Commun. Math. Phys. 93, 219–258 (1984)

Communications in
Mathematical
Physics

Algebraic Properties of Cellular Automata

Olivier Martin[1,★], Andrew M. Odlyzko[2], and Stephen Wolfram[2,3,★★]

1 California Institute of Technology, Pasadena, CA 91125, USA
2 Bell Laboratories, Murray Hill, NJ 07974, USA
3 The Institute for Advanced Study, Princeton, NJ 08540, USA

Abstract. Cellular automata are discrete dynamical systems, of simple construction but complex and varied behaviour. Algebraic techniques are used to give an extensive analysis of the global properties of a class of finite cellular automata. The complete structure of state transition diagrams is derived in terms of algebraic and number theoretical quantities. The systems are usually irreversible, and are found to evolve through transients to attractors consisting of cycles sometimes containing a large number of configurations.

1. Introduction

In the simplest case, a cellular automaton consists of a line of sites with each site carrying a value 0 or 1. The site values evolve synchronously in discrete time steps according to the values of their nearest neighbours. For example, the rule for evolution could take the value of a site at a particular time step to be the sum modulo two of the values of its two nearest neighbours on the previous time step. Figure 1 shows the pattern of nonzero sites generated by evolution with this rule from an initial state containing a single nonzero site. The pattern is found to be self-similar, and is characterized by a fractal dimension $\log_2 3$. Even with an initial state consisting of a random sequence of 0 and 1 sites (say each with probability $\frac{1}{2}$), the evolution of such a cellular automaton leads to correlations between separated sites and the appearance of structure. This behaviour contradicts the second law of thermodynamics for systems with reversible dynamics, and is made possible by the irreversible nature of the cellular automaton evolution. Starting from a maximum entropy ensemble in which all possible configurations appear with equal probability, the evolution increases the probabilities of some configurations at the expense of others. The configurations into which this concentration occurs then dominate ensemble averages and the system is "organized" into having the

★ Address from September 1983: Physics Department, Columbia University, New York, NY 10027, USA
★★ Address from January 1983

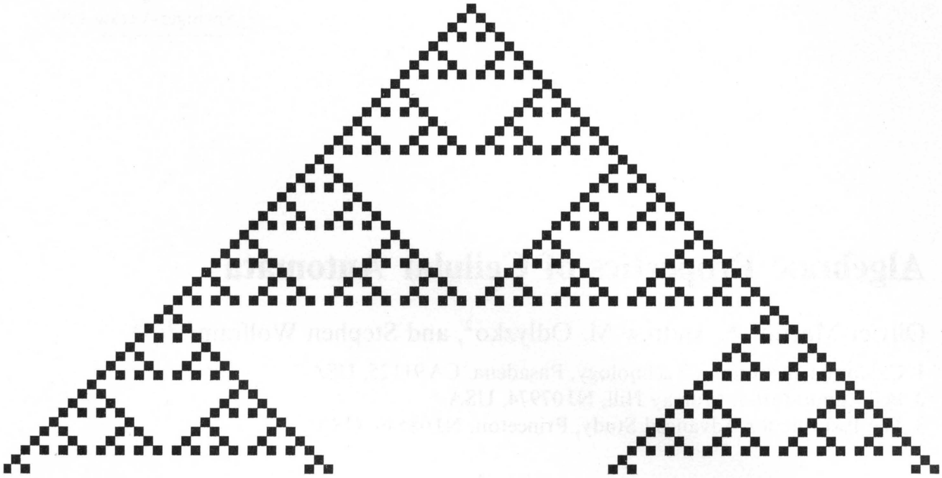

Fig. 1. Example of evolution of a one-dimensional cellular automaton with two possible values at each site. Configurations at successive time steps are shown as successive lines. Sites with value one are black; those with value zero are left white. The cellular automaton rule illustrated here takes the value of a site at a particular time step to be the sum modulo two of the values of its two nearest neighbours on the previous time step. This rule is represented by the polynomial $\mathbb{T}(x)=x+x^{-1}$, and is discussed in detail in Sect. 3

properties of these configurations. A finite cellular automaton with N sites (arranged for example around a circle so as to give periodic boundary conditions) has 2^N possible distinct configurations. The global evolution of such a cellular automaton may be described by a state transition graph. Figure 2 gives the state transition graph corresponding to the cellular automaton described above, for the cases $N=11$ and $N=12$. Configurations corresponding to nodes on the periphery of the graph are seen to be depopulated by transitions; all initial configurations ultimately evolve to configurations on one of the cycles in the graph. Any finite cellular automaton ultimately enters a cycle in which a sequence of configurations are visited repeatedly. This behaviour is illustrated in Fig. 3.

Cellular automata may be used as simple models for a wide variety of physical, biological and computational systems. Analysis of general features of their behaviour may therefore yield general results on the behaviour of many complex systems, and may perhaps ultimately suggest generalizations of the laws of thermodynamics appropriate for systems with irreversible dynamics. Several aspects of cellular automata were recently discussed in [1], where extensive references were given. This paper details and extends the discussion of global properties of cellular automata given in [1]. These global properties may be described in terms of properties of the state transition graphs corresponding to the cellular automata.

This paper concentrates on a class of cellular automata which exhibit the simplifying feature of "additivity". The configurations of such cellular automata satisfy an "additive superposition" principle, which allows a natural representation of the configurations by characteristic polynomials. The time evolution of

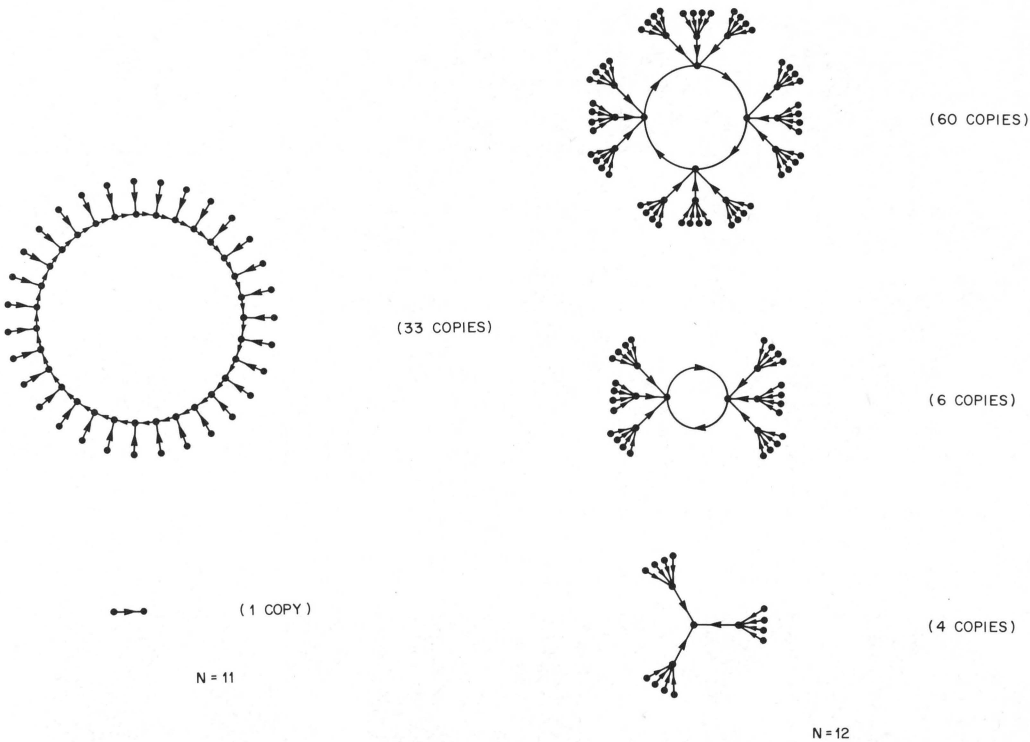

Fig. 2. Global state transition diagrams for finite cellular automata with size N and periodic boundary conditions evolving according to the rule $\mathbb{T}(x)=x+x^{-1}$, as used in Fig. 1, and discussed extensively in Sect. 3. Each node in the graphs represents one of the 2^N possible configurations of the N sites. The directed edges of the graphs indicate transitions between these configurations associated with single time steps of cellular automaton evolution. Each cycle in the graph represents an "attractor" for the configurations corresponding to the nodes in trees rooted on it

the configurations is represented by iterated multiplication of their characteristic polynomials by fixed polynomials. Global properties of cellular automata are then determined by algebraic properties of these polynomials, by methods analogous to those used in the analysis of linear feedback shift registers [2, 3]. Despite their amenability to algebraic analysis, additive cellular automata exhibit many of the complex features of general cellular automata.

Having introduced notation in Sect. 2, Sect. 3 develops algebraic techniques for the analysis of cellular automata in the context of the simple cellular automaton illustrated in Fig. 1. Some necessary mathematical results are reviewed in the appendices. Section 4 then derives general results for all additive cellular automata. The results allow more than two possible values per site, but are most complete when the number of possible values is prime. They also allow influence on the evolution of a site from sites more distant than its nearest neighbours. The results are extended in Sect. 4D to allow cellular automata in which the sites are arranged in a square or cubic lattice in two, three or more dimensions, rather than

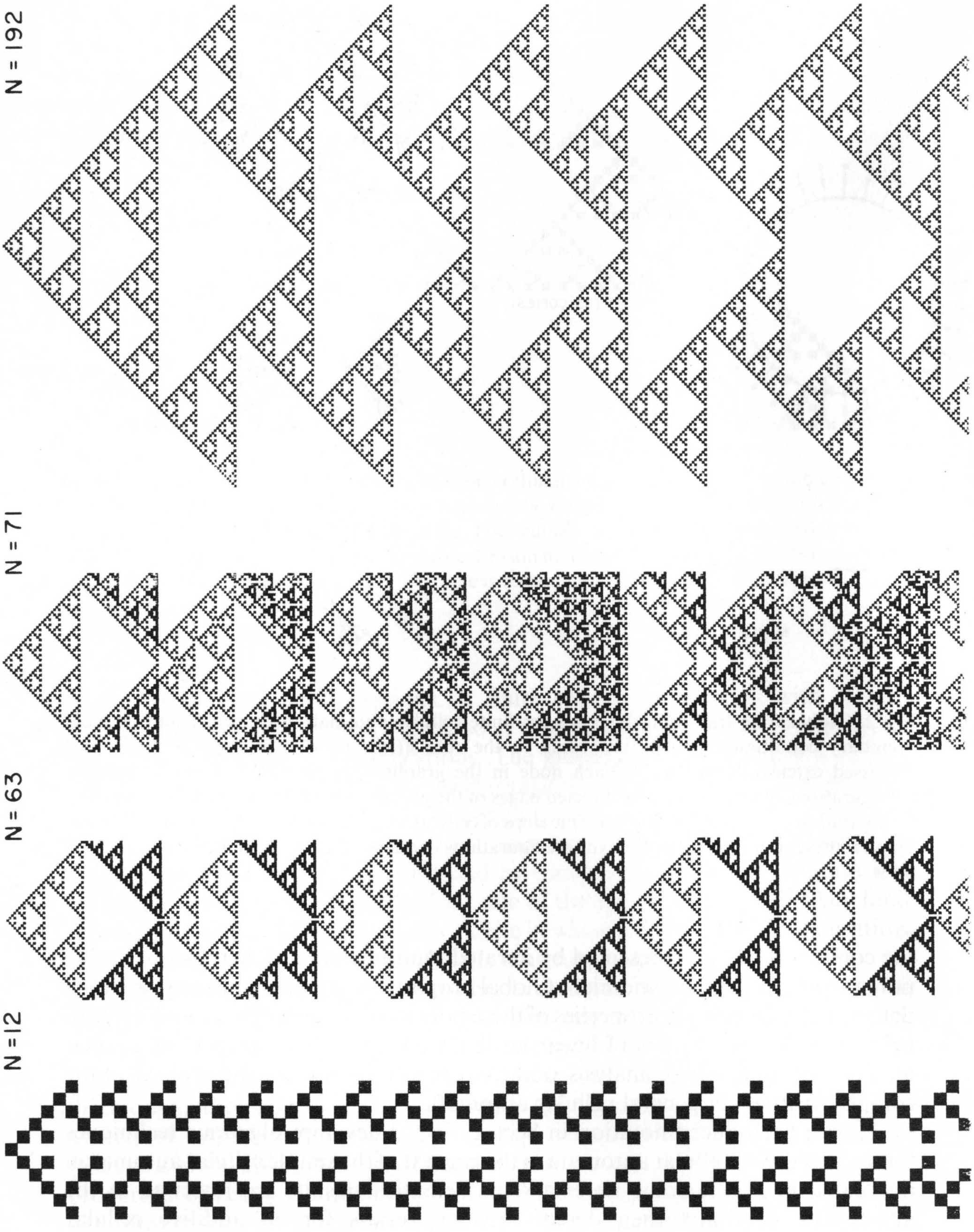

Fig. 3. Evolution of cellular automata with N sites arranged in a circle (periodic boundary conditions) according to the rule $\mathbb{T}(x) = x + x^{-1}$ (as used in Fig. 1 and discussed in Sect. 3). Finite cellular automata such as these ultimately enter cycles in which a sequence of configurations are visited repeatedly. This behaviour is evident here for $N = 12$, 63, and 192. For $N = 71$, the cycle has length $2^{35} - 1$

just on a line. Section 4E then discusses generalizations in which the cellular automaton time evolution rule involves several preceding time steps. Section 4F considers alternative boundary conditions. In all cases, a characterization of the global structure of the state transition diagram is found in terms of algebraic properties of the polynomials representing the cellular automaton time evolution rule.

Section 5 discusses non-additive cellular automata, for which the algebraic techniques of Sects. 3 and 4 are inapplicable. Combinatorial methods are nevertheless used to derive some results for a particular example.

Section 6 gives a discussion of the results obtained, comparing them with those for other systems.

2. Formalism

We consider first the formalism for one-dimensional cellular automata in which the evolution of a particular site depends on its own value and those of its nearest neighbours. Section 4 generalizes the formalism to several dimensions and more neighbours.

We take the cellular automaton to consist of N sites arranged around a circle (so as to give periodic boundary conditions). The values of the sites at time step t are denoted $a_0^{(t)}, \ldots, a_{N-1}^{(t)}$. The possible site values are taken to be elements of a finite commutative ring $\mathbb{R}_k$ with k elements. Much of the discussion below concerns the case $\mathbb{R}_k = \mathbb{Z}_k$, in which site values are conveniently represented as integers modulo k. In the example considered in Sect. 3, $\mathbb{R}_k = \mathbb{Z}_2$, and each site takes on a value 0 or 1.

The complete configuration of a cellular automaton is specified by the values of its N sites, and may be represented by a characteristic polynomial (generating function) (cf. [2, 3])

$$A^{(t)}(x) = \sum_{i=0}^{N-1} a_i^{(t)} x^i , \tag{2.1}$$

where the value of site i is the coefficient of x^i, and all coefficients are elements of the ring $\mathbb{R}_k$. We shall often refer to configurations by their corresponding characteristic polynomials.

It is often convenient to consider generalized polynomials containing both positive and negative powers of x: such objects will be termed "dipolynomials". In general, $H(x)$ is a dipolynomial if there exists some integer m such that $x^m H(x)$ is an ordinary polynomial in x. As discussed in Appendix A, dipolynomials possess divisibility and congruence properties analogous to those of ordinary polynomials.

