

Predecessor States for Certain Cellular Automata Evolutions

Burton Voorhees

Faculty of Arts and Sciences, Athabasca University, Box 10,000, Athabasca, Alberta, Canada T0G 2R0

Abstract. This paper reports the solution of the problem of finding which inputs for a function of discrete variables will result in any specified output for the set of binomially determined nearest neighbor additive cellular automata defined on finite or half-infinite sequences. In computing the solution to this problem a process which is the discrete analog to backward integration is defined. This process is determined in terms of an operator which exhibits an interesting period multiplying property.

I. Introduction

A cellular automaton consists of a finite or infinite lattice with values at each lattice site drawn from a discrete set, together with a deterministic local rule which specifies the site values at time $t + 1$ in terms of site values at time t . They were initially introduced by Von Neumann [1] in an attempt to find simple mathematical systems which exhibited some features of life. Applications of cellular automata have been made in modeling heart fibrillation [2]; as parallel processors [3,4]; as prime number sieves [5]; in image processing and pattern recognition [6,7]. More recently, work of Wolfram [8,9,10] has stimulated a renewal of interest (see, e.g., papers in Physica 10D) and it has been suggested [11] that cellular automata may have a major role to play “complexity engineering;” i.e., in the design of complex systems which exhibit specific properties.

Before such applications can be realized, however, there are several problems which must be solved. One of these is the predecessor problem [11]: is it possible to determine the predecessor states for any given state of an arbitrary cellular automata? As Wolfram points out, there may be no general solution to this problem as it is, in the general case, NP-complete.

This paper presents the solution to the predecessor problem for the special case of binomially determined nearest neighbor additive cellular automata defined over Z_p , where p is prime. Although this is a limited subset of the set of all cellular automata, the solution presented is significant for several reasons: it is a first step in attack on the general case; it is a direct analog of backwards integration; an interesting period multiplying property emerges; and, most of the current results appearing in the literature are based on analysis of additive cellular automata—

indeed, the algebraic approach in terms of characteristic polynomials developed by Martin et al. [12] works only for this subset.

The solution presented is based on a new approach to analysis of cellular systems in terms of operators on an appropriate state space [13,14]. The basic idea behind this approach is sketched in Sect. II. Section III introduces an operator B and indicates how, for certain nearest neighbor additive cellular automata a process defined in terms of this operator, analogues to backwards integration, yields all possible predecessor states for any given automata state. The analogy to integration suggests that, although there may not be any general procedure for “inverting” cellular automata evolution, it may be possible to find particular procedures for other classes of cellular automata than those dealt with in this paper.

II. Nearest Neighbor Additive Cellular Automata

We first consider finite automata. Let p be prime. A finite cellular automata over \mathbf{Z}_p is represented as a set of n cells located on a circle. Each cell contains a value chosen from \mathbf{Z}_p . If the value of cell i at time $t + 1$ is determined only on the basis of the values of cells $i - 1$, i , and $i + 1$ at time t then the automaton follows a nearest neighbor rule. The set of p^n possible automaton states is denoted E_n . The evolution rule for a given automaton is naturally represented as an operator $Q: E_n \rightarrow E_n$ [13]. In this approach a particular automaton, with evolution rule represented by an operator Q , is denoted (Q, E_n) . If, for all μ, μ' in E_n , and all k , $Q^k(\mu + \mu') = Q^k(\mu) + Q^k(\mu')$, then Q is said to be additive.

If μ_i denotes the value of the i^{th} cell in the state μ then the general component form for the operator representing an additive nearest neighbor rule is

$$[Q(\mu)]_i = x\mu_{i-1} + y\mu_i + z\mu_{i+1}, \tag{II.1}$$

where x, y , and z take values in \mathbf{Z}_p and all sums and products are reduced modulo p . (Note, however, that subscripted component indices are reduced modulo n corresponding to periodic boundary conditions.) There are p^3 distinct operators Q defined by (II.1). If I is the identity on E_n and σ^{-1}, σ are respectively the right and left shift operators, then (II.1) is equivalent to the operator equation

$$Q = x\sigma^{-1} + yI + z\sigma, \tag{II.2}$$

which yields

$$Q^k = \sum_{r,s=0}^{r+s \leq k} T_{rs}(k+1)x^r y^{k-r-s} z^s \sigma^s \sigma^{-r} \tag{II.3}$$

in which the $T_{rs}(k+1)$ are the trinomial coefficients of $(x + y + z)^k$ reduced modulo p . In component form this becomes

$$[Q^k(\mu)]_i = \sum_{r,s=0}^{r+s \leq k} T_{rs}(k+1)x^r y^{k-r-s} z^s \mu_{(i-r+s)}. \tag{II.4}$$

