneracy p^{k+l}. So we have:

Corollary 4.3. The fraction of the states that are on cycles for the CA evolving under the rule specified by (4.1) is $|K|^{-\lambda}$, where

$$\lambda = p^{l+k} \sum_{i=0}^{s-1} \deg[g_i(x)]$$

Theorem 4.2. The trees rooted at all vertices on all cycles of the state transition diagram of the CA evolving under the rule specified by (4.1) are identical.

[6] The cases (a) $(p, N) = (p, M) = 1$, (b) $(p, M) \neq (p, N) = 1$, and (c) $(p, N) \neq (p, M) = 1$ correspond to (a) $l = k = 0$, (b) $k \neq l = 0$, and (c) $l \neq k = 0$, respectively.

The proof is exactly the same as for Theorem 3.2. The structure of the trees is given exactly as in the Corollary in Section 3.

We now determine the lengths of cycles. Note that

$$A \sim \Lambda = \sum_{i=0}^{M-1} \left[\left(\bigoplus_{j=0}^{s-1} P_j^i \right) \otimes \left(\bigoplus_{m=0}^{r-1} \Lambda_i^{(m)} \right) \right] \tag{4.16}$$

Since P_j^i and $\Lambda_i^{(m)}$ are upper triangular blocks, Λ is also an upper triangular matrix. Therefore

$$\begin{aligned} A \sim \Lambda &= \bigoplus_{j=0}^{s-1} \left\{ \sum_{i=0}^{M-1} \left[P_j^i \otimes \left(\bigoplus_{m=0}^{r-1} \Lambda_i^{(m)} \right) \right] \right\} \\ &\equiv \bigoplus_{j=0}^{s-1} \tilde{\Lambda}_j \end{aligned} \tag{4.17}$$

The diagonal elements of Λ are eigenvalues ρ_{jm} of A where

$$\rho_{jm} = \sum_{i=0}^{N-1} \left(\sum_{t=0}^{M-1} a_i^{(t)} \xi_j^t \right) \eta_m^i$$

As in the higher-order CA case, if $\bar{l}$ is the smallest integer such that $p^l \geqslant \bar{d}$ where $\bar{d}$ is the dimension of the largest Jordan block of A, $A^{p^{\bar{l}}}$ is similar to a diagonal matrix.

We therefore, have,

Theorem 4.3. The possible cycle lengths of a CA evolving under the rule specified by (4.1) are p^i times the orders of the nonzero eigenvalues[7] of A, p^i ord(ρ_{jm}). $(i \leqslant l_{jm}$. l_{jm} is the smallest integer such that $p^{l_{jm}} \geqslant d_i$ where d_i is the dimension of the Jordan block corresponding. to $\rho_{jm})$ and their least common multiples

$$p^i \times lcm[\operatorname{ord}(\rho_{i_1 j_1}), \operatorname{ord}(\rho_{i_2 j_2}), \ldots, \operatorname{ord}(\rho_{i_m j_m})] \begin{pmatrix} i_i = 0, 1, \ldots, s'-1 \\ j_i = 0, 1, \ldots, r'-1 \end{pmatrix}$$

($s'r'$ is the total number of distinct nonzero eigenvalues and $i \leqslant \bar{l}$). The maximum cycle length L is $L = p^{\bar{l}} \times lcm[\operatorname{ord}(\rho_{00}), \operatorname{ord}(\rho_{01}), \ldots, \operatorname{ord}(\rho_{s'-1\, r'-1})]$. Again, the possible cycle lengths are divisors of L, and L is a divisor of $P^{\bar{l}}(p^\alpha - 1)$, where $\alpha = lcm(q, \operatorname{ord}_r p, \operatorname{ord}_s p)$.

The multiplicities of cycles can be worked out exactly as in Section 3.

[7] Since $\rho_{jm} \to \rho_{jm}^p$ is a Frobenius automorphism of $K(\xi, \eta)$, the order of ρ_{jm}^p is the same as that of ρ_{jm}.

As an illustrative example we have worked out the multiplicities and lengths of cycles of a CA on a two-dimensional square lattice of size $N \times N$ (with N up to 22) with the following rule

$$\sigma_{(i,j)}(t+1) = \sigma_{(i+1,j)}(t) + \sigma_{(i-1,j)}(t) + \sigma_{(i,j+1)}(t) + \sigma_{(i,j-1)}(t) \bmod 2 \qquad (4.18)$$

The results are displayed in Table I. The requisite factorization of polynomials was carried out using MACSYMA.