Multiplication of a characteristic polynomial $A(x)$ by $x^{\pm j}$ yields a dipolynomial which represents a configuration in which the value of each site has been transferred (shifted) to a site j places to its right (left). Periodic boundary conditions in the cellular automaton are implemented by reducing the characteristic dipolynomial modulo the fixed polynomial $x^N - 1$ at all stages, according to

$$\sum_i a_i x^i \bmod (x^N - 1) = \sum_{i=0}^{N-1} \left(\sum_j a_{i+jN} \right) x^i . \tag{2.2}$$

Note that any dipolynomial is congruent modulo $(x^N - 1)$ to a unique ordinary polynomial of degree less than N.

In general, the value $a_i^{(t)}$ of a site in a cellular automaton is taken to be an arbitrary function of the values $a_{i-1}^{(t-1)}$, $a_i^{(t-1)}$, and $a_{i+1}^{(t-1)}$ at the previous time step. Until Sect. 5, we shall consider a special class of "additive" cellular automata which evolve with time according to simple linear combination rules of the form (taking the site index i modulo N)

$$a_i^{(t)} = \alpha_{-1} a_{i-1}^{(t-1)} + \alpha_0 a_i^{(t-1)} + \alpha_{+1} a_{i+1}^{(t-1)}, \tag{2.3}$$

where the α_j are fixed elements of $\mathbb{R}_k$, and all arithmetic is performed in $\mathbb{R}_k$. This time evolution may be represented by multiplication of the characteristic polynomial by a fixed dipolynomial in x,

$$\mathbb{T}(x) = \alpha_{-1} x + \alpha_0 + \alpha_{+1} x^{-1}, \tag{2.4}$$

according to

$$A^{(t)}(x) \equiv \mathbb{T}(x) A^{(t-1)}(x) \quad \bmod (x^N - 1), \tag{2.5}$$

where arithmetic is again performed in $\mathbb{R}_k$. Additive cellular automata obey an additive superposition principle which implies that the configuration obtained by evolution for t time steps from an initial configuration $A^{(0)}(x) + B^{(0)}(x)$ is identical to $A^{(t)}(x) + B^{(t)}(x)$, where $A^{(t)}(x)$ and $B^{(t)}(x)$ are the results of separate evolution of $A^{(0)}(x)$ and $B^{(0)}(x)$, and all addition is performed in $\mathbb{R}_k$. Since any initial configuration can be represented as a sum of "basis" configurations $\Delta(x) = x^j$ containing single nonzero sites with unit values, the additive superposition principle determines the evolution of all configurations in terms of the evolution of $\Delta(x)$. By virtue of the cyclic symmetry between the sites it suffices to consider the case $j = 0$.

3. A Simple Example

A. Introduction

This section introduces algebraic techniques for the analysis of additive cellular automata in the context of a specific simple example. Section 4 applies the techniques to more general cases. The mathematical background is outlined in the appendices.

The cellular automaton considered in this section consists of N sites arranged around a circle, where each site has value 0 or 1. The sites evolve so that at each time step the value of a site is the sum modulo two of the values of its two nearest neighbours at the previous time step:

$$a_i^{(t)} = a_{i-1}^{(t-1)} + a_{i+1}^{(t-1)} \quad \bmod 2. \tag{3.1}$$

This rule yields in many respects the simplest non-trivial cellular automaton. It corresponds to rule 90 of [1], and has been considered in several contexts elsewhere (e.g. [4]).

The time evolution (3.1) is represented by multiplication of the characteristic polynomial for a configuration by the dipolynomial

$$\mathbb{T}(x) = x + x^{-1} \tag{3.2}$$

according to Eq. (2.5). At each time step, characteristic polynomials are reduced modulo $x^N - 1$ (which is equal to $x^N + 1$ since all coefficients are here, and throughout this section, taken modulo two). This procedure implements periodic boundary conditions as in Eq. (2.2) and removes any inverse powers of x.

Equation (3.2) implies that an initial configuration containing a single nonzero site evolves after t time steps to a configuration with characteristic dipolynomial

$$\mathbb{T}(x)^t 1 = (x + x^{-1})^t = \sum_{i=0}^{t} \binom{t}{i} x^{2i-t}. \tag{3.3}$$

For $t < N/2$ (before "wraparound" occurs), the region of nonzero sites grows linearly with time, and the values of sites are given simply by binomial coefficients modulo two, as discussed in [1] and illustrated in Fig. 1. (The positions of nonzero sites are equivalently given by $\pm 2^{j_1} + 2^{j_2} \pm \ldots$, where the j_i give the positions of nonzero digits in the binary decomposition of the integer t.) The additive superposition property implies that patterns generated from initial configurations containing more than one nonzero site may be obtained by addition modulo two (exclusive disjunction) of the patterns (3.3) generated from single nonzero sites.

B. Irreversibility

Every configuration in a cellular automaton has a unique successor in time. A configuration may however have several distinct predecessors, as illustrated in the state transition diagram of Fig. 2. The presence of multiple predecessors implies that the time evolution mapping is not invertible but is instead "contractive". The cellular automaton thus exhibits irreversible behaviour in which information on initial states is lost through time evolution. The existence of configurations with multiple predecessors implies that some configurations have no predecessors[1]. These configurations occur only as initial states, and may never be generated in the time evolution of the cellular automaton. They appear on the periphery of the state transition diagram of Fig. 2. Their presence is an inevitable consequence of irreversibility and of the finite number of states.

Lemma 3.1. *Configurations containing an odd number of sites with value* 1 *can never be generated in the evolution of the cellular automaton defined in Sect. 3A, and can occur only as initial states.*

Consider any configuration specified by characteristic polynomial $A^{(0)}(x)$. The successor of this configuration is $A^{(1)}(x) = \mathbb{T}(x)A^{(0)}(x) = (x + x^{-1})A^{(0)}(x)$, taken, as always, modulo $x^N - 1$. Thus

$$A^{(1)}(x) = (x^2 + 1)B(x) + R(x)(x^N - 1)$$

for some dipolynomials $R(x)$ and $B(x)$. Since $x^2 + 1 = x^N - 1 = 0$ for $x = 1$, $A^{(1)}(1) = 0$. Hence $A^{(1)}(x)$ contains an even number of terms, and corresponds to a configuration with an even number of nonzero sites. Only such configurations can therefore be reached from some initial configuration $A^{(0)}(x)$.

An extension of this lemma yields the basic theorem on the number of unreachable configurations:

---

1 Such configurations have been termed "Gardens of Eden" [5]

Theorem 3.1. *The fraction of the 2^N possible configurations of a size N cellular automaton defined in Sect. 3A which can occur only as initial states, and cannot be reached by evolution, is* 1/2 *for N odd and* 3/4 *for N even.*

A configuration $A^{(1)}(x)$ is reachable after one time step of cellular automaton evolution if and only if for some dipolynomial $A^{(0)}(x)$,

$$A^{(1)}(x) \equiv \mathbb{T}(x)A^{(0)}(x) \equiv (x+x^{-1})A^{(0)}(x) \quad \mathrm{mod}(x^N-1), \tag{3.4}$$

so that

$$A^{(1)}(x) = (x^2+1)B(x) + R(x)(x^N-1) \tag{3.5}$$

for some dipolynomials $R(x)$ and $B(x)$. To proceed, we use the factorization of (x^N-1) given in Eq. (A.7), and consider the cases N even and N odd separately.

(a) N even. Since by Eq. (A.4), $(x^2+1)=(x+1)^2=(x-1)^2$ (taken, as always, modulo 2), and by Eq. (A.7),

$$(x-1)^2 \mid (x^{N/2}-1)^2 = (x^N-1)$$

for even N, Eq. (3.5) shows that

$$(x-1)^2 \mid A^{(1)}(x)$$

in this case. But since $(x-1)^2$ contains a constant term, $A^{(1)}(x)/(x-1)^2$ is thus an ordinary polynomial if $A^{(1)}(x)$ is chosen as such. Hence all reachable configuratons represented by a polynomial $A^{(1)}(x)$ are of the form

$$A^{(1)}(x) = (x-1)^2 C(x),$$

for some polynomial $C(x)$. The predecessor of any such configuration is $xC(x)$, so any configuration of this form may in fact be reached. Since $\deg A(x) < N$, $\deg C(x) < N-2$. There are thus exactly 2^{N-2} reachable configurations, or 1/4 of all the 2^N possible configurations.

(b) N odd. Using Lemma 3.1 the proof for this case is reduced to showing that all configurations containing an even number of nonzero sites have predecessors. A configuration $A^{(1)}(x)$ with an even number of nonzero sites can always be written in the form $(x+1)D(x)$. But

$$\begin{aligned} A^{(1)}(x) = (x+1)D(x) &\equiv (x+x^{-1})(x^2+x^4+ \dots +x^{N-1})D(x) \quad \mathrm{mod}(x^N-1) \\ &\equiv \mathbb{T}(x)(x^2+x^4+ \dots +x^{N-1})D(x) \quad \mathrm{mod}(x^N-1), \end{aligned}$$

giving an explicit predecessor for $A^{(1)}(x)$.

The additive superposition principle for the cellular automaton considered in this section yields immediately the result:

Lemma 3.2. *Two configurations $A^{(0)}(x)$ and $B^{(0)}(x)$ yield the same configuration $C(x) \equiv \mathbb{T}(x)A^{(0)}(x) \equiv \mathbb{T}(x)B^{(0)}$ after one time step in the evolution of the cellular automaton defined in Sect. 3A if and only if $A^{(0)}(x) = B^{(0)}(x) + Q(x)$, where $\mathbb{T}(x)Q(x) \equiv 0$.*

Theorem 3.2. *Configurations in the cellular automaton defined in Sect. 3A which have at least one predecessor have exactly two predecessors for N odd and exactly four for N even.*

This theorem is proved using Lemma 3.2 by enumeration of configurations $Q(x)$ which evolve to the null configuration after one time step. For N odd, only the configurations 0 and $1+x+\ldots+x^{N-1}=\frac{x^N-1}{x-1}$ (corresponding to site values 11111 ...) have this property. For N even, $Q(x)$ has the form

$$(1+x^2+\ldots+x^{N-2})S_i(x)=\frac{x^N-1}{x^2-1}S_i(x),$$

where the $S_i(x)$ are the four polynomials of degree less than two. Explicitly, the possible forms for $Q(x)$ are 0, $1+x^2+\ldots+x^{N-2}$, $x+x^3+\ldots+x^{N-1}$, and $1+x+x^2+\ldots+x^{N-1}$.

C. Topology of the State Transition Diagram

This subsection derives topological properties of the state transition diagrams illustrated in Fig. 2. The results determine the amount and rate of "information loss" or "self organization" associated with the irreversible cellular automaton evolution.

The state transition network for a cellular automaton is a graph, each of whose nodes represents one of the possible cellular automaton configurations. Directed arcs join the nodes to represent the transitions between cellular automaton configurations at each time step. Since each cellular automaton configuration has a unique successor, exactly one arc must leave each node, so that all nodes have out-degree one. As discussed in the previous subsection, cellular automaton configurations may have several or no predecessors, so that the in-degrees of nodes in the state transition graph may differ. Theorems 3.1 and 3.2 show that for N odd, 1/2 of all nodes have zero in-degree and the rest have in-degree two, while for N even, 3/4 have zero in-degree and 1/4 in-degree four.

As mentioned in Sect. 1, after a possible "transient", a cellular automaton evolving from any initial configuration must ultimately enter a loop, in which a sequence of configurations are visited repeatedly. Such a loop is represented by a cycle in the state transition graph. At every node in this cycle a tree is rooted; the transients consist of transitions leading towards the cycle at the root of the tree.

Lemma 3.3. *The trees rooted at all nodes on all cycles of the state transition graph for the cellular automaton defined in Sect. 3A are identical.*

This result is proved by showing that trees rooted on all cycles are identical to the tree rooted on the null configuration. Let $A(x)$ be a configuration which evolves to the null configuration after exactly t time steps, so that $\mathbb{T}(x)^t A(x) \equiv 0 \bmod (x^N-1)$. Let $R(x)$ be a configuration on a cycle, and let $R^{(-t)}(x)$ be another configuration on the same cycle, such that $\mathbb{T}(x)^t R^{(-t)}(x) \equiv R(x) \bmod (x^N-1)$. Then define

$$\Psi_{R(x)}[A(x)]=A(x)+R^{(-t)}(x).$$

We first show that as $A(x)$ ranges over all configurations in the tree rooted on the null configuration, $\Psi_{R(x)}[A(x)]$ ranges over all configurations in the tree rooted at $R(x)$. Since

$$\mathbb{T}(x)^t\Psi_{R(x)}[A(x)]=\mathbb{T}(x)^tA(x)+\mathbb{T}(x)^tR^{(-t)}(x)\equiv R(x) \quad \bmod (x^N-1),$$

it is clear that all configurations $\Psi_{R(x)}[A(x)]$ evolve after t time steps [where the value of t depends on $A(x)$] to $R(x)$. To show that these configurations lie in the tree rooted at $R(x)$, one must show that their evolution reaches no other cycle configurations for any $s<t$. Assume this supposition to be false, so that there exists some $m \neq 0$ for which

$$R^{(-m)}(x) \equiv \mathbb{T}(x)^s \Psi_{R(x)}[A(x)] = \mathbb{T}(x)^s A(x) + R^{(s-t)}(x) \qquad \mathrm{mod}(x^N - 1).$$

Since $\mathbb{T}(x)^t A(x) \equiv 0 \,\mathrm{mod}(x^N - 1)$, this would imply $R^{(t-s-m)}(x) = R^{(0)}(x) = R(x)$, or $R^{(-m)}(x) = R^{(s-t)}(x)$. But $R^{(-m)}(x) - R^{(s-t)}(x) \equiv \mathbb{T}(x)^s A(x)$, and by construction $\mathbb{T}(x)^s A(x) \neq 0$ for any $s<t$, yielding a contradiction. Thus $\Psi_{R(x)}$ maps configurations at height t in the tree rooted on the null configuration to configurations at height t in the tree rooted at $R(x)$, and the mapping Ψ is one-to-one. An analogous argument shows that Ψ is onto. Finally one may show that Ψ preserves the time evolution structure of the trees, so that if $\mathbb{T}(x) A^{(0)}(x) = A^{(1)}(x)$, then

$$\mathbb{T}(x) \Psi_{R(x)}[A^{(0)}(x)] = \Psi_{R(x)}[A^{(1)}(x)],$$

which follows immediately from the definition of Ψ. Hence Ψ is an isomorphism, so that trees rooted at cycle configurations are all isomorphic to that rooted at the null configuration.

Notice that this proof makes no reference to the specific form (3.2) chosen for $\mathbb{T}(x)$ in this section; Lemma 3.3 thus holds for any additive cellular automaton.

Theorem 3.3. *For N odd, a tree consisting of a single arc is rooted at each node on each cycle in the state transition graph for the cellular automaton defined in Sect. 3A.*

By virtue of Lemma 3.3, it suffices to show that the tree rooted on the null configuration consists of a single node corresponding to the configuration 111 ... 111. This configuration has no predecessors by virtue of Lemma 3.1.

Corollary. *For N odd, the fraction of the 2^N possible configurations which may occur in the evolution of the cellular automaton defined in Sect. 3A is $1/2$ after one or more time steps.*

The "distance" between two nodes in a tree is defined as the number of arcs which are visited in traversing the tree from one node to the other (e.g. [6]). The "height" of a (rooted) tree is defined as the maximum number of arcs traversed in a descent from any leaf or terminal (node with zero in-degree) to the root of the tree (formally node with zero out-degree). A tree is "balanced" if all its leaves are at the same distance from its root. A tree is termed "quaternary" ("binary") if each of its non-terminal nodes has in-degree four (two).

Let $D_2(N)$ be the maximum 2^j which divides N (so that for example $D_2(12) = 4$).