If only one of x, y, z is non-zero, then Q will be a combination of a multiplication and a shift. (If y is the non-zero element this is only a multiplication.) If two of x, y, z are non-zero the coefficients in (II.4) reduce to the entries in the $(k + 1)$ -st

row of Pascal's triangle modulo p . Such automata will be said to be binomially determined.

For $p = 2$ and 3 the possible additive operators are shown in Tables 1 and 2, respectively.

Following the notation used in Tables 1 and 2 we define operators $D_{(r,s)}$ and $D^-_{(r,s)}$ on E_n by $D_{(r,s)} = rI + s\sigma$ and $D^-_{(r,s)} = rI + s\sigma^{-1}$.

Now consider a state space E^+ which consists of all right half-infinite sequences of values drawn from \mathbf{Z}_p . (By reflection symmetry similar results will hold for the state space E^- of all left half-infinite sequences.) Since these sequences are bounded on the left some of the operators defining specific automaton evolutions must be

Table 1. $p = 2$ Nearest Neighbor Additive Cellular Automata

(x, y, z)	Operator	Component Form	Rule *(Wolfram, [8])
$(0, 0, 0)$	0	$[0(\mu)]_i = 0$	0
$(1, 0, 0)$	σ^{-1}	$[\sigma^{-1}(\mu)]_i = \mu_{i-1}$	240
$(0, 1, 0)$	I	$[I(\mu)]_i = \mu_i$	204
$(0, 0, 1)$	σ	$[(\mu)]_i = \mu_{i+1}$	170
$(1, 1, 0)$	D^-	$[D^-(\mu)]_i = \mu_i + \mu_{i-1}$	60
$(0, 1, 1)$	D	$[D(\mu)]_i = \mu_i + \mu_{i+1}$	102
$(1, 0, 1)$	D^-D	$[D^-D(\mu)]_i = \mu_{i-1} + \mu_{i+1}$	90
$(1, 1, 1)$	Δ	$[\Delta(\mu)]_i = \mu_{i-1} + \mu_i + \mu_{i+1}$	150

Table 2. $p = 3$ Nearest Neighbor Additive Cellular Automata

(x, y, z)	Operator	Component Form
The cases for which (x, y, z) take values in $[0, 1]$ are identical to those given in Table 1 with the exception of the operator D^-D . Operators which are multiples of $p = 2$ operators are: $(2, 0, 0)$, $(0, 2, 0)$, $(0, 0, 2)$, $(2, 2, 0)$, $(0, 2, 2)$, and $(2, 2, 2)$. $(2, 0, 2) = 2\partial$.		
$(1, 0, 1)$	∂	$[\partial(\mu)]_i = \mu_{i-1} + \mu_{i+1}$
$(2, 1, 0)$	$D^-_{(1,2)}$	$[D^-_{(1,2)}(\mu)]_i = \mu_i + 2\mu_{i-1}$
$(0, 2, 1)$	$D_{(2,1)}$	$[D_{(2,1)}(\mu)]_i = 2\mu_i + \mu_{i+1}$
$(1, 0, 2)$	$D^-_{(2,1)}D$	$[D^-_{(2,1)}D(\mu)]_i = \mu_{i-1} + 2\mu_{i+1}$
$(2, 0, 1)$	$D^-D_{(2,1)}$	$[D^-D_{(2,1)}(\mu)]_i = 2\mu_{i-1} + \mu_{i+1}$
$(0, 1, 2)$	$D_{(1,2)}$	$[D_{(1,2)}(\mu)]_i = \mu_i + 2\mu_{i+1}$
$(1, 2, 0)$	$D^-_{(2,1)}$	$[D^-_{(2,1)}(\mu)]_i = \mu_{i-1} + 2\mu_i$
$(2, 1, 1)$	$\Delta + \sigma^{-1}$	$[(\Delta + \sigma^{-1})(\mu)]_i = 2\mu_{i-1} + \mu_{i+1}$
$(1, 2, 1)$	$I + \Delta$	$[(I + \Delta)(\mu)]_i = \mu_{i-1} + 2\mu_i + \mu_{i+1}$
$(1, 1, 2)$	$\Delta + \sigma$	$[(\Delta + \sigma)(\mu)]_i = \mu_{i-1} + \mu_i + 2\mu_{i+1}$
$(2, 2, 1)$	$\Delta + D^-$	$[(\Delta + D^-)(\mu)]_i = 2\mu_{i-1} + 2\mu_i + \mu_{i+1}$
$(2, 1, 2)$	$\Delta + \partial$	$[(\Delta + \partial)(\mu)]_i = 2\mu_{i-1} + \mu_i + 2\mu_{i+1}$
$(1, 2, 2)$	$\Delta + D$	$[(\Delta + D)(\mu)]_i = \mu_{i-1} + 2\mu_i + 2\mu_{i+1}$