Table I. Cycle Length L and Multiplicity M for $N \times N$ Lattice with Rule defined in (4.18)[a]

N	$[L]$: M
3	[1]: (4, 0)
4	[1]: (0, 0)
5	[1]: (8, 0); [3]: (8, 0)(4, 1)(2, 1)
6	[1]: (8, 0); [2]: (8, −1)(7, 0)
7	[1]: (0, 0); [7]: (36, −1)/(3, −1)
8	[1]: (0, 0)
9	[1]: (4, 0); [7]: (60, −1)(4, 0)/(3, −1)
10	[1]: (16, 0); [2]: (16, −1)(15, 0); [3]: (16, 0)(16, −1)/(1, 1); [6]: (48, −(17, −1))(15, 0)/(1, 1)
11	[1]: (0, 0); [31]: (100, −1)/(5, −1)
12	[1]: (16, 0); [2]: (16, −1)(15, 0); [4]: (32, −1)(30, 0)
13	[1]: (0, 0); [7]: (24, −1)/(3, −1); [21]: (48, −1)(24, 0)/(3, −1)(1, 1); [63]: (72, 0)(72, −1)/(6, −1)
14	[1]: (0, 0); [7]: (72, −1)/(3, −1); [14]: (72, −1)(71, 0)/(3, −1)
15	[1]: (12, 0); [3]: (40, −1)(12, 0)/(1, 1); [5]: (64, −1)(12, 0)/(2, 1); [15]: (184, −(64, (40, −1)))(12, 0)/(4, −1)
16	[1]: (0, 0)
17	[1]: (16, 0); [3]: (48, −1)(16, 0)/(1, 1); [5]: (80, −1)(16, 0)/(2, 1); [15]: (240, −(80, (48, −1)))(16, 0)/(4, −1)
18	[1]: (8, 0); [2]: (8, −1)(7, 0); [7]: (120, −1)(8,0)/(3, −1); [14]: (248, −(120, (8, −1)))(7, 0)/(3, −1)
19	[1]: (0, 0); [511]: (324, −1)/(9, −1)
20	[1]: (32, 0); [2]: (32, −1)(31, 0); [3]: (32, 0)(32, −1)/(1, 1); [4]: (64, −1)(62, 0); [6]: (96, −(33, −1))(31, 0)/(1, 1); [12]: (192, −(65, −1))(62, 0)/(1, 1)
21	[1]: (4, 0); [7]: (84, −1)(4, 0)/(3, −1); [9]: (48, −1)(4, 0)/(3, 1); [21]: (88, 0)(24, 1)(12, 1)(6, 1)(1, 1); [63]: (396, −(132, (48, −1)))(4, 0)/(6, −1)
22	[1]: (0, 0); [31]: (200, −1)/(5, −1); [62]: (200, −1)(199, 0)/(5, −1)

[a] The notation (a, b) in the table means $2^a + b$. For example, for $N = 10$, [6]: (48, −(17, −1)) (15, 0)/(1, 1) means that the multiplicity of 6-cycle is $(2^{48} - 2^{17} + 1)\, 2^{15}/3$.

In summary, we have shown that in order to compute the state transition diagram one simply finds the Jordan form J of the transition matrix A. Then the order of the nonzero diagonal elements of J (eigenvalues of A) yields the cycle lengths. To decide whether a state $\boldsymbol{\sigma}$ is on a cycle or how far it is away from a cycle, one needs to know the matrix which transforms A to J. The state $\boldsymbol{\sigma}$ is on a tree if it has nonzero components in the zero-eigenvalue subspace. This can be determined easily by examining $\boldsymbol{\sigma}$ in a Jordanized basis. Furthermore, the distance from the root can be obtained by considering the projection of $\boldsymbol{\sigma}$ onto an appropriate basis for the zero-eigenvalue subspace. All the computations are standard and the number of steps needed is $O(N^3)$ where N is the dimension of the transition matrix. Therefore, all additive CA discussed in this paper are computationally reducible and their time evolution can be determined explicitly.

ACKNOWLEDGMENTS

We thank Dr. C. Jayaprakash for helpful discussions and a reading of the manuscript. One of us (Y. H.) is grateful to the National Science Foundation (NSF DMR 83-15770) for financial support.

APPENDIX

In this appendix, we illustrate the use of the general formalism developed in the paper by determining the state transition diagram for a simple rule. We have chosen the one-dimensional nearest-neighbor mod 2 rule (rule 90 in Ref. 1), i.e., $\sigma_i(t+1) = \sigma_{i-1}(t) + \sigma_{i+1}(t)$ mod 2 as a pedagogical example. We proceed as follows to obtain the state transition diagram for a lattice with $N = 2^l r$ sites.