Theorem 3.4. *For N even, a balanced tree with height $D_2(N)/2$ is rooted at each node on each cycle in the state transition graph for the cellular automaton defined in Sect. 3A; the trees are quaternary, except that their roots have in-degree three.*

Theorem 3.2 shows immediately that the tree is quaternary. In the proof of Theorem 3.1, we showed that a configuration $Q_1(x)$ can be reached from some configuration $Q_0(x)$ if and only if $(1+x^2)|Q_1(x)$; Theorem 3.2 then shows that if $Q_1(x)$ is reachable, it is reachable from exactly four distinct configurations $Q_0(x)$. We now extend this result to show that a configuration $Q_m(x)$ can be reached from some configuration $Q_0(x)$ by evolution for m time steps, with $m \leqq D_2(N)/2$, if and only if $(1+x^2)^m|Q_m(x)$. To see this, note that if

$$Q_m(x) \equiv \mathbb{T}(x)^m Q_0(x) \quad \mod(x^N-1), \tag{3.6}$$

then

$$(x^N-1) \mid Q_m(x) + (x^2+1)^m x^{N-m} Q_0(x), \tag{3.7}$$

and so, since by Eq. (A.7), $(x^2+1)^m|(x^N-1)$ for $m \leqq D_2(N)/2$, it follows that

$$(x^2+1)^m \mid Q_m(x) \tag{3.8}$$

for $m \leqq D_2(N)/2$. On the other hand, if $(x^2+1)^m|Q_m(x)$, say $Q_m(x)=(x^2+1)^m Q_0(x)$, then $Q_m(x) \equiv \mathbb{T}(x)^m x^m Q_0(x)$, which shows that $Q_m(x)$ is reachable in m steps. The balance of the trees is demonstrated by showing that for $m < D_2(N)/2$, if $(x^2+1)^m|Q_m(x)$, then $Q_m(x)$ can be reached from exactly 4^m initial configurations $Q_0(x)$. This may be proved by induction on m. If

$$(1+x^2)^m \mid Q_m(x) \quad (1 \leqq m < D_2(N)/2),$$

then all of the four states $Q_{m-1}(x)$ from which $Q_m(x)$ may be reached in one step satisfy $(x^2+1)^{m-1}|Q_{m-1}(x)$. Consider now the configurations $Q(x)$ which satisfy

$$(x^2+1)^{D_2(N)/2} \mid Q(x). \tag{3.9}$$

If we write $Q(x)=(x+1)^{D_2(N)}R(x)$, then as in Theorem 3.2, the four predecessors of $Q(x)$ are exactly

$$Q_{-1}(x)=(x+1)^{D_2(N)-2}R^*(x)+\left(\frac{x^{N/2}-1}{x-1}\right)^2 S_i(x), \tag{3.10}$$

where $xR(x) \equiv R^*(x) \mod(x^N-1)$. $S_i(x)$ ranges over the four polynomials of degree less than two, as in Theorem 3.2. Exactly one of these polynomials satisfies Eq. (3.9), whereas the other three satisfy only

$$(x+1)^{D_2(N)-2} \mid Q_{-1}(x).$$

Any state satisfying Eq. (3.9) thus belongs to a cycle, since it can be reached after an arbitrary number of steps. Conversely, since any cycle configuration must be reachable after $D_2(N)/2$ time steps, any and all configurations $Q_{-1}(x)$ satisfying Eq. (3.9) are indeed on cycles. But, as shown above, the three $Q_{-1}(x)$ which do not satisfy Eq. (3.9) are roots of balanced quaternary trees of height $D_2(N)/2$–1. The proof of the theorem is thus completed.

Corollary. *For N even, a fraction* 4^{-t} *of the* 2^N *possible configurations appear after t steps in the evolution of the cellular automaton defined in Sect. 3A for* $t \leqq D_2(N)/2$. *A fraction* $2^{-D_2(N)}$ *of the configurations occur in cycles, and are therefore generated at arbitrarily large times.*

Corollary. *All configurations* $A(x)$ *on cycles in the cellular automaton of Sect. 3A are divisible by* $(1+x)^{D_2(N)}$.

This result follows immediately from the proof of Theorems 3.3 and 3.4.

Entropy may be used to characterize the irreversibility of cellular automaton evolution (cf. [1]). One may define a set (or topological) entropy for an ensemble of configurations i occurring with probabilities p_i according to

$$s=\frac{1}{N}\log_2\sum_i\theta(p_i)\,, \tag{3.11}$$

where $\theta(p)=1$ for $p>0$, and 0 otherwise. One may also define a measure entropy

$$s_\mu=-\frac{1}{N}\sum_i p_i\log_2 p_i\,. \tag{3.12}$$

For a maximal entropy ensemble in which all 2^N possible cellular automaton configurations occur with equal probabilities,

$$s=s_\mu=1\,.$$

These entropies decrease in irreversible cellular automaton evolution, as the probabilities for different configurations become unequal. However, the balance property of the state transition trees implies that configurations either do not appear, or occur with equal nonzero probabilities. Thus the set and measure entropies remain equal in the evolution of the cellular automaton of Sect. 3A. Starting from a maximal entropy ensemble, both nevertheless decrease with time t according to

$$s(t)=s_\mu(t)=1-2t/N\,,\qquad 0\leqq t\leqq D_2(N)/2\,,$$
$$s(t)=s_\mu(t)=1-D_2(N)/N\,,\qquad t\geqq D_2(N)/2\,.$$

D. Maximal Cycle Lengths

Lemma 3.4. *The lengths of all cycles in a cellular automaton of size N as defined in Sect. 3A divide the length Π_N of the cycle obtained with an initial configuration containing a single site with value one.*

This follows from additivity, since any configuration can be considered as a superposition of configurations with single nonzero initial sites.

Lemma 3.5. *For the cellular automaton defined in Sect. 3A, with N of the form 2^j, $\Pi_N=1$.*

In this case, any initial configuration evolves ultimately to a fixed point consisting of the null configuration, since

$$(x+x^{-1})^{2^j}1\equiv(x^{2^j}+x^{-2^j})\equiv(x^N+x^{-N})\equiv 0\qquad \mathrm{mod}(x^N-1)\,.$$

Lemma 3.6. *For the cellular automaton defined in Sect. 3A, with N even but not of the form 2^j, $\Pi_N=2\,\Pi_{N/2}$.*

A configuration $A(x)$ appears in a cycle of length π if and only if

$$\mathbb{T}(x)^\pi A(x)\equiv A(x)\qquad \mathrm{mod}(x^N-1)\,,$$

and therefore

$$(x^N-1)\,|\,[(x^2+1)^\pi+x^\pi]A(x)\,.$$

After t time steps, the configuration obtained by evolution from an initial state containing a single nonzero site is $(x+x^{-1})^t$; by Theorems 3.3 and 3.4 and the additive superposition principle, the configuration

$$A(x)\equiv(x+x^{-1})^{D_2(N)/2}$$

is therefore on the maximal length cycle. Thus the maximal period Π_N is given by the minimum π for which

$$(x^N-1)\,|\,[(x^2+1)^\pi+x^\pi]\,(x+1)^{D_2(N)}\,,$$

and so

$$\left(\frac{x^n-1}{x+1}\right)^{D_2(N)}\,|\,[(x^2+1)^{\Pi_N}+x^{\Pi_N}]\,, \tag{3.13}$$

with $N=D_2(N)n$, n odd. Similarly,

$$\begin{gathered}(x^{N/2}-1)\,|\,[(x^2+1)^{\Pi_{N/2}}+x^{\Pi_{N/2}}]\,(x+1)^{D_2(N/2)}\,,\\ \left(\frac{x^n-1}{x+1}\right)^{D_2(N)/2}\,|\,[(x^2+1)^{\Pi_{N/2}}+x^{\Pi_{N/2}}]\,.\end{gathered} \tag{3.14}$$

Squaring this yields

$$\left(\frac{x^n-1}{x+1}\right)^{D_2(N)}\,|\,[(x^2+1)^{2\Pi_{N/2}}+x^{2\Pi_{N/2}}]\,,$$

from which it follows that

$$\Pi_N\,|\,2\Pi_{N/2}\,. \tag{3.15}$$

Since x^N-1 divides $[(x^2+1)^{\Pi_N}+x^{\Pi_N}]\,(x+1)^{D_2(N)}$, so does its square root, $x^{N/2}-1$, and therefore

$$\Pi_{N/2}\,|\,\Pi_N\,. \tag{3.16}$$

Combining Eqs. (3.15) and (3.16) implies that either $\Pi_N=2\Pi_{N/2}$ or $\Pi_N=\Pi_{N/2}$. To exclude the latter possibility, we use derivatives. Using Eq. (A.6), and the fact that the derivative of x^2+1 vanishes over $GF(2)$, one obtains from (3.13),

$$\left(\frac{x^n-1}{x+1}\right)\,|\,\Pi_N x^{\Pi_N-1}\,.$$

If Π_N were odd, the right member would be non-trivial, and the divisibility condition could not hold. Thus Π_N must be even. But then the right member of (3.13) is a perfect square, so that

$$\left(\frac{x^{N/2}-1}{(x+1)^{D_2(N)/2}}\right)^2\,|\,[(x^2+1)^{\Pi_N/2}+x^{\Pi_N/2}]^2\,.$$

Thus $\Pi_{N/2}|\Pi_N/2$, and the proof is complete.

Theorem 3.5. *For the cellular automaton defined in Sect. 3A, with N odd,* $\Pi_N|\Pi_N^* = 2^{\mathrm{sord}_N(2)} - 1$ *where* $\mathrm{sord}_N(2)$ *is the multiplicative "sub-order" function of* 2 *modulo N, defined as the least integer j such that* $2^j = \pm 1 \bmod N$. *(Properties of the suborder functions are discussed in Appendix B.)*

By Lemma 3.1, an initial configuration containing a single nonzero site cannot be reached in cellular automaton evolution. The configuration $(x+x^{-1}) \bmod (x^N - 1)$ obtained from this after one time step can be reached, and in fact appears again after $2^{\mathrm{sord}_N(2)} - 1$ time steps, since

$$\begin{aligned}\mathbb{T}(x)^{2^{\mathrm{sord}_N(2)}}1 &\equiv (x+x^{-1})^{2^{\mathrm{sord}_N(2)}} \equiv (x^{2^{\mathrm{sord}_N(2)}} + x^{-2^{\mathrm{sord}_N(2)}}) \\ &\equiv (x^{\pm 1} + x^{\mp 1}) \equiv (x+x^{-1}) \qquad \bmod (x^N - 1).\end{aligned}$$

The maximal cycle lengths Π_N for the cellular automaton considered in this section are given in the first column of Table 1. The values are plotted as a function of N in Fig. 4. Table 1 together with Table 4 show that $\Pi_N = \Pi_N^*$ for almost all odd N. The first exception appears for $N=37$, where $\Pi_N = \Pi_N^*/3$; subsequent exceptions are $\Pi_{95} = \Pi_{95}^*/3$, $\Pi_{101} = \Pi_{101}^*/3$, $\Pi_{141} = \Pi_{141}^*/3$, $\Pi_{197} = \Pi_{197}^*/3$, $\Pi_{199} = \Pi_{199}^*/7$, $\Pi_{203} = \Pi_{203}^*/105$ and so on.

As discussed in Appendix B, $\mathrm{sord}_N(2) \leqq (N-1)/2$. This bound can be attained only when N is prime. It implies that the maximal period is $2^{(N-1)/2} - 1$. Notice that this period is the maximum that could be attained with any reflection symmetric initial configuration (such as the single nonzero site configuration to be considered by virtue of Lemma 3.4).

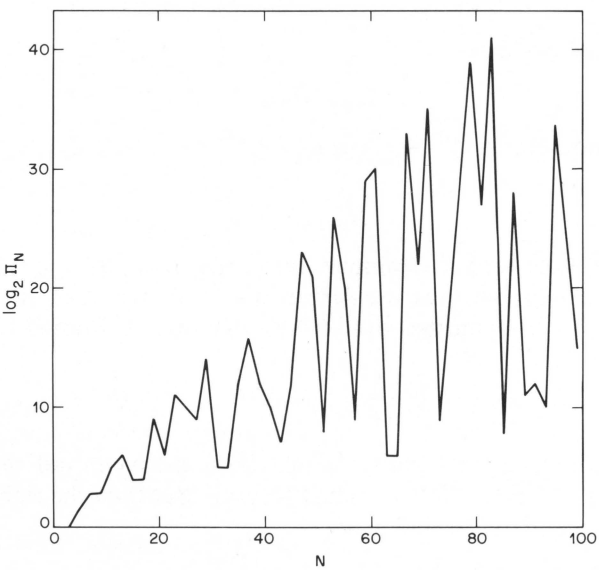

Fig. 4. The maximal length Π_N of cycles generated in the evolution of a cellular automaton with size N and $\mathbb{T}(x) = x + x^{-1}$, as a function of N. Only values for integer N are plotted. The irregular behaviour of Π_N as a function of N is a consequence of the dependence of Π_N on number theoretical properties of N

Table 1. Maximal cycle lengths Π_N for one-dimensional nearest-neighbour additive cellular automata with size N and k possible values at each site. Results for all possible nontrivial symmetrical rules with $k \leqq 4$ are given. For $k=2$, the fixed time evolution polynomials are $\mathbb{T}(x)=x+x^{-1}$ and $x+1+x^{-1}$ (corresponding to rules 90 and 150 of [1], respectively). For $k=3$, the polynomials are $x+x^{-1}$, $x+1+x^{-1}$, and $x+2+x^{-1}$, while for $k=4$, they are $x+x^{-1}$, $x+1+x^{-1}$, $x+2+x^{-1}$, and $x+3+x^{-1}$

N	$k=2$		$k=3$			$k=4$			
3	1	1	6	1	3	2	2	1	1
4	1	2	2	2	2	1	4	1	4
5	3	3	8	8	4	6	6	3	6
6	2	1	6	6	3	2	2	2	2
7	7	7	26	26	13	14	14	7	14
8	1	4	4	8	8	1	8	1	8
9	7	7	18	1	9	14	14	7	14
10	6	6	8	8	8	6	12	6	12
11	31	31	242	121	121	62	62	31	62
12	4	2	6	6	6	4	4	4	4
13	63	21	26	13	13	126	42	63	42
14	14	14	26	26	13	14	28	14	28
15	15	15	24	24	12	30	30	15	30
16	1	8	16	80	80	1	16	1	16
17	15	15	1,640	6,560	820	30	30	15	30
18	14	14	18	18	9	14	28	14	28
19	511	511	19,682	19,682	9,841	1,022	1,022	511	1,022
20	12	12	16	40	40	12	24	12	24
21	63	63	78	78	39	126	126	63	126
22	62	62	242	242	242	62	124	62	124
23	2,047	2,047	177,146	88,573	88,573	4,094	4,094	2,047	4,094
24	8	4	12	24	24	8	8	8	8
25	1,023	1,023	59,048	59,048	29,524	2,046	2,046	1,023	2,046
26	126	42	26	26	26	126	84	126	84
27	511	511	54	1	27	1,022	1,022	511	1,022
28	28	28	26	26	26	28	56	28	56
29	16,383	16,383	4,782,968	4,782,968	2,391,484	32,766	32,766	16,383	32,766
30	30	30	24	24	24	30	60	30	60
31	31	31	1,103,762	14,348,906	551,881	62	62	31	62
32	1	16	160	6,560	6,560	1	32	1	32
33	31	31	726	363	363	62	62	31	62
34	30	30	1,640	6,560	6,560	30	60	30	60
35	4,095	4,095	265,720	265,720	132,860	8,190	8,190	4,095	8,190
36	28	28	18	18	18	28	56	28	56
37	87,381	29,127	19,682	19,682	9,841	174,762	58,254	87,381	58,254
38	1,022	1,022	19,682	19,682	9,841	1,022	2,044	1,022	2,044
39	4,095	4,095	78	39	39	8,190	8,190	4,095	8,190
40	24	24	80	40	40	24	48	24	48

E. Cycle Length Distribution

Lemma 3.4 established that all cycle lengths must divide Π_N and Theorems 3.3 and 3.4 gave the total number of states in cycles. This section considers the number of distinct cycles and their lengths.