redefined. The operator σ^{-1} is defined on E^+ by

$$[\sigma^{-1}(\mu)]_i = \begin{cases} \mu_{i-1} & i > 1 \\ 0 & i = 1 \end{cases} \tag{II.5}$$

All operators defined in terms of σ^- are similarly modified.

The spaces E_n embed in E^+ as the subspaces of all half-infinite sequences with period n , and properties of operators not involving σ^- in their definition are preserved from the finite case.

III. The Operator B and the Predecessor Problem

Let (Q, E^+) be as described in Sect. II. In general the map $Q: E^+ \rightarrow E^+$ may have several attracting sets. If C is an attractor of this map we wish to discover the set M_C having the property that for all μ in E^+ , μ is in M_C if and only if there is a $k > 0$ such that $Q^k(\mu)$ is in C . That is, we want the basin of attraction of C . The solution of this problem is presented in several steps of increasing generality.

An operator $B: E^+ \rightarrow E^+$ is defined by

$$[B(\mu)]_i = \sum_{j=1}^i \mu_j \tag{III.1}$$

B cannot be defined on a finite automaton since if μ has period n then $B(\mu)$ will, under conditions to be made precise in Sect. IV, have period pn , requiring a p -fold covering. Nevertheless B is additive.

Under iteration B has components given by:

$$[B^k(\mu)]_i = \sum_{j=1}^i p^{(k+i-j)} \mu_j \tag{III.2}$$

where $p^{(k)}_i$ is the i^{th} entry of the k^{th} row of Pascal's triangle mod(p). The operator B can be shown to be self-accumulation (i.e., in the natural topology on E^+ continued iteration of B comes arbitrarily close to past iterates) but not solipsistic (i.e., B has accumulation points other than its own past iterates), and to have no dense orbits [14].

Theorem 1. *The general solution of $D_{(r,p-r)}(\mu) = \beta$ is*

$$\mu = bB\sigma^{-1}(\beta) + \mu_1 B(\alpha_1) \tag{III.4}$$

where α_1 has one in the first position and zero's in all other positions, μ_1 is an "initial condition" chosen from \mathbf{Z}_p , and b satisfies the conditions $1 \leq b < p$; $b(p-r) = 1 \pmod{p}$.

Proof. Let μ be the sequence $(\mu_1, \mu_1 + b_1\beta_1 + \pi_1, \mu_1 + b_1\beta_1 + b_2\beta_2 + \pi_2, \dots)$ having general term $\mu_1 + b_1\beta_1 + \dots + b_{i-1}\beta_{i-1} + \pi_{i-1}$, where μ_1 , the b_i , and the π_i are chosen from \mathbf{Z}_p . It is possible to write any sequence in E^+ in this form, although such representation is obviously not unique. The general term of $D_{(r,p-r)}(\mu)$ is computed to be $r\pi_{i-1} + (p-r)[b_i\beta_i + \pi_i]$. If μ is to be a solution this must equal β_i . Multiply by a number b which satisfies $0 < b < p$, $b(p-r) = 1 \pmod{p}$

to obtain $br\pi_{i-1} + b_i\beta_i + \pi_i = b\beta_i$. Since $b(p-r) = bp - br = 1 \pmod{p}$, $br = bp - 1 = -1$. Thus $\pi_i = \pi_{i-1} + (b - b_i)\beta_i$. Substituting this recursively into μ gives the general term of the solution μ as $\mu_i = \mu_1 + b(\beta_1 + \dots + \beta_{i-2} + \beta_{i-1})$, which is identical to (III.4). \parallel