1. Write down the transition matrix and its eigenvalues.

The transition matrix A (see (2.2)) for this rule is given in terms of $a_1 = a_{N-1} = 1$ with the rest of a_i's being zero. The eigenvalues of A are determined from (2.8): $\lambda_k = \xi_k + \xi_k^{N-1} = \xi^k + \xi^{-k}$ ($k = 0, 1,..., N-1$) where ξ is an rth primitive root of unity.

2. Determine the order of the eigenvalues.

This is done as follows: Given N and hence r, one factorizes $x^r - 1$ on $GF(2)$. $x_r - 1 = f_1(x) \cdots f_n(x)$. Here $f_n(x)$ is an nth degree polynomial whose roots are rth primitive roots of unity, i.e., $f_n(\xi) = 0$. Then, one finds the smallest m such that $(\lambda_k)^m = 1 \bmod f_n(\xi)$ (Since $m \mid 2^n - 1$, one only needs to try those integers which are factors of $2^n - 1$). The order of λ_k is given by m.

For example, let $N = 15$. Factorizing $X^{15} - 1$ gives $n = 4$ and $f_4(x) = x^4 + x + 1$. Since $2^n - 1 = 15$, the order of λ_k can only be 1, 3, 5 or 15. For $\lambda_1 = \xi + \xi^{-1}$, it turns out $\lambda_1^{15} = 1 \bmod f_4(\xi)$. Therefore, $\operatorname{ord}(\lambda_1) = 15$. Similarly, one can find the orders of the rest of the eigenvalues. The results are: $\lambda_0 = 0$, two eigenvalues have order one (i.e., n_1, the number of order one eigenvalues, is 2), four have order three ($n_3 = 4$) and eight have order fifteen ($n_{15} = 8$).

3. Determine the Jordan form of A, cycle lengths and dimension of subspace corresponding to various cycles.

For $N = 15$, A can be diagonalized (Theorem 2.1), so the cycle lengths are simply given by the order of λ's, i.e., 1, 3, and 15 (Theorem 4.3). The dimension D_i of the subspace which corresponds to cycle of length i is calculated as follows (see the end of Sec. 3). $D_1 = n_1 = 2$, $D_3 = n_1 + n_3 = 6$ and $D_{15} = n_1 + n_3 + n_{15} = 14$.

The state transition diagram follows from the above. Since there is one zero eigenvalue ($d_m = 1$), the rule is irreversible. Thus the height of the tree rooted on each vertex of cycles is one (corollary in Sec. 3). The fraction of states which are on cycles is $p^{-d_m} = 2^{-1}$ (corollary 4.3). The multiplicity of cycles are given by (3.14) and (3.15): $m(1) = 2^2 - 1 = 3$. $m(3) = [2^6 - m(1) - 1]/3 = 20$ and $m(15) = [2^{14} - 3m(3) - m(1) - 1]/15 = 1088$. Including the trivial one-cycle corresponding to the zero state, the multiplicity of cycles of length one is $m(1) + 1 = 4$.

Similarly, one can work out the even N case. If $N = 2^l \cdot r$, we get the same eigenvalues as in $N = r$ except that in this case the degeneracy of eigenvalues are increased by a factor 2^l. For example, for $N = 30 = 2 \cdot 15$, the cycle lengths are $= 1, 3, 15, 2 \times 1, 2 \times 3, 2 \times 15$ while for $N = 60 = 2^2 \cdot 15$, the lengths are $= 1, 3, 15, 2 \times 1, 2 \times 3, 2 \times 15, 4 \times 1, 4 \times 3, 4 \times 15$ (Theorem 4.3). For $N = 30$, the dimension of zero-eigenspace d_m is 2. Therefore, the height of each tree is 2 and the fraction of states which are on cycles is $p^{-d_m} = 2^{-2}$. The multiplicity of each cycle length is given by (3.14) and (3.15) with $D_1 = 2$, $D_2 = 4$, $D_3 = 6$, $D_6 = 12$, $D_{15} = 14$ and $D_{30} = 28$.

REFERENCES

1. S. Wolfram, *Rev. Mod. Phys.* **55**:601 (1983); *Physica* 10D:247 (1984).
2. O. Martin, A. M. Odlyzko, and S. Wolfram, *Commun. Math. Phys.* **93**:219 (1984).
3. Philip J. Davis, *Circulant Matrices* (John Wiley & Sons, New York, 1979).
4. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland, New York, 1977).