Lemma 3.7. *For the cellular automaton defined in Sect. 3A, with N a multiple of* 3, *there are four distinct fixed points (cyles of length one); otherwise, only the null configuration is a fixed point.*

For $N=3n$, the only stationary configurations are 000000 ... (null configuration), 0110110..., 1011011 ..., and 1101101 ....

Table 2 gives the lengths and multiplicities of cycles in the cellular automaton defined in Sect. 3A, for various values of N. One result suggested by the table is that the multiplicity of cycles for a particular N increases with the length of the cycle, so that for large N, an overwhelming fraction of all configurations in cycles are on cycles with the maximal length.

When Π_N is prime, the only possible cycle lengths are Π_N and 1. Then, using Lemma 3.7, the number of cycles of length Π_N is $(2^{(N-1)}-4)/\Pi_N$ for $N=3n$, and is $(2^{(N-1)}-1)/\Pi_N$ otherwise.

When Π_N is not prime, cycles may exist with lengths corresponding to various divisors of Π_N. It has not been possible to express the lengths and multiplicities of cycles in this case in terms of simple functions. We nevertheless give a computationally efficient algorithm for determining them.

Theorems 3.3 and 3.4 show that any configuration $A(x)$ on a cycle may be written in the form

$$A(x)=(1+x)^{D_2(N)}B(x),$$

where $B(x)$ is some polynomial. The cycle on which $A(x)$ occurs then has a length given by the minimum π for which

$$\mathbb{T}(x)^\pi B(x)\equiv(x+x^{-1})^\pi B(x)\equiv B(x) \quad \bmod\left(\frac{x^n-1}{x+1}\right)^{D_2(N)}, \tag{3.17}$$

where $N=D_2(N)n$ with n odd, and $(x^n-1)^{D_2(N)}=x^N-1$. Using the factorization [given in Eq. (A.8)]

$$x^n-1=(x-1)\prod_{\substack{d\mid n\\ d\neq 1}}\ \prod_{i=1}^{\frac{\phi(d)}{\mathrm{ord}_d(2)}} C_{d,i}(x), \tag{3.18}$$

where the $C_{d,i}(x)$ are the irreducible cyclotomic polynomials over $\mathbb{Z}_2$ of degree $\mathrm{ord}_d(2)$, Eq. (3.17) can be rewritten as

$$(x+x^{-1})^\pi B(x)\equiv B(x) \quad \bmod C_{d,i}(x)^{D_2(N)} \tag{3.19}$$

for all $d\mid n$, $d\neq 1$, and for all i such that $1\leqq i\leqq\phi(d)/\mathrm{ord}_d(2)$. Let $\pi_{d,i}[B(x)]$ denote the smallest π for which (3.19) holds with given d, i. Then the length of the cycle on which $A(x)$ occurs is exactly the least common multiple of all the $\pi_{d,i}[B(x)]$. If $C_{d,i}(x)^{D_2(N)}\mid B(x)$, then clearly Eq. (3.19) holds for $\pi=1$, and $\pi_{d,i}[B(x)]=1$. If $C_{d,i}(x)^{r_{d,i}[B(x)]}\| B(x)$ (and $0\leqq r_{d,i}[B(x)]<D_2(N)$), then Eq. (3.19) is equivalent to

$$(x+x^{-1})^\pi\equiv 1 \quad \bmod C_{d,i}(x)^{D_2(N)-r_{d,i}[B(x)]}. \tag{3.20}$$

The values of $\pi_{d,i}$ for configurations with $r_{d,i}[B(x)]=s$ are therefore equal, and will be denoted $\pi_{d,i,s}$ $(0\leqq s\leqq D_2(N))$. Since $C_{d,i}(x)\mid(x^d-1)/(x+1)$ $(d\neq 1)$, the value of $\pi_{d,i,1}$ divides the minimum π for which $(x+x^{-1})^\pi\equiv 1 \bmod (x^d-1)/(x+1)$. This

Table 2. Multiplicities and lengths of cycles in the cellular automaton of Sect. 3A with size N. The notation $g_i \times \pi_i$ indicates the occurence of g_i distinct cycles each of length π_i. The last column of the table gives the total number of distinct cycles or "attractors" in the system

N		
3	4×1	4
4	1×1	1
5	1×1; 5×3	6
6	4×1; 6×2	10
7	1×1; 9×7	10
8	1×1	1
9	4×1; 36×7	40
10	1×1; 5×3; 40×6	46
11	1×1; 33×31	34
12	4×1; 6×2; 60×4	70
13	1×1; 65×63	66
14	1×1; 9×7; 288×14	298
15	4×1; 20×3; $1{,}088 \times 15$	1,112
16	1×1	1
17	1×1; 51×5; $4{,}352 \times 15$	4,404
18	4×1; 6×2;36×7; $4{,}662 \times 14$	4,708
19	1×1; 513×511	514
20	1×1; 5×3; 40×6; $5{,}440 \times 12$	5,486
21	4×1; 36×7; $16{,}640 \times 63$	16,680
22	1×1; 33×31; $16{,}896 \times 62$	16,930
23	1×1; $2{,}049 \times 2{,}047$	2,050
24	4×1; 6×2; 60×4; $8{,}160 \times 8$	8,230
25	1×1; 5×3; $16{,}400 \times 1{,}023$	16,406
26	1×1; 65×63; $133{,}120 \times 126$	133,186
27	4×1; 36×7; $131{,}328 \times 511$	131,368
28	1×1; 9×7; 288×14; $599{,}040 \times 28$	599,338
29	1×1; $16{,}385 \times 16{,}383$	16,386
30	4×1; 6×2; 20×3; 670×6; $1{,}088 \times 15$; $8{,}947{,}168 \times 30$	8,948,956
31	1×1; $34{,}636{,}833 \times 31$	34,636,834
32	1×1	1
33	4×1; $138{,}547{,}332 \times 31$	138,547,336
34	1×1; 51×5; $6{,}528 \times 10$; $4{,}352 \times 15$; $143{,}161{,}216 \times 30$	143,172,148
35	1×1; 5×3; 9×7; 45×21; $4{,}195{,}328 \times 4{,}095$	4,195,388
36	4×1; 6×2; 60×4; 36×7; $4{,}662 \times 14$; $153{,}389{,}340 \times 28$	153,394,108
37	1×1; $786{,}435 \times 87{,}381$	786,436
38	1×1; 513×511; $67{,}239{,}936 \times 1{,}022$	672,340,450
39	4×1; 260×63; $49{,}164 \times 1{,}365$; $67{,}108{,}860 \times 4{,}095$	67,158,288
40	1×1; 5×3; 40×6; $5{,}440 \times 12$; $178{,}954{,}240 \times 24$	178,959,726

equation is the same as the one for the maximal cycle length of a size d cellular automaton: the derivation of Theorem 3.5 then shows that

$$\pi_{d,i,1} \mid 2^{\mathrm{sord}_d(2)} - 1 . \tag{3.21}$$

It can also be shown that $\pi_{d,i,2s} = \pi_{d,i,s}$ or $\pi_{d,i,2s} = 2\pi_{d,i,s}$.

As an example of the procedure described above, consider the case $N=30$. Here,

$$x^{30}+1=(x^{15}+1)^2=C_{1,1}(x)^2C_{3,1}(x)^2C_{5,1}(x)^2C_{15,1}(x)^2C_{15,2}(x)^2, \quad (3.22)$$

where

$$\begin{aligned} C_{1,1}(x)&=x+1, \\ C_{3,1}(x)&=x^2+x+1, \\ C_{5,1}(x)&=x^4+x^3+x^2+x+1, \\ C_{15,1}(x)&=x^4+x+1, \\ C_{15,2}(x)&=x^4+x^3+1. \end{aligned}$$

Then

$$\begin{aligned} &\pi_{d,i,2}=1, \\ &\pi_{3,1,1}=1, \quad \pi_{3,1,0}=2, \\ &\pi_{5,1,1}=3, \quad \pi_{5,1,0}=6, \\ &\pi_{15,1,1}=\pi_{15,2,1}=15, \\ &\pi_{15,1,0}=\pi_{15,2,0}=30. \end{aligned} \quad (3.23)$$

Thus the cycles which occur in the case $N=30$ have lengths 1, 2, 3, 6, 15, and 30.

To determine the number of distinct cycles of a given length, one must find the number of polynomials $B(x)$ with each possible set of values $r_{d,i}[B(x)]$. This number is given by

$$\prod_{\substack{d|n \\ d\neq 1}} \prod_{i} V(r_{d,i}, d, D_2(N)),$$

where $V(D_2(N), d, D_2(N))=1$ and

$$V(r, d, D_2(N))=2^{\mathrm{ord}_d(2)(D_2(N)-r)}-2^{\mathrm{ord}_d(2)(D_2(N)-r-1)}$$

for $0 \leqq r < D_2(N)$. The cycle lengths of these polynomials are determined as above by the least common multiple of the $\pi_{d,i,r_{d,i}}$.

In the example $N=30$ discussed above, one finds that configurations on cycles of length 3 have $(r_{3,1}, r_{5,1}, r_{15,1}, r_{15,2})=(1,1,2,2)$ or $(2,1,2,2)$, implying that 60 such configurations exist, in 20 distinct cycles.

4. Generalizations

A. Enumeration of Additive Cellular Automata

We consider first one-dimensional additive cellular automata, whose configurations may be represented by univariate characteristic polynomials. We assume that the time evolution of each site depends only on its own value and the value of its two nearest neighbours, so that the time evolution dipolynomial $\mathbb{T}(x)$ is at most of degree two. Cyclic boundary conditions on N sites are implemented by reducing the characteristic polynomial at each time step modulo x^N-1 as in Eq. (2.2). There are taken to be k possible values for each site. With no further constraints imposed, there are k^3 possible $\mathbb{T}(x)$, and thus k^3 distinct cellular automaton rules. If the coefficients of x and x^{-1} in $\mathbb{T}(x)$ both vanish, then the characteristic polynomial is at most multiplied by an overall factor at each time step, and the behaviour of the cellular automaton is trivial. Requiring nonzero coefficients for x and x^{-1} in $\mathbb{T}(x)$ reduces the number of possible rules to $k^3—2k^2+k$. If the cellular automaton evolution is assumed reflection symmetric, then $\mathbb{T}(x)=\mathbb{T}(x^{-1})$, and only k^2-k rules are possible. Further characterisation of possible rules depends on the nature of k.

(a) k Prime. In this case, integer values $0, 1, \ldots, k-1$ at each site may be combined by addition and multiplication modulo k to form a field (in which each nonzero element has a unique multiplicative inverse) $\mathbb{Z}_k$. For a symmetrical rule, $\mathbb{T}(x)$ may always be written in the form

$$\mathbb{T}(x)=x+s+x^{-1} \tag{4.1}$$

up to an overall multiplicative factor. For $k=2$, the rule $\mathbb{T}(x)=x+x^{-1}$ was considered above; the additional rule $\mathbb{T}(x)=x+1+x^{-1}$ is also possible (and corresponds to rule 150 of [1]).

(b) k Composite.

Lemma 4.1. *For $k=p_1^{\alpha_1}p_2^{\alpha_2}\ldots$, with p_i prime, the value $a^{[k]}$ of a site obtained by evolution of an additive cellular automaton from some initial configuration is given uniquely in terms of the values $a^{[p^\alpha]}$ attained by that site in the evolution of the set of cellular automata obtained by reducing $\mathbb{T}(x)$ and all site values modulo $p_i^{\alpha_i}$.*

This result follows from the Chinese remainder theorem for integers (e.g. [8, Chap. 8]), which states that if k_1 and k_2 are relatively prime, then the values n_1 and n_2 determine a unique value of n modulo k_1k_2 such that $n \equiv n_i \bmod k_i$ for $i=1,2$.

Lemma 4.1 shows that results for any composite k may be obtained from those for k a prime or a prime power.

When k is composite, the ring $\mathbb{Z}_k$ of integers modulo k no longer forms a field, so that not all commutative rings $\mathbb{R}_k$ are fields. Nevertheless, for k a prime power, there exists a Galois field $GF(k)$ of order k, unique up to isomorphism (e.g. [9; Chap. 4]). For example, the field $GF(4)$ may be taken to act on elements $0, 1, \kappa, \kappa^2$ with multiplication taken modulo the irreducible polynomial $\kappa^2+\kappa+1$. Time evolution for a cellular automaton with site values in this Galois field can be reduced to that given by $x+\sigma+x^{-1}$, where σ is any element of the field. The behaviour of this subset of cellular automata with k composite is directly analogous to those over $\mathbb{Z}_p$ for prime p.

It has been assumed above that the value of a site at a particular time step is determined solely by the values of its nearest neighbours on the previous time step. One generalization allows dependence on sites out to a distance $r>1$, so that the evolution of the cellular automaton corresponds to multiplication by a fixed dipolynomial $\mathbb{T}(x)$ of degree $2r$. Most of the theorems to be derived below hold for any r.

B. Cellular Automata over $\mathbb{Z}_p$ (p Prime)

Lemma 4.2. *The lengths of all cycles in any additive cellular automaton over $\mathbb{Z}_p$ of size N divide the length Π_N of the cycle obtained for an initial configuration containing a single site with value* 1.

This lemma is a straightforward generalization of Lemma 3.4, and follows directly from the additivity assumed for the cellular automaton rules.

Lemma 4.3. *For N a multiple of p, $\Pi_N | p\Pi_{N/p}$ for an additive cellular automaton over $\mathbb{Z}_p$.*

Remark. For N a multiple of p, but not a power of p, it can be shown that $\Pi_N = p\Pi_{N/p}$ for an additive cellular automaton over $\mathbb{Z}_p$ with $\mathbb{T}(x) = x + x^{-1}$. In addition, $\Pi_{p^j} = 1$ in this case.

Theorem 4.1. *For any N not a multiple of p, $\Pi_N | \Pi_N^* = p^{\mathrm{ord}_N(p)} - 1$, and $\Pi_N | \Pi_N^* = p^{\mathrm{sord}_N(p)} - 1$ if $\mathbb{T}(x)$ is symmetric, for any additive cellular automaton over $\mathbb{Z}_p$.*

The period Π_N divides Π_N^* if

$$[\mathbb{T}(x)]^{\Pi_N^* + 1} \equiv \mathbb{T}(x) \quad \bmod (x^N - 1). \tag{4.2}$$

Taking

$$\mathbb{T}(x) = \sum_i \alpha_i x^{\gamma_i},$$

Eq. (A.3) yields

$$[\mathbb{T}(x)]^{p^{\mathrm{ord}_N(p)}} \equiv \sum_i \alpha_i x^{\gamma_i p^{\mathrm{ord}_N(p)}} \equiv \sum_i \alpha_i x^{\gamma_i} = \mathbb{T}(x) \quad \bmod (x^N - 1),$$

since $\alpha^{p^\lambda} \equiv \alpha \bmod p$ and $p^{\mathrm{ord}_N(p)} \equiv 1 \bmod N$, and the first part of the theorem follows. Since $x^{p^{\mathrm{sord}_N(p)}} \equiv x^{\pm 1} \bmod p$, Eq. (4.2) holds for

$$\Pi_N^* = p^{\mathrm{sord}_N(p)} - 1$$

if $\mathbb{T}(x)$ is symmetric, so that $\mathbb{T}(x) = \mathbb{T}(x^{-1})$.