The only free parameter in (III.4) is μ_1 which takes values in \mathbf{Z}_p . Hence there is an immediate consequence of Theorem 1:

Corollary. *There are exactly p distinct predecessor states for every state of the automaton $(D_{(r,p-r)}E^+)$, counting fixed points of $D_{(r,p-r)}$ as predecessors of themselves.*

Iteration of (III.4), noting that B and σ^{-1} commute, introducing a basis $\{\alpha_s | (\alpha_s)_i = \delta_{is}\}$ for E^+ , and observing that $\sigma^{-1}(\alpha_s) = \alpha_{s+1}$, yields

Theorem 2. *The general solution of $D_{(r,p-r)}^k(\mu) = \beta$ is*

$$\mu = b^k B^k \sigma^{-k}(\beta) + \sum_{s=1}^k \mu_s b^{s-1} B^s(\alpha_s). \tag{III.5}$$

The same methods used in the proofs of Theorems 1 and 2 can be used for the more general case of the operator $D_{(r,s)}$ with $1 \leq r, s < p$.

Theorem 3. *Let $0 < b, r, s < p$, and let b be such that $bs = 1 \pmod{p}$. Then the general solution of $D_{(r,s)}(\mu) = \beta$ is given by*

$$\mu = \mu_1 B_{(b,r)}(\alpha_1) + b B_{(b,r)} \sigma^{-1}(\beta), \tag{III.6}$$

where $B_{(b,r)}E^+ \rightarrow E^+$ is the operator defined by

$$[B_{(b,r)}(\beta)]_j = \sum_{j=1}^j [b(p-r)^{i-j} \beta_j]. \tag{III.7}$$

Theorem 4. *The general solution of $D_{(r,s)}^k(\mu) = \beta$ is given by*

$$\mu = b^k B_{(b,r)}^k \sigma^{-k}(\beta) + \sum_{j=1}^k \mu_j b^{j-1} B_{(b,r)}^j(\alpha_j), \tag{III.8}$$

where $0 < b < p$ and $bs = 1 \pmod{p}$.

Turning attention to $D_{(r,s)}^-$ we find by direct calculation that this operator commutes with $B_{(b,t)}$, and that

$$[B_{(b,t)} D_{(r,s)}^-(\mu)]_i = r\mu_i + [s + b(p-t)r] \sum_{j=1}^{i-1} [b(p-t)]^{i-j-1} \mu_j. \tag{III.9}$$

Choosing b and t such that $s + b(p-t)r = 0 \pmod{p}$, and a number c such that $cr = 1 \pmod{p}$ yields $cB_{(b,t)} D_{(r,s)}^- = 1$. Further, although there are several values of b and t which will satisfy the required condition it turns out, since all coefficients in the expansion of $B_{(b,t)}$ are powers of $b(p-r)$, that all choices of b and t which give $s + b(p-t)r = 0$ give the same form for the operator $B_{(b,t)}$. This yields:

Theorem 5. *Let $0 < b, c, t, r, s < p$ and let these numbers be chosen so that, modulo p , the relations $cr = 1$ and $s + b(p-t)r = 0$ are satisfied. Then $cB_{(b,t)}$ is the unique inverse of $D_{(r,s)}^-$.*

IV. Period Multiplication

Suppose that μ is periodic in E^+ with period n . By (III.7) the operator $B_{(b,r)}$ satisfies

$$[B_{(b,r)}(\mu)]_{i+1} = b(p-r)[B_{(b,r)}(\mu)]_i + \mu_{i+1}. \tag{IV.1}$$

On this basis it is possible to state a period multiplication theorem:

Theorem 6. *Let μ in E^+ have period n .*

1. *If $[B_{(b,r)}(\mu)]_n = 0$, then $B_{(b,r)}(\mu)$ also has period n .*
2. *If $[B_{(b,r)}(\mu)]_n \neq 0$, let k be the smallest positive integer such that $[B_{(b,r)}(\mu)]_{kn} = 0$.*

Then $B_{(b,r)}(\mu)$ has period kn .