This result generalizes Theorem 3.5 for the particular $k=2$ cellular automaton considered in Sect. 3.

Table 1 gives the values of Π_N for all non-trivial additive symmetrical cellular automata over $\mathbb{Z}_2$ and $\mathbb{Z}_3$. Just as in the example of Sect. 3 (given as the first column of Table 1), one finds that for many values of N not divisible by p

$$\Pi_N = p^{\mathrm{sord}_N(p)} - 1. \tag{4.3}$$

When $p=2$, all exceptions to (4.3) when $\mathbb{T}(x) = x + x^{-1}$ are also exceptions for $\mathbb{T}(x) = x + 1 + x^{-1}$ [19]. We outline a proof for the simplest case, when N is relatively prime to 6 (as well as 2). Let $\Pi_N(x + x^{-1})$ be the maximal period obtained with $\mathbb{T}(x) = x + x^{-1}$, equal to the minimum integer π for which

$$(x+1)^{2\pi} \equiv x^\pi \quad \bmod \left(\frac{x^N - 1}{x + 1}\right). \tag{4.4}$$

We now show that $\Pi_N(x + x^{-1})$ is a multiple of the maximum period $\Pi_N(x + 1 + x^{-1})$ obtained with $\mathbb{T}(x) = x + 1 + x^{-1}$. Since the mapping $x \to x^3$ is a homomorphism in the field of polynomials with coefficients in $GF(2)$, one has

$$(x^3+1)^{2\pi} \equiv x^{3\pi} \quad \bmod\left(\frac{x^N-1}{x+1}\right)$$

for any π such that $\Pi_N(x+x^{-1})|\pi$. Dividing by Eq. (4.4), and using the fact that N is odd to take square roots, yields

$$\left(\frac{x^3+1}{x+1}\right)^{\pi} \equiv x^{\pi} \quad \bmod\left(\frac{x^N-1}{x+1}\right) \tag{4.5}$$

for any π such that $\Pi_N(x+x^{-1})|\pi$. But since $x+1+x^{-1}=x^{-1}\left(\frac{x^3+1}{x+1}\right)$, Eq. (4.5) is the analogue of Eq. (4.4) for $\mathbb{T}(x)=x+1+x^{-1}$, and the result follows.

More exceptions to Eq. (4.3) are found with $p=3$ than with $p=2$.

Lemma 4.4. *A configuration $A(x)$ is reachable in the evolution of a size N additive cellular automaton over $\mathbb{Z}_p$, as described by $\mathbb{T}(x)$ if and only if $A(x)$ is divisible by $\Lambda_1(x)=(x^N-1, \mathbb{T}(x))$.*

Appendix A.A gives conventions for the greatest common divisor $(A(x), B(x))$.

If $A^{(1)}(x)$ can be reached, then

$$A^{(1)}(x)=\mathbb{T}(x)A^{(0)}(x) \quad \bmod(x^N-1)$$

for some $A^{(0)}(x)$, so that

$$(x^N-1) \mid A^{(1)}(x)-\mathbb{T}(x)A^{(0)}(x).$$

But $\Lambda_1(x)|x^N-1$ and $\Lambda_1(x)|\mathbb{T}(x)$, and hence if $A^{(1)}(x)$ is reachable,

$$\Lambda_1(x) \mid A^{(1)}(x). \tag{4.6}$$

We now show by an explicit construction that all $A^{(1)}(x)$ satisfying (4.6) in fact have predecessors $A^{(0)}(x)$. Using Eq. (A.10), one may write

$$\Lambda_1(x)=r(x)\mathbb{T}(x)+\xi(x)(x^N-1)$$

for some dipolynomials $r(x)$ and $\xi(x)$, so that

$$\Lambda_1(x) \equiv r(x)\mathbb{T}(x) \quad \bmod(x^N-1).$$

Then taking $A^{(1)}(x)=\Lambda_1(x)B(x)$, the configuration given by the polynomial obtained by reducing the dipolynomial $r(x)B(x)$ satisfies

$$\mathbb{T}(x)r(x)B(x) \equiv \Lambda_1(x)B(x) \equiv A^{(1)}(x) \quad \bmod(x^N-1)$$

and thus provides an explicit predecessor for $A^{(1)}(x)$.

Corollary. *$A(x)$ is reachable in j steps if and only if $\Lambda_j(x)=(x^N-1, \mathbb{T}^j(x))$ divides $A(x)$.*

This is a straightforward extension of the above lemma.

Theorem 4.2. *The fraction of possible configurations which may be reached by evolution of an additive cellular automaton over $\mathbb{Z}_p$ of size N is $p^{-\deg \Lambda_1(x)}$, where $\Lambda_1(x)=(x^N-1, \mathbb{T}(x))$.*

By Lemma 4.4, only configurations divisible by $\Lambda_1(x)$ may be reached. The number of such configurations is $p^{N-\deg \Lambda_1(x)}$, while the total number of possible configurations is p^N.

Let $D_p(N)$ be the maximum p^j which divides N and let v_i denote the multiplicity of the i^{th} irreducible factor of $\Lambda_1(x)$ in $\mathbb{T}^*(x)$, where $\mathbb{T}^*(x) = x^r \mathbb{T}(x)$ is a polynomial with a nonzero constant term. We further define $\chi = \min_i v_i$, so that $0 \leqq \chi \leqq D_p(N)$.

Theorem 4.3. *The state transition diagram for an additive cellular automaton of size N over $\mathbb{Z}_p$ consists of a set of cycles at all nodes of which are rooted identical $p^{\deg \Lambda_1(x)}$-ary trees. A fraction $p^{-D_p(N) \deg \Lambda_1(x)}$ of the possible configurations appear on cycles. For $\chi > 0$, the height of the trees is $\lceil D_p(N)/\chi \rceil$. The trees are balanced if and only if* (a) *$v_i \geqq D_p(N)$ for all i, or* (b) *$v_i = v_j$ for all i and j, and $v_i | D_p(N)$.*

To determine the in-degrees of nodes in the trees, consider a configuration $A(x)$ with predecessors represented by the polynomials $B_1(x)$ and $B_2(x)$, so that

$$A(x) \equiv \mathbb{T}(x) B_i(x) \quad \mathrm{mod}\,(x^N - 1).$$

Then since

$$\mathbb{T}(x)\,(B_1(x) - B_2(x)) \equiv 0 \quad \mathrm{mod}\,(x^N - 1),$$

and $\Lambda_1(x) | x^N - 1$, it follows that

$$B_1(x) - B_2(x) \equiv 0 \quad \mathrm{mod}\left(\frac{x^N - 1}{\Lambda_1(x)}\right).$$

Since $C(x) = (x^N - 1)/\Lambda_1(x)$ has a non-zero constant term, $(B_1(x) - B_2(x))/C(x)$ is an ordinary polynomial. The number of solutions to this congruence and thus the number of predecessors $B_i(x)$ of $A(x)$ is $p^{\deg \Lambda_1(x)}$.

The proof of Lemma 3.3 demonstrates the identity of the trees. The properties of the trees are established by considering the tree rooted on the null configuration. A configuration $A(x)$ evolves to the null configuration after j steps if $\mathbb{T}(x)^j A(x) \equiv 0 \,\mathrm{mod}\,(x^N - 1)$, so that

$$\frac{x^N - 1}{\Lambda_j(x)} \,\Big|\, A(x). \tag{4.7}$$

Hence all configurations on the tree are divisible by $(x^N - 1)/\Lambda_\infty(x)$, where $\Lambda_\infty(x) = \lim_{j \to \infty} \Lambda_j(x)$. All configurations in the tree evolve to the null configuration after at most $\lceil D_p(N)/\chi \rceil$ steps, which is thus an upper bound on the height of the trees. But since the configuration $(x^N - 1)/\Lambda_\infty(x)$ evolves to the null configuration after exactly $\lceil D_p(N)/\chi \rceil$ steps, this quantity gives the height of the trees. The tree of configurations which evolve to the null configuration (and hence all other trees in the state transition diagram) is balanced if and only if all unreachable (terminal) configurations evolve to the null configuration after the same number of steps. First suppose that neither condition (a) nor (b) is true. One possibility is that some irreducible factor $\sigma(x)$ of $\Lambda_1(x)$ satisfies $\sigma^v(x) \| \Lambda_1(x)$ with $v < D_p(N)$ but v does not divide $D_p(N)$. The configuration $(x^N-1)/\sigma^{D_p(N)}(x)$ reaches 0 *in* $\lceil D_p(N)/v \rceil$ steps whereas $(x^N-1)/\sigma^{D_p(N)+1-v}(x)$ reaches 0 in one step fewer, yet both are unreachable, so that the tree cannot be balanced. The only other possibility is that there exist two irreducible factors $\sigma_1(x)$ and $\sigma_2(x)$ of multiplicities v_1 and v_2, respectively, with v_1 and v_2 dividing $D_p(N)$ but $v_1 \neq v_2$. Then $(x^N-1)/\sigma_1^{D_p(N)}(x)$ reaches 0 in $D_p(N)/v_1$ steps, whereas $(x^N-1)/\sigma_2^{D_p(N)}(x)$ reaches 0 in $D_p(N)/v_2$ steps. Neither of these configurations is reachable, so again the trees cannot be balanced. This establishes that in all cases either condition (a) or (b) must hold. The sufficiency of condition (a) is evident. If the condition (b) is true, then

$$\Lambda_1(x) = [\prod \sigma(x)]^v, \qquad \Lambda_\infty(x) = [\prod \sigma(x)]^{D_p(N)},$$

and $\Lambda_j(x) = \Lambda_1^j(x)$. Equation (4.7) shows that any configuration $A(x)$ which evolves to the null configuration after j steps is of the form

$$A(x) = \frac{x^N - 1}{\Lambda_1^j(x)} R(x),$$

where $R(x)$ is some polynomial. The proof is completed by showing that all such configurations $A(x)$ with $j < D_p(N)/v$ are indeed reachable. To construct an explicit predecessor for $A(x)$, define the dipolynomial $S(x)$ by $\mathbb{T}(x) = \Lambda_1(x)S(x)$, so that $(S(x), x^N-1) = 1$. Then there exist dipolynomials $r(x)$ and $\xi(x)$ such that

$$r(x)S(x) + \xi(x)(x^N - 1) = 1.$$

The configuration given by the dipolynomial

$$B(x) = \frac{x^N - 1}{\Lambda_1^{j+1}(x)} r(x)R(x)$$

then provides a predecessor for $A(x)$.

Notice that whenever the balance condition fails, the set and measure entropies of Eqs. (3.11) and (3.12) obtained by evolution from an initial maximal entropy ensemble become unequal.

The results of Theorems 4.2 and 4.3 show that if $\deg \Lambda_1(x) = 0$, then the evolution of an additive cellular automaton if effectively reversible, since every configuration has a unique predecessor.

In general,

$$\deg \Lambda(x) \leqq \deg \mathbb{T}^*(x),$$

so that for the one-dimensional additive cellular automata considered so far, the maximum decrease in entropy starting from an initial equiprobable ensemble is $D_p(N)$.

Note that for a cellular automaton over $\mathbb{Z}_p$ $(p>2)$ of length N with $\mathbb{T}(x) = x + x^{-1}$, $\deg \Lambda(x) = 2$ if $4|N$ and $\deg \Lambda(x) = 0$ otherwise. Such cellular automata are thus effectively reversible for $p>2$ whenever N is not a multiple of 4.

Remark. A configuration $A(x)$ lies on a cycle in the state transition diagram of an additive cellular automaton if and only if $\Lambda_\infty(x)|A(x)$.

This may be shown by the methods used in the proof of Theorem 4.3.

C. Cellular Automata over $\mathbb{Z}_k$ (k Composite)

Theorem 4.4. *For an additive cellular automaton over $\mathbb{Z}_k$,*

$$\Pi_N(\mathbb{Z}_k; \mathbb{T}_k(x)) = \operatorname{lcm}(\Pi_N(\mathbb{Z}_{p_1^{\alpha_1}}; \mathbb{T}_{p_1^{\alpha_1}}(x)), \Pi_N(\mathbb{Z}_{p_2^{\alpha_2}}; \mathbb{T}_{p_2^{\alpha_2}}(x)), \ldots),$$

where $k = p_1^{\alpha_1} p_2^{\alpha_2} \ldots$, and in $\mathbb{T}_j(x)$ all coeffficients are reduced modulo j.

This result follows immediately from Lemma 4.1.

Theorem 4.5. *$\Pi_N(\mathbb{Z}_{p^{\alpha+1}}; \mathbb{T}_{p^{\alpha+1}}(x))$ is equal to either* (a) *$p\Pi_N(\mathbb{Z}_{p^\alpha}; \mathbb{T}_{p^\alpha}(x))$ or* (b) *$\Pi_N(\mathbb{Z}_{p^\alpha}; \mathbb{T}_{p^\alpha}(x))$ for an additive cellular automaton.*

First, it is clear that

$$\Pi_N(\mathbb{Z}_{p^\alpha}; \mathbb{T}_{p^\alpha}(x) \mid \Pi_N(\mathbb{Z}_{p^{\alpha+1}}; \mathbb{T}_{p^{\alpha+1}}(x)).$$

To complete the proof, one must show that in addition

$$\Pi_N(\mathbb{Z}_{p^{\alpha+1}}; \mathbb{T}_{p^{\alpha+1}}(x)) \mid p\Pi_N(\mathbb{Z}_{p^\alpha}; \mathbb{T}_{p^\alpha}(x)).$$

$\Pi_N(\mathbb{Z}_{p^\alpha}; \mathbb{T}_{p^\alpha}(x))$ is the smallest positive integer π for which a positive integer m and dipolynomials $U(x)$ and $V(x)$ satisfying

$$\mathbb{T}(x)^{m+\pi} = \mathbb{T}(x)^m + (x^N - 1)U(x) + p^\alpha V(x) \tag{4.8}$$

exist, where all dipolynomial coefficients (including those in $\mathbb{T}(x)$) are taken as ordinary integers in $\mathbb{Z}$, and irrelevant powers of x on both sides of the equation have been dropped. Raising both sides of Eq. (4.8) to the power p, one obtains

$$\begin{aligned} \mathbb{T}(x)^{mp+\pi p} &= (x^N - 1)W(x) + (\mathbb{T}(x)^m + p^\alpha V(x))^p \\ &= (x^N - 1)W(x) + \mathbb{T}(x)^{mp} + p^{\alpha+1}Q(x). \end{aligned}$$

Reducing modulo $p^{\alpha+1}$ yields the required result.

For $p = 2$ and $\alpha = 1$, it can be shown that case (a) of Theorem 4.5 always obtains if $\mathbb{T}(x) = x + x^{-1}$, but case (b) can occur when $\mathbb{T}(x) = x + 1 + x^{-1}$.

Theorem 4.6. *With $k = k_1 k_2 \ldots$ (all k_i relatively prime), the number of configurations which can be reached by evolution of an additive cellular automaton over $\mathbb{Z}_k$ is equal to the product of the numbers reached by evolution of cellular automata with the same $\mathbb{T}(x)$ over each of the $\mathbb{Z}_{k_i}$. The state transition diagram for the cellular automaton over $\mathbb{Z}_k$ consists of a set of identical trees rooted on cycles. The in-degrees of non-terminal nodes in the trees are the product of those for each of the $\mathbb{Z}_{k_i}$ cases. The height of the trees is the maximum of the heights of trees for the $\mathbb{Z}_{k_i}$ cases, and the trees are balanced only if all these heights are equal.*

These results again follow directly from Lemma 4.1.

Theorem 4.6 gives a characterisation of the state transition diagram for additive cellular automata over $\mathbb{Z}_k$ when k is a product of distinct primes. No general results are available for the case of prime power k. However, for example, with $\mathbb{T}(x) = x + x^{-1}$, one may obtain the fraction of reachable states by direct combinatorial methods. With $k = 2^\alpha$ one finds in this case that the fraction is $1/2$ for N odd, $1/4$ for $N \equiv 2 \bmod 4$, and $2^{-2\alpha}$ for $4|N$. With $k = p^\alpha$ $(p \neq 2)$ the systems are reversible (all configurations reachable) unless $4|N$, in which case a fraction $p^{-2\alpha}$ may be reached.

D. Multidimensional Cellular Automata

The cellular automata considered above consist of a sequence of sites on a line. One generalization takes the sites instead to be arranged on a square lattice in two dimensions. The evolution of a site may depend either on the values of its four orthogonal neighbours (type I neighbourhood) or on the values of all eight neighbours including those diagonally adjacent (type II neighbourhood) (e.g. [1]). Configurations of two-dimensional cellular automata may be represented by bivariate characteristic polynomials $A(x_1, x_2)$. Time evolution for additive cellular automaton rules is obtained by multiplication of these characteristic polynomials by a fixed bivariate dipolynomial $\mathbb{T}(x_1, x_2)$. For a type I neighbourhood, $\mathbb{T}(x_1, x_2)$ contains no $x_1 x_2$ cross-terms; such terms may be present for a type II neighbourhood. Periodic boundary conditions with periods N_1 and N_2 may be implemented by reduction modulo $x_1^{N_1}-1$ and modulo $x_2^{N_2}-1$ at each time step. Cellular automata may be generalized to an arbitrary d-dimensional cubic or hypercubic lattice. A type I neighbourhood in d dimensions contains $2d+1$ sites, while a type II neighbourhood contains 3^d sites. As before, we consider cellular automata with k possible values for each site.

Theorem 4.7. *For an additive cellular automaton over $\mathbb{Z}_k$ on a d-dimensional cubic lattice, with a type I or type II neighbourhood, and with periodicities $N_1, N_2, \ldots, N_d$,* $\mathrm{lcm}(\Pi_{N_1}(\mathbb{Z}_k; \mathbb{T}(x_1, 1, \ldots, 1)), \ldots, \Pi_{N_d}(\mathbb{Z}_k; \mathbb{T}(1, \ldots, 1, x_d))) | \Pi_{N_1, \ldots, N_d}(\mathbb{Z}_k; \mathbb{T}(x_1, \ldots, x_d))$.

The result may be proved by showing that

$$\Pi_{N_i}(\mathbb{Z}_i; \mathbb{T}(1, \ldots, 1, x_i, 1, \ldots, 1)) \,|\, \Pi_{N_1, \ldots, N_d}(\mathbb{Z}_k, \mathbb{T}(x_1, \ldots, x_d)) \tag{4.9}$$

for all i (such that $1 \leq i \leq d$). The right member of Eq. (4.9) is given by the smallest integer π for which there exists a positive integer m such that

$$[\mathbb{T}(x_1, \ldots, x_d)]^{\pi+m} = [\mathbb{T}(x_1, \ldots, x_d)]^m + \sum_{j=1}^{d} (x_j^{N_j}-1) U_j(x_1, \ldots, x_d) \tag{4.10}$$

for some dipolynomials U_j. Taking $x_j = 1$ with $j \neq i$ in Eq. (4.10), all terms in the sum vanish except for the one associated with x_i, and the resulting value of π corresponds to the left member of Eq. (4.9).

Theorem 4.8. *For an additive cellular automaton over $\mathbb{Z}_p$ on a d-dimensional cubic lattice (type I or type II neighbourhood) with periodicities $N_1, N_2, \ldots, N_d$ none of which are multiples of p,*

$$\Pi_{N_1, \ldots, N_d}(\mathbb{Z}_p; \mathbb{T}(x_1, \ldots, x_d)) \,|\, \Pi^*_{N_1, \ldots, N_d} = p^{\mathrm{ord}_{N_1, \ldots, N_d}(p)} - 1 .$$

If $\mathbb{T}(x_1, \ldots, x_d)$ is symmetrical, so that

$$\mathbb{T}(x_1, \ldots, x_i, \ldots, x_d) = \mathbb{T}(x_1, \ldots, x_i^{-1}, \ldots, x_d)$$

for all i, then

$$\Pi^*_{N_1, \ldots, N_d} = p^{\mathrm{sord}_{N_1, \ldots, N_d}(p)} - 1 .$$

The $\mathrm{ord}_{n_1,\ldots,n_d}(p)$ *and* $\mathrm{sord}_{n_1,\ldots,n_d}(p)$ *are multidimensional generalizations of the multiplicative order and suborder functions, described in Appendix B.*

This theorem is proved by straightforward extension of the one-dimensional Theorem 4.1.

Using the result (B.13), one finds for symmetrical rules

$$\Pi^*_{N_1,\ldots,N_d} = p^{\mathrm{lcm}(\mathrm{sord}_{N_1}(p),\ldots,\mathrm{sord}_{N_d}(p))} - 1\,.$$

The maximal cycle length is thus bounded by

$$\Pi_{N_1,\ldots,N_d} \leqq p^{\mathrm{lcm}((N_1-1)/2,\ldots,(N_d-1)/2} - 1 \leqq p^{(N_1-1)\ldots(N_d-1)/2^d} - 1\,,$$

with the upper limits achieved only if all the N_i are prime. (For example,

$$\Pi_{83,59} = 2^{1189} \simeq 10^{358}$$

saturates the upper bound.)

Algebraic determination of the structure of state transition diagrams is more complicated for multi-dimensional cellular automata than for the one dimensional cellular automata considered above[2]. The generalization of Lemma 4.4 states that a configuration $A(x_1,\ldots,x_d)$ is reachable only if $A(z_1,\ldots,z_d)$ vanishes whenever the z_i are simultaneous roots of $\mathbb{T}(x_1,\ldots,x_d)$, $x^{N_1}-1,\ldots,x^{N_d}-1$. The root sets z_i form an algebraic variety over $\mathbb{Z}_k$ (cf. [9]).

E. Higher Order Cellular Automata

The rules for cellular automaton evolution considered above took configurations to be determined solely from their immediate predecessors. One may in general consider higher order cellular automaton rules, which allow dependence on say s preceding configurations. The time evolution for additive one-dimensional higher-order cellular automata (with N sites and periodic boundary conditions) may be represented by the order s recurrence relation

$$A^{(t)}(x) = \sum_{j=1}^{s} \mathbb{T}_j(x) A^{(t-j)}(x) \qquad \mathrm{mod}(x^N - 1)\,. \tag{4.11}$$

This may be solved in analogy with order s difference equations to yield

$$A^{(t)}(x) = \sum_{j=1}^{s} c_j(x)[U_j(x)]^t\,,$$

where the $U_j(x)$ are solutions to the equation

$$[U(x)]^s = \sum_{j=1}^{s} [U(x)]^{s-j}\mathbb{T}_j(x)\,,$$

and the $c_j(x)$ are analogous to "constants of integration" and are determined by the initial configurations $A^{(0)}(x),\ldots,A^{(s-1)}(x)$. The state of an order s cellular

2 In the specific case $\mathbb{T}(x_1,x_2) = x_1 + x_1^{-1} + x_2 + x_2^{-1}$, one finds that the in-degrees I_{N_1,N_2} of trees in the state transition diagrams for a few $N_1 \times N_2$ cellular automata are: $I_{2,2}=16$, $I_{2,3}=4$, $I_{2,4}=16$, $I_{2,5}=4$, $I_{2,6}=16$, $I_{3,3}=32$, $I_{3,4}=4$, $I_{3,5}=2$, $I_{4,4}=256$

automaton depends on the values of its N sites over a sequence of s time steps; there are thus a total of k^{Ns} possible states. The transition diagram for these states can in principle be derived by algebraic methods starting from Eq. (4.11). In practice, however, the $U_j(x)$ are usually not polynomials, but elements of a more general function field, leading to a somewhat involved analysis not performed here.

For first-order additive cellular automata, any configuration may be obtained by superposition of the configuration 1 (or its translates x^j). For higher-order cellular automata, several "basis" configurations must be included. For example, when $s=2$, $\{0,1\}$, $\{1,0\}$, and $\{x^j,1\}$ are all basis configurations, where in $\{A_1(x), A_2(x)\}$, $A_1(x)$, and $A_2(x)$ represent configurations at successive time steps.

As discussed in Sect. 4B, some first-order cellular automata over $\mathbb{Z}_p$ $(p>2)$ are effectively reversible for particular values of N, so that all states are on cycles. The class of second-order cellular automata with $\mathbb{T}_2(x)=-1$ is reversible for all N and k, and for any $\mathbb{T}_1(x)$ [10]. In the simple case $\mathbb{T}_1(x)=x+x^{-1}$, one finds $U_1(x)=x$, $U_2(x)=x^{-1}$. It then appears that

$$\begin{aligned} \Pi_N &= kN/2 \quad (k \text{ even}, N \text{ even}) \\ &= kN \quad (\text{otherwise}). \end{aligned}$$

(The proof is straightforward when $k=2$.) In the case $\mathbb{T}_1(x)=x+1+x^{-1}$, the $U_j(x)$ are no longer polynomials. For the case $k=2$, the results for Π_N with N between 3 and 30 are: 6, 6, 15, 12, 9, 12, 42, 30, 93, 24, 63, 18, 510, 24, 255, 84, 513, 60, 1170, 186, 6141, 48, 3075, 126, 3066, 36, 9831, 1020.

F. Other Boundary Conditions

The cellular automata discussed above were taken to consist of N indistinguishable sites with periodic boundary conditions, as if arranged around a circle. This section considers briefly cellular automata with other boundary conditions. The discussion is restricted to the case of symmetric time evolution rules $\mathbb{T}(x)=\mathbb{T}(x^{-1})$.

The periodic boundary conditions considered above are not the only possible choice which preserve the translation invariance of cellular automata (or the indistinguishability of their sites)[3]. One-dimensional cellular automata may in general be viewed as $\mathbb{R}_k$ bundles over $\mathbb{Z}_N$. Periodic boundary conditions correspond to trivial bundles. Non-trivial bundles are associated with "twisted" boundary conditions. Explicit realizations of such boundary conditions require a twist to be introduced at a particular site. The evolution of particular configurations then depends on the position of the twist, but the structure of the state transition diagram does not.

A twist of value R at position $i=\sigma$ causes sites with $i \geqq \sigma$ to appear multiplied by R in the time evolution of sites with $i<\sigma$, and correspondingly, for sites with $i<\sigma$ to appear multiplied by R^{-1} in the evolution of sites with $i \geqq \sigma$. In the presence of a twist taken at position $\sigma=0$, the time evolution formula (2.5) becomes

$$A^{(t)}(x)=\mathbb{T}(x)A^{(t-1)}(x) \quad \mathrm{mod}(x^N-R). \tag{4.12}$$

3 We are grateful to L. Yaffe for emphasizing this point

Multiple twists are irrelevant; only the product of their values R_j is significant for the structure of the state transition diagram. If $\mathbb{R}_k = \mathbb{Z}_p$ with p prime, then $\mathbb{R}_k$ (with the zero element removed) forms a multiplicative group, and twists with any value R not equal to 0 or 1 yield equivalent results. When $\mathbb{R}_k = \mathbb{Z}_k$ with k composite, several equivalence classes of R values may exist.

Using Eq. (4.12) one may obtain general results for twisted boundary conditions analogous to those derived above for the case of periodic boundary conditions (corresponding to $R=1$). When $\mathbb{R}_k = \mathbb{Z}_p$ (p prime), one finds for example,

$$\Pi_N^{[R \neq 1]} \mid \Pi_{N(p-1)}^{[R=1]} .$$

An alternative class of boundary conditions introduces fixed values at particular cellular automaton sites. One may consider cellular automata consisting of N sites with values $a_1, \ldots, a_N$ arranged as if along a line, bounded by sites with fixed values a_0 and a_{N+1}. Maximal periods obtained with such boundary conditions will be denoted $\Pi_N^{(a_0, a_{N+1})}$. The case $a_0 = a_{N+1} = 0$ is simplest. In this case, configurations

$$A(x) = \sum_{i=1}^{N} a_i x^i$$

of the length N system with fixed boundary conditions may be embedded in configurations

$$\tilde{A}(x) = \sum_{i=1}^{N} a_i x^i + \sum_{i=1}^{N} (k - a_{N+1-i}) x^{N+1+i} \tag{4.13}$$

of a length $\tilde{N} = 2N + 2$ system with periodic boundary conditions. The condition $a_0 = a_{N+1} = 0$ is preserved by time evolution, so that one must have

$$\Pi_N^{(0,0)} \mid \Pi_{2N+2} .$$

The periods are equal if the configurations obtained by evolution from a single nonzero initial site have the symmetry of Eq. (4.13). (The simplest cellular automaton defined in Sect. 3A satisfies this condition.)

Fixed boundary conditions $a_0 = r$, $a_{N+1} = 0$, may be treated by constructing configurations $\tilde{A}(x)$ of the form (4.13), with periodic boundary conditions, but now with time evolution

$$\tilde{A}^{(t)}(x) \equiv [\mathbb{T}(x) \tilde{A}^{(t-1)}(x) + r(1 - \alpha_0)] \quad \operatorname{mod}(x^{\tilde{N}} - 1),$$

where $\mathbb{T}(x)$ is taken of the form $x + \alpha_0 + x^{-1}$. Iteration generates a geometric series in $\mathbb{T}(x)$, which may be summed to yield a rational function of x. For $k=2$, $r=1$, one may then show that with $\mathbb{T}(x) = x + 1 + x^{-1}$, $\Pi_N^{(0,1)} = \Pi_{2N+2}$, while with $\mathbb{T}(x) = x + x^{-1}$ (the case of Sect. 3A), $\Pi_N^{(0,1)} \mid \Pi_{2(2N+2)}$.

5. Non-Additive Cellular Automata

Equation (2.3) defines the time evolution for a special class of "additive" cellular automata, in which the value of a site is given by a linear combination (in $\mathbb{R}_k$) of the values of its neighbours on the previous time step. In this section we discuss "non-additive" cellular automata, which evolve according to

$$a_i^{(t)} = \mathbb{F}[a_{i-1}^{(t-1)}, a_i^{(t-1)}, a_{i+1}^{(t-1)}], \tag{5.1}$$

where $\mathbb{F}[a_{-1}, a_0, a_{+1}]$ is an arbitrary function over $\mathbb{R}_k$, not reducible to linear form. The absence of additivity in general prevents use of the algebraic techniques developed for additive cellular automata in Sects. 3 and 4. The difficulties in the analysis of non-additive cellular automata are analogous to those encountered in the analysis of non-linear feedback shift registers (cf. [11]). In fact, the possibility of universal computation with sufficiently complex non-additive cellular automata demonstrates that a complete analysis of these systems is fundamentally impossible. Some results are nevertheless available (cf. [12]). This section illustrates some methods which may be applied to the analysis of non-additive cellular automata, and some of the results which may be obtained.

As in [1], most of the discussion in this section will be for the case $k=2$. In this case, there are 32 possible functions $\mathbb{F}$ satisfying the symmetry condition

$$\mathbb{F}[a_{-1}, a_0, a_{+1}] = \mathbb{F}[a_{+1}, a_0, a_{-1}]$$

and the quiescence condition

$$\mathbb{F}[0,0,0] = 0.$$

Reference [1] showed the existence of two classes of these "legal" cellular automata. The "simple" class evolved to fixed points or short cycles after a small number of time steps. The "complex" class (which included the additive rules discussed above) exhibited more complicated behaviour.