For given n, b, r it is possible, on the basis of some elementary number theoretic considerations, to determine the value of k . If $p = 2$ the only possible value of (r, s) and (b, r) are $(1, 1)$. $B_{(1,1)} = B$ as defined in (III.1), and we write $D_{(1,1)} = D$, $D_{(1,1)}^- = D^-$.

Theorem 7. *For $p = 2$, let μ be a periodic element of E^+ with period n and define*

$$\mu_n^* = (\mu_1, \dots, \mu_n),$$

$$\#_1(\mu_n^*) = \text{number of ones in } \mu_n^* \text{ taken mod } (2).$$

1. *If $\#_1(\mu_n^*) = 1$, then $B(\mu)$ will have period $2n$.*
2. *If $\#_1(\mu_n^*) = 0$ then, for some $k(2 \leq k \leq n)$, $B^k(\mu)$ will have period $2n$.*

Proof. In mod (2) it is clear from the definition of the operator B that if $\#_1(\mu_n^*) = 1$ then $[B(\mu)]_n = 1$. Thus, for $n + 1 \leq i \leq 2n$ we can write the equality $[B(\mu)]_i = 1 + [B(\mu)]_{i-n}$. In particular, $[B(\mu)]_{2n} = 0$. Hence, for an index j satisfying $2n + 1 \leq j \leq 4n$ we have $[B(\mu)]_j = [B(\mu)]_{j-2n}$ so that $B(\mu)$ has period $2n$.

If $\#_1(\mu_n^*) = 0$ let $\mu_r(1 \leq r \leq n)$ be the last element of μ_n^* which equals 1. Then, since addition to an even number of ones equals zero, the last non-zero element of $\{[B(\mu)]_i | 1 \leq i \leq n\}$ will be, at most, $[B(\mu)]_{r-1}$. Let μ_s be the first non-zero element of μ_n^* . Then, for all k , $[B^k(\mu)]_s = 1$. No iteration of B can reduce all of the first n elements of $B^k(\mu)$ to zero unless $\mu = 0$. Thus, for some k between 1 and $r - s$, it must be the case that $\#_1(B^k(\mu)) = 1$. The desired result now follows by appeal to the first part of this theorem. \parallel

For p an odd prime suppose μ has period n in E^+ , $[B_{(b,r)}(\mu)]_n \neq 0$, and let k be the smallest positive integer such that $[B_{(b,r)}(\mu)]_{kn} = 0 \pmod{p}$. For simplicity of notation take $y = b(p-r)$ and $x = y^n$. Expansion of (111.7), taking note of the periodicity of μ , and rearranging terms now yields

$$0 = [B_{(b,r)}(\mu)]_{kn} = (1 + x + \dots + x^{k-1})(y^{n-1}\mu_1 + y^{n-2}\mu_2 + \dots + \mu_n). \tag{IV.2}$$

Thus at least one of the two factors on the right must be zero. But it cannot be the second factor since this would imply that $[B_{(b,r)}(\mu)]_{kn}$ was zero for all values of k and we have required that $[B_{(b,r)}(\mu)]_n \neq 0$. Therefore $1 + x + \dots + x^{k-1} = 0$. Further, by definition k is the smallest integer for which this is true. Addition of x^k to each side of this equation yields $x^k = 1 + x + \dots + x^{k-1} + x^k = 1 + x(1 + x + \dots + x^{k-1}) = 1$. In number theory x is said to have order k modulo p .

Lemma. *Let p be prime, $1 \leq x < p$. Then x has order $k > 1$ modulo p if and only if $1 + x + x^2 + \dots + x^{k-1} = 0$ modulo p .*

Proof. The if portion of the lemma has already been demonstrated. Suppose that x has order k modulo p , then $x + x^2 + \dots + x^k = 1 + x + x^2 + \dots + x^{k-1}$ or $x(1 + x + \dots + x^{k-1}) = 1 + x + \dots + x^{k-1}$. Thus $(x - 1)(1 + x + \dots + x^{k-1}) = 0 \pmod{p}$. If $x = 1$ then x has order 1 so if the order of x is to be greater than one $1 + x + \dots + x^{k-1} = 0$ and the lemma is demonstrated. \parallel