We consider as an example the complex non-additive $k=2$ rule defined by

$$\begin{aligned} &\mathbb{F}[1,0,0] = \mathbb{F}[0,0,1] = 1, \\ &\mathbb{F}[a_{-1}, a_0, a_{+1}] = 0 \quad \text{otherwise}, \end{aligned} \tag{5.2}$$

and referred to as rule 18 in [1]. This function yields a time evolution rule equivalent to

$$a_i^{(t)} \equiv (1 + a_i^{(t-1)})(a_{i-1}^{(t-1)} + a_{i+1}^{(t-1)}) \quad \mod 2. \tag{5.3}$$

The rule does not in general satisfy any superposition principle. However, for the special class of configurations with $a_{2j}=0$ or $a_{2j+1}=0$, Eq. (5.3) implies that the evolution of even (odd) sites on even (odd) time steps is given simply by the rule defined in Sect. 3A. Any configuration may be considered as a sequence of "domains" in which all even (or odd) sites have value zero, separated by "domain walls" or "kinks" [13]. In the course of time the kinks annihilate in pairs. If sites are nonzero only in some finite region, then at sufficiently large times in an infinite cellular automaton, all kinks (except perhaps one) will have annihilated, and an effectively additive system will result. However, out of all 2^N possible initial configurations for a cellular automaton with N sites and periodic boundary conditions, only a small fraction are found to evolve to this form before a cycle is reached: in most cases, "kinks" are frozen into cycles, and contribute to global behaviour in an essential fashion.

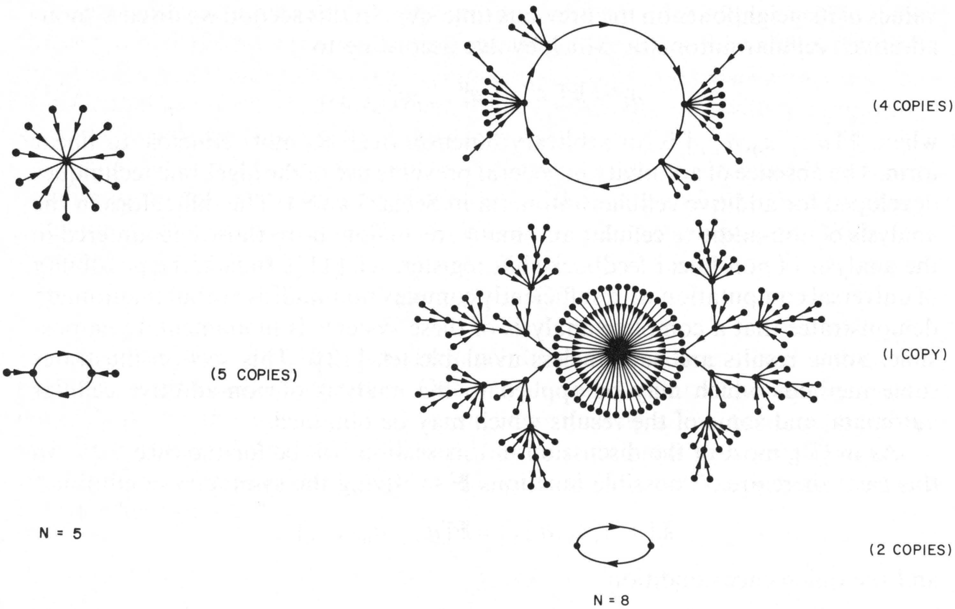

Fig. 5. Global state transition diagrams for a typical finite non-additive cellular automaton discussed in Sect. 5

Typical examples of the state transition diagrams with the rule (5.3) are shown in Fig. 5. They are seen to be much less regular than those for additive rules illustrated in Fig. 2. In particular, not all transient trees are identical, and few of the trees are balanced. Just as for the additive rules discussed in Sects. 3 and 4, only a fraction of the 2^N possible configurations may be reached by evolution according to Eq. (5.3); the rest are unreachable and appear as nodes with zero in-degree on the periphery of the state transition diagram of Fig. 5. An explicit characterization of these unreachable configurations may be found by lengthy but straightforward analysis.

Lemma 5.1. *A configuration is unreachable by cellular automaton time evolution according to Eq.* (5.3) *if and only if one of the following conditions holds:*

(a) *The sequence of site values* 111 *appears.*

(b) *No sequence* 11 *appears, but the total number of* 1 *sites is odd.*

(c) *A sequence* $11a_1a_2 \ldots a_n11$ *appears, with an odd number of the* a_i *having value* 1. *The two* 11 *sequences may by cyclically identified.*

The number of reachable configurations may now be found by enumerating the configurations defined by Lemma 5.1. This problem is analogous to the enumeration of legal sentences in a formal language. As a simple example of the techniques required (e.g. [14]), consider the enumeration of strings of N symbols 0 or 1 in which no sequence 111 appears (no periodicity is assumed). Let the number of such strings be α. In addition, let β_N be the number of length N strings containing no 111 sequences in their first $N-1$ positions, but terminating with the sequence 111. Then

$$\beta_0=\beta_1=\beta_2=0, \quad \beta_3=1, \quad \alpha_0=1, \quad \alpha_1=2, \tag{5.4a}$$

and

$$2\alpha_N = \alpha_{N+1} + \beta_{N+1} \quad (N \geqq 0), \tag{5.4b}$$

$$\alpha_N = \beta_{N+1} + \beta_{N+2} + \beta_{N+3} \quad (N \geqq 0). \tag{5.4c}$$

The recurrence relations (5.4) may be solved by a generating function technique. With

$$A(z) = \sum_{n=0}^{\infty} \alpha_n z^n, \qquad B(z) = \sum_{n=0}^{\infty} \beta_n z^n, \tag{5.5a}$$

Eq. (5.4) may be written as

$$2A(z) = z^{-1}(A(z) - 1) + z^{-1}B(z),$$

$$A(z) = z^{-3}B(z) + z^{-2}B(z) + z^{-1}B(z).$$

Solving these equations yields the result

$$A(z) = \frac{1 + z + z^2}{1 - z - z^2 - z^3}. \tag{5.5b}$$

Results for specific N are obtained as the coefficients of z^N in a series expansion of $A(z)$. Taking

$$A(z) = \frac{A_N(z)}{A_D(z)},$$

Eq. (5.5a) may be inverted to yield

$$\alpha_N = \sum_i \left(\frac{-A_N(z_i)}{z_i A_D'(z_i)} \right) (1/z_i)^N, \tag{5.5c}$$

where the z_i are the roots of $A_D(z)$ (all assumed distinct), and prime denotes differentiation. This yields finally

$$\alpha_N \simeq 1.14(1.84)^N + 0.283(0.737)^N \cos(2.176N + 2.078). \tag{5.6}$$

The behaviour of the coefficients for large N is dominated by the first term, associated with the smallest root of $A_D(N)$. The first ten values of α_N are 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, 504.

A lengthy calculation shows that the number of possible strings of length N which do not satisfy the conditions in Lemma 5.1, and may therefore be reached by evolution of the cellular automaton defined by Eq. (5.3), is given as the coefficient of z^N in the expansion of the generating function

$$P(z) = \frac{z - 3z^2 + 6z^3 - 8z^4 + 4z^5 - z^7}{1 - 4z + 6z^2 - 5z^3 + 2z^4 + z^5 - z^6 + z^7}$$

$$= \frac{3 - 4z + z^2}{1 - 2z + z^2 - z^3} - \frac{2 - z}{2(1 - z + z^2)} + \frac{2 - z}{2(-1 + z + z^2)} - 1. \tag{5.7}$$

Inverting according to Eq. (5.5c), the number of reachable configurations of length N is given by

$$\varrho_N = \kappa^N - (\phi^N + (-\phi)^{-N}) - \cos(N\pi/3) + 2\mu^N \cos(N\theta), \tag{5.8}$$

Table 3. Fraction of configurations appearing in cycles for the non-additive cellular automaton of Eq. (5.2)

N	ϱ_N^∞
4	0.3125
5	0.3438
6	0.1094
7	0.0078
8	0.1133
9	0.1426
10	0.0791
11	0.0435
12	0.0466
13	0.0350
14	0.0163
15	0.00308
16	0.00850
17	0.00857

where $\kappa \simeq 1.7548$ is the real root of $z^3 - z^2 + 2z - 1 = 0$, $\phi = (1+\sqrt{5})/2 = 1.6182$, and $\mu \simeq 0.754$, $\theta \simeq 1.408$. The first ten values of ϱ_N are 1, 1, 4, 7, 11, 19, 36, 67, 121, 216. For large N, $\varrho_N \sim \kappa^N$. Equation (5.8) shows that corrections decrease rapidly and smoothly with N. This behaviour is to be contrasted with the irregular behaviour as a function of N found for additive cellular automata in Theorems 3.1 and 4.2.

Equation (5.8) shows that the fraction of all 2^N possible configurations which are reachable after one time step in the evolution of the cellular automaton of Eq. (5.2) is approximately $(\kappa/2)^N \simeq 0.92^N$. Thus, starting from an initial maximal entropy ensemble with $s=1$, evolution for one time step according to Eq. (5.2) yields a set entropy

$$s(t=1) \simeq \log_2 \kappa \simeq 0.88\,. \tag{5.9}$$

The irregularity of the transient trees illustrated in Fig. 5 implies a measure entropy $s_\mu < s$.

The result (5.9) becomes exact in the limit $N \to \infty$. A direct derivation in this limit is given in [17, 18], where it is also shown that the set of infinite configurations generated forms a regular formal language. The set continues to contract with time, so that the set entropy decreases below the value given by Eq. (5.9) [18].

Techniques similar to those used in the derivation of Eq. (5.5) may in principle be used to deduce the number of configurations reached after any given number of steps in the evolution of the cellular automaton (5.2). The fraction of configurations which appear in cycles is an irregular function of N; some results for small N are given in Table 3.

6. Discussion

The analysis of additive cellular automata in Sects. 3 and 4 yielded results on the global behaviour of additive cellular automata more complete than those available for most other dynamical systems. The extensive analysis was made possible by the discrete nature of cellular automata, and by the additivity property which led to the algebraic approach developed in Sect. 3. Similar algebraic techniques should be applicable to some other discrete dynamical systems.

The analysis of global properties of cellular automata made in this paper complements the analysis of local properties of ref. [1].

One feature of the results on additive cellular automata found in Sects. 3 and 4, is the dependence of global quantities not only on the magnitude of the size parameter N, but also on its number theoretical properties. This behaviour is shared by many dynamical systems, both discrete and continuous. It leads to the irregular variation of quantities such as cycle lengths with N, illustrated in Table 1 and Fig. 3. In physical realizations of cellular automata with large size N, an average is presumably performed over a range of N values, and irregular dependence on N is effectively smoothed out. A similar irregular dependence is found on the number k of possible values for each site: simple results are found only when k is prime.

Despite such detailed dependence on N, results such as Theorem 4.1–4.3 show that global properties of additive cellular automata exhibit a considerable universality, and independence of detailed aspects of their construction. This property is again shared by many other dynamical systems. It potentially allows for generic results, valid both in the simple cases which may easily be analysed, and in the presumably complicated cases which occur in real physical systems.

The discrete nature of cellular automata makes possible an explicit analysis of their global behaviour in terms of transitions in the discrete phase space of their configurations. The results of Sect. 4 provide a rather complete characterization of the structure of the state transition diagrams for additive cellular automata. The state transition diagrams consists of trees corresponding to irreversible "transients", leading to "attractors" in the form of distinct finite cycles. The irreversibility of the cellular automata is explicitly manifest in the convergence of several distinct configurations to single configurations through motion towards the roots of the trees. This irreversibility leads to a decrease in the entropy of an initially equiprobable ensemble of cellular automaton configurations; the results of Sect. 4 show that in most cases the entropy decreases by a fixed amount at each time step, reflecting the balanced nature of the trees. Theorem 4.3 gives an algebraic characterization of the magnitude of the irreversibility, in terms of the in-degrees of nodes in the trees. The length of the transients during which the entropy decreases is given by the height of the trees in Theorem 4.3, and is found always to be less than N. After these transients, any initial configurations evolve to configurations on attractors or cycles. Theorem 4.3 gives the total number of configurations on cycles in terms of N and algebraic properties of the cellular automaton time evolution polynomial. At one extreme, all configurations may be on cycles, while at the other extreme, all initial configurations may evolve to a single limit point consisting simply of the null configuration.

Theorem 4.1 gives a rather general result on the lengths of cycles in additive cellular automata. The maximum possible cycle length is found to be of order the square root of the total number of possible configurations. Rather long cycles are therefore possible. No simple results on the total number of distinct cycles or attractors were found; however, empirical results suggest that most cycles have a length equal to the maximal length for a particular cellular automaton.

The global properties of additive cellular automata may be compared with those of other mathematical systems. One closely related class of systems are linear feedback shift registers. Most results in this case concentrate on analogues of the cellular automaton discussed in Sect. 3, but with the values at a particular time step in general depending on those of a few far-distant sites. The boundary conditions assumed for feedback shift registers are typically more complicated than the periodic ones assumed for cellular automata in Sect. 3 and most of Sect. 4. The lack of symmetry in these boundary conditions allows for maximal length shift register sequences, in which all 2^N-1 possible configurations occur on a single cycle [2, 3].

A second mathematical system potentially analogous to cellular automata is a random mapping [15]. While the average cycle length for random mappings is comparable to the maximal cycle length for cellular automata, the probability for a node in the state transition diagram of a random mapping to have in-degree d is $\sim 1/d!$ and is much more sharply peaked at low values than for a cellular automaton, leading to many differences in global properties.

Non-additive cellular automata are not amenable to the algebraic techniques used in Sects. 3 and 4 for the additive case. Section 5 nevertheless discussed some properties of non-additive cellular automata concentrating on a simple one-dimensional example with two possible values at each site. Figure 5 indicates that the state transition diagrams for such non-additive cellular automata are less regular than those for additive cellular automata. Combinatorial methods were nevertheless used to derive the fraction of configurations with no predecessors in these diagrams, giving the irreversibility and thus entropy decrease associated with one time step in the cellular automaton evolution. Unlike the case of additive cellular automata, the result was found to be a smooth function of N.

Appendix A: Notations and Elementary Results on Finite Fields

Detailed discussion of the material in this appendix may be found in [8].

A. Basic Notations

$a \bmod b$ denotes a reduced modulo b, or the remainder of a after division by b.

(a, b) or $\gcd(a, b)$ denotes the greatest common divisor of a and b. When a and b are polynomials, the result is taken to be a polynomial with unit leading coefficient (monic).

$a|b$ represents the statement that a divides b (with no remainder).

$a^n \| b$ indicates that a^n is the highest power of a which divides b.

Exponentiation is assumed right associative, so that a^{b^c} denotes $a^{(b^c)}$ not $(a^b)^c$.

p usually denotes a prime integer.

$\mathbb{R}_k$ denotes an arbitrary commutative ring of k elements.

$\mathbb{Z}_k$ denotes the ring of integers modulo k.

$\deg P(x)$ denotes the highest power of x which appears in $P(x)$.

B. Finite Fields

There exists a finite field unique up to isomorphism with any size p^α (p prime), denoted $\mathrm{GF}(p^\alpha)$. p is termed the characteristic of the field.

The ring $\mathbb{Z}_k$ of integers modulo k forms a field only when k is prime, since only in this case do unique inverses under multiplication modulo k exist for all nonzero elements. (For example, in $\mathbb{Z}_4$, 2 has no inverse.) $\mathrm{GF}(p)$ is therefore isomorphic to $\mathbb{Z}_p$.

The field $\mathrm{GF}(p^\alpha)$ is conveniently represented by the set of polynomials of degree less than α with coefficients in $\mathbb{Z}_p$, with all polynomial operations performed modulo a fixed irreducible polynomial of degree α over $\mathrm{GF}(p)$. For example, $\mathrm{GF}(4)$ may be represented by elements 0, 1, κ, $\kappa+1$ with operations performed modulo 2 and modulo $\kappa^2+\kappa+1$. In this case for example $\kappa\times\kappa\equiv\kappa+1$. Notice that, as mentioned in Sect. A.C below, polynomials over a field form a unique factorization domain.

Any field of size q yields a group of size $q-1$ under multiplication if the zero element is removed. Thus for any element of $\mathrm{GF}(q)$,

$$x^q=x\,, \tag{A.1}$$

and $x^{q-1}=1$ for $x\neq 0$. Notice that if $x\in\mathrm{GF}(p^\alpha)$ and $x^{p^\beta}=x$, then $x\in\mathrm{GF}(p^\beta)$.

C. Polynomials over Finite Fields

Polynomials in any number of variables with coefficients in $\mathrm{GF}(q)$ form a unique factorization domain. For such polynomials, therefore $A(x)B(x)\equiv A(x)C(x)\bmod P(x)$ implies $B(x)\equiv C(x)\bmod P(x)$ if $A(x), P(x))=1$.

For any polynomials $A(x)$ and $B(x)$ with coefficients in $\mathrm{GF}(q)$, there exist polynomials $\alpha(x)$ and $\beta(x)$ such that

$$C(x)=(A(x),B(x))=\alpha(x)A(x)+\beta(x)B(x)\,. \tag{A.2}$$

There are exactly q^n univariate polynomials over $\mathrm{GF}(q)$ with degree less than n. With a polynomial $Q(x)$ of degree m, the number of polynomials $P(x)$ with degree not exceeding n for which $Q(x)|P(x)$ is q^{n-m} for $m\leqq n$.

For any prime p, and for elements a_i of $\mathrm{GF}(p^\beta)$,

$$\left(\sum a_i x^i\right)^{p^\alpha}=\sum (a_i x^i)^{p^\alpha}\,. \tag{A.3}$$

Thus for example,

$$(x^{2^\alpha}+1)\equiv(x+1)^{2^\alpha} \quad \bmod 2\,, \tag{A.4}$$

a result used extensively in Sect. 3.

If $P(x)|Q(x)$, then every root of $P(x)$ must be a root of $Q(x)$. If $\lambda\geqq 2$ and

$$[P(x)]^\lambda \mid Q(x)\,, \tag{A.5}$$

then

$$P(x)\mid Q'(x)\,, \tag{A.6}$$

where $Q'(x)$ is the formal derivative of $Q(x)$, obtained by differentiation of each term in the polynomial. [Note that integration is not defined for polynomials over $\mathrm{GF}(q)$.]

The number of roots (not necessarily distinct) of a polynomial over GF(q) is equal to the degree of the polynomial. The roots may lie in an extension of GF(q).

Over the field GF(p),

$$x^N - 1 = (x^n - 1)^{D_p(N)}, \tag{A.7}$$

where $N = D_p(N)n$, with $D_p(N)$ defined in Sects. 3 and 4 as the maximum power of p which divides N. The polynomial $x^n - 1$ with n not a multiple of p then factorizes over GF(p) according to

$$x^n - 1 = (x - 1) \prod_{\substack{d|n \\ d \neq 1}} \prod_{i=1}^{\frac{\phi(d)}{\mathrm{ord}_d(p)}} C_{d,i}(x), \tag{A.8}$$

where the $C_{d,i}(x)$ are irreducible cyclotomic polynomials of degree $\mathrm{ord}_d(p)$. Note that the multiplicity of any irreducible factor of $x^N - 1$ is exactly $D_p(N)$, and that

$$C_{d,i}(x) \mid x^d - 1. \tag{A.9}$$

D. Dipolynomials over Finite Fields

A dipolynomial $A(x)$ is taken to divide a dipolynomial $B(x)$ if there exists a dipolynomial $C(x)$ such that $B(x) = A(x)C(x)$. Hence if $A(x)$ and $B(x)$ are polynomials, with $A(0) \neq 0$, and if $A(x) \mid B(x)$ are dipolynomials, then $A(x) \mid B(x)$ are polynomials.

Congruence in the ring of dipolynomials is defined as follows: $A(x) \equiv B(x) \bmod C(x)$ for dipolynomials $A(x)$, $B(x)$, and $C(x)$ if $C(x) \mid A(x) - B(x)$.

The greatest common divisor of two nonzero dipolynomials $A_1(x)$ and $A_2(x)$ is defined as the ordinary polynomial $(A_1^*(x), A_2^*(x))$, where $A_i^*(x) = x^{m_i} A_i(x)$ and m_i is chosen to make $A_i^*(x)$ a polynomial with nonzero constant term. Note that by analogy with Eq. (A.2), for any dipolynomials $A_1(x)$ and $A_2(x)$, there exist dipolynomials $\alpha_1(x)$ and $\alpha_2(x)$ such that

$$(A_1(x), A_2(x)) = \alpha_1(x)A_1(x) + \alpha_2(x)A_2(x). \tag{A.10}$$

Appendix B: Properties and Values of some Number Theoretical Functions

A. Euler Totient Function $\phi(N)$

$\phi(N)$ is defined as the number of integers less than N which are relatively prime to N [7]. $\phi(N)$ is a multiplicative function, so that

$$\phi(mn) = \phi(m)\phi(n), \quad (m, n) = 1. \tag{B.1}$$

For p prime,

$$\phi(p^\alpha) = p^{\alpha-1}(p-1). \tag{B.2}$$

Hence

$$\phi(n) = \prod_{p^\alpha \| n} p^{\alpha-1}(p-1), \tag{B.3}$$

providing a formula by which $\phi(N)$ may be computed. Some values of $\phi(N)$ are given in Table 4.

$\phi(N)$ is bounded (for $N>1$) by

$$cN/\log\log N \leqq \phi(N) \leqq N-1\,, \tag{B.4}$$

where c is some positive constant, and the upper bound is achieved if and only if N is prime. For large N, $\phi(N)/N$ tends on average to a constant value.

$\phi(n)$ satisfies the Euler-Fermat theorem

$$k^{\phi(n)}=1 \quad \mathrm{mod}\, n \quad (k,n)=1\,. \tag{B.5}$$

B. Multiplicative Order Function $\mathrm{ord}_N(k)$

The multiplicative order function $\mathrm{ord}_N(k)$ is defined as the minimum positive integer j for which [8]

$$k^j=1 \quad \mathrm{mod}\, N\,. \tag{B.6}$$

This condition can only be satisfied if $(k,N)=1$.

By the Euler-Fermat theorem (B.5),

$$\mathrm{ord}_N(k)\,|\,\phi(N)\,. \tag{B.7}$$

In addition, $\mathrm{ord}_{mn}(k)=\mathrm{lcm}(\mathrm{ord}_n(k),\ \mathrm{ord}_m(k))$, $(n,k)=(m,k)=(n,m)=1$. Some special cases are

$$\mathrm{ord}_{k^\alpha-1}(k)=\alpha\,,$$

$$\mathrm{ord}_{k^\alpha+1}(k)=2\alpha\,.$$

A rigorous bound on $\mathrm{ord}_N(k)$ is

$$\log_k(N) \leqq \mathrm{ord}_N(k) \leqq N-1\,, \tag{B.8}$$

where the upper bound is attained only if N is prime. It can be shown that on average, for large N, $\mathrm{ord}_N(k) \gtrsim \sqrt{N}$; the actual average is presumably closer to N. Nevertheless, for large N, $\mathrm{ord}_N(k)/N$ tends to zero on average.

Some values of the multiplicative order function are given in Table 4.

The multidimensional generalization $\mathrm{ord}_{N_1,\ldots,N_d}(k)$ of the multiplicative order function is defined as the minimum positive integer j for which $k^j=1$ simultaneously modulo $N_1, N_2, \ldots$, and N_d. It is clear that

$$\begin{gathered}\mathrm{ord}_{N_1,\ldots,N_d}(k)=\mathrm{lcm}(\mathrm{ord}_{N_1}(k),\ \ldots,\ \mathrm{ord}_{N_d}(k))=\mathrm{ord}_{\mathrm{lcm}(N_1,\ldots,N_d)}(k)\,,\\ (k,N_1)=\ \ldots\ =(k,N_d)=1\,.\end{gathered} \tag{B.9}$$

C. Multiplicative Suborder Function $\mathrm{sord}_N(k)$

The multiplicative suborder function is defined as the minimum j for which

$$k^j=\pm 1\, \mathrm{mod}\, N\,, \tag{B.10}$$

again assuming $(k,N)=1$. Comparison with (B.6) yields

$$\mathrm{sord}_N(k)=\mathrm{ord}_N(k)\,, \tag{B.11a}$$

or

$$\mathrm{sord}_N(k)=\tfrac{1}{2}\mathrm{ord}_N(k)\,. \tag{B.11b}$$

The second case becomes comparatively rare for large N; the fraction of integers less than X for which it is realised may be shown to be asymptotic to $c/[\log X]^\lambda$

Table 4. Values of the multiplicative order $\mathrm{ord}_N(k)$ and suborder $\mathrm{sord}_N(k)$ functions defined in Eqs. (B.6) and (B.10), respectively, together with values of the Euler totient function $\phi(N)$. Each column gives values of the pair $\mathrm{ord}_N(k)$, $\mathrm{sord}_N(k)$

N	$k=2$		$k=3$		$k=4$		$k=5$		$\phi(N)$
1									1
2			1	1			1	1	1
3	2	1			1	1	2	1	2
4			2	1			1	1	2
5	4	2	4	2	2	1			4
6							2	1	2
7	3	3	6	3	3	3	6	3	6
8			2	2			2	2	4
9	6	3			3	3	6	3	6
10			4	2					4
11	10	5	5	5	5	5	5	5	10
12							2	2	4
13	12	6	3	3	6	3	4	2	12
14			6	3			6	3	6
15	4	4			2	2			8
16			4	4			4	4	8
17	8	4	16	8	4	2	16	8	16
18							6	3	6
19	18	9	18	9	9	9	9	9	18
20			4	4					8
21	6	6			3	3	6	3	12
22			5	5			5	5	10
23	11	11	11	11	11	11	22	11	22
24							2	2	8
25	20	10	20	10	10	5			20
26			3	3			4	2	12
27	18	9			9	9	18	9	18
28			6	3			6	6	12
29	28	14	28	14	14	7	14	7	28
30									8
31	5	5	30	15	5	5	3	3	30
32			8	8			8	8	16
33	10	5			5	5	10	10	20
34			16	8			16	8	16
35	12	12	12	12	6	6			24
36							6	6	12
37	36	18	18	9	18	9	36	18	36
38			18	9			9	9	18
39	12	12			6	6	4	4	24
40			4	4					16

[16], where c and λ are constants determined by k.

In general,

$$\log_k(N) \leqq \mathrm{sord}_N(k) \leqq (N-1)/2\,, \tag{B.12}$$

the upper limit again being achieved only if N is prime. For large N, $\mathrm{sord}_N(k)/N \to 0$ on average.

The multidimensional generalization $\mathrm{sord}_{N_1,\ldots,N_d}(k)$ of the multiplicative suborder function is defined as the minimum positive integer j for which $k^j = \pm 1$ simultaneously modulo $N_1, \ldots, N_d$, with $+1$ and -1 perhaps taken variously for the different N_i. The analogue of Eq. (B.9) for this function is

$$\mathrm{sord}_{N_1,\ldots,N_d}(k) = \mathrm{lcm}(\mathrm{sord}_{N_1}(k), \ldots, \mathrm{sord}_{N_d}(k)), \tag{B.13a}$$

and

$$\mathrm{lcm}(\mathrm{sord}_{N_1}(k), \ldots, \mathrm{sord}_{N_d}(k)) = \mathrm{sord}_{\mathrm{lcm}(N_1,\ldots,N_d)}(k), \tag{B.13b}$$

or

$$\mathrm{lcm}(\mathrm{sord}_{N_1}(k), \ldots, \mathrm{sord}_{N_d}(k)) = \tfrac{1}{2}\mathrm{sord}_{\mathrm{lcm}(N_1,\ldots,N_d)}(k). \tag{B.13c}$$

Acknowledgement. We are grateful to O. E. Lanford for several suggestions.

References

1. Wolfram, S.: Statistical mechanics of cellular automata. Rev. Mod. Phys. **55**, 601 (1983)
2. Golomb, S.W.: Shift register sequences. San Francisco: Holden-Day 1967
3. Selmer, E.S.: Linear recurrence relations over finite fields. Dept. of Math., Univ. of Bergen, Norway (1966)
4. Miller, J.C.P.: Periodic forests of stunted trees. Philos. Trans. R. Soc. Lond. A**266**, 63 (1970); A**293**, 48 (1980)
   ApSimon, H.G.: Periodic forests whose largest clearings are of size 3. Philos. Trans. R. Soc. Lond. A**266**, 113 (1970)
   ApSimon, H.G.: Periodic forests whose largest clearings are of size $n \geqq 4$. Proc. R. Soc. Lond. A**319**, 399 (1970)
   Sutton, C.: Forests and numbers and thinking backwards. New Sci. **90**, 209 (1981)
5. Moore, E.F.: Machine models of self-reproduction. Proc. Symp. Appl. Math. **14**, 17 (1962) reprinted in: Essays on cellular automata, A. W. Burks. Univ. of Illinois Press (1966)
   Aggarwal, S.: Local and global Garden of Eden theorems. Michigan University technical rept. 147 (1973)
6. Knuth, D.: Fundamental algorithms, Reading, MA: Addison-Wesley 1968
7. Hardy, G.H., Wright, E.M.: An introduction to the theory of numbers. Oxford: Oxford University Press 1968
8. Mac Williams, F.J., Sloane, N.J.A.: The theory of error-correcting codes. Amsterdam: North-Holland 1977
9. Griffiths, P., Harris, J.: Principles of algebraic geometry. New York: Wiley 1978
10. Fredkin, E., Margolus, N.: Private communications
11. Ronse, C.: Non-linear shift registers: A survey. MBLE Research Lab. report, Brussels (May 1980)
12. Harao, M., Noguchi, S.: On some dynamical properties of finite cellular automaton. IEEE Trans. Comp. C-**27**, 42 (1978)
13. Grassberger, P.: A new mechanism for deterministic diffusion. Phys. Rev. A (to be published)
14. Guibas, L.J., Odlyzko, A.M.: String overlaps, pattern matching, and nontransitive games. J. Comb. Theory (A) **30**, 83 (1981)
15. Knuth, D.: Seminumerical algorithms. 2nd ed. Reading, MA: Addison-Wesley 1981
    Gelfand, A.E.: On the cyclic behavior of random transformations on a finite set. Tech. rept. 305, Dept. of Statistics, Stanford Univ. (August 1981)
16. Odlyzko, A.M.: Unpublished

17. Lind, D.A.: Applications of ergodic theory and sofic systems to cellular automata. Physica D **10** (to be published)
18. Wolfram, S.: Computation theory of cellular automata. Institute for Advanced Study preprint (January 1984)
19. Lenstra, H.W., Jr.: Private communication

Communicated by O.E. Lanford

Received February 11, 1983; in revised form September 7, 1983