The only remaining case is $x = 1$. In this case $1 + x + \dots + x^{k-1} = k$ which must be zero mod(p) if $[B_{(b,r)}(\mu)]_{kn}$ is to be zero. The smallest positive value of k for which this is true is $k = p$. Thus we have:

Theorem 8. *Let μ have period n in E^+ , $[B_{(b,r)}(\mu)]_n \neq 0$, and $x = b^n(p - r)^n > 1$ have order k modulo p . Then $B_{(b,r)}(\mu)$ has period kn . If $x = 1 \pmod{p}$ then $B_{(b,r)}(\mu)$ has period pn .*

We briefly summarize some standard results of number theory [15]:

If $x \neq 1$ has order k modulo p , then $k|(p - 1)$; the number of distinct values of x with order k is given by $\phi(k)$, which ϕ is the Euler function; and

$$\sum_{k|(p-1)} \phi(k) = p - 1. \tag{IV.3}$$

Since $(p - 1)^2 = p^2 - 2p + 1 = 1 \pmod{p}$, $p - 1$ has order 2. Also, if x has order k , then $(p - x)^k = (-x)^k = (-1)^k$. Hence if k is even the order of $p - x$ divides k , while if k is odd $(p - x)^k = -1 = p - 1$ so the order of $p - x$ is $2k$. Table 3 illustrates the pattern of k values for $p \leq 17$.

Finally, let $x = b^n(p - r)^n$ have order k modulo p and consider the quantity

$$\lambda_i = \sum_{m=0}^{k-1} [B_{(b,r)}(\mu)]_{i+mn}. \tag{IV.4}$$

Table 3. Values of k for p prime, $3 \leq p \leq 17$

	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$	$p = 17$
2	2	4	3	10	12	8
3		4	6	5	3	16
4		2	3	5	6	4
5			6	5	4	16
6			2	10	12	16
7				10	12	16
8				10	4	8
9				5	3	8
10				2	6	16
11					12	16
12					2	16
13						4
14						16
15						8
16						2

That is, an element of E_n is defined by breaking $B_{(b,r)}(\mu)$ into k blocks of n elements each and summing elements which are congruent modulo n . After a good deal of computation, making extensive use of the periodicity of μ , we obtain

$$\lambda_i = \left[\sum_{m=1}^{k-1} (k-m)x^{m-1} \right] \sum_{j=i+1}^{i+n} y^{i+n-j} \mu_j. \tag{IV.5}$$

Denoting the constant term in brackets by K (IV.5) can be written as a matrix equation $\lambda = KY_\mu$,

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = K \begin{pmatrix} 1 & y^{n-1} & y^{n-2} & \cdots & y \\ y & 1 & y^{n-1} & \cdots & y^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y^{n-1} & y^{n-2} & y^{n-3} & \cdots & 1 \end{pmatrix} \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_n \end{pmatrix} \tag{IV.6}$$

The matrix Y is a circulant. It is easy to compute $\text{Det}(Y) = (1 - y^n)^{n-1}$. Suppose that $y \neq 1$ has order d modulo p . Then $\text{Det}(Y) = 0$ if and only if $d|n$. If this is the case $\text{rank}(Y) = 1$ and

$$\begin{aligned} \lambda_1 &= K \sum_{m=1}^n y^{n-m+1} \mu_m, \\ \lambda_i &= y^{i-1} \lambda_1. \end{aligned} \tag{IV.7}$$

If $y = 1 \pmod{p}$, then for all i ,

$$\lambda_i = K(\mu_1 + \mu_2 + \cdots + \mu_n). \tag{IV.8}$$

If d does not divide n , then (Y, E_n) will be called the global period n cellular automaton induced by $B_{(b,r)}$.

V. Discussion

The operators $D^-_{(1,p-1)}$ and $D_{(p-1,1)}$ are analogues to derivatives with respect to sequence index through comparison to the first order Taylor approximation to a differentiable function: $f(x+a) \approx f(a) + f'(a)(x-a)$. For $D_{(p-1,1)}$ and $D^-_{(1,p-1)}$

$$\mu_{i+1} = \mu_i + [D_{(p-1,1)}(\mu)]_i = \mu_i + [D^-_{(1,p-1)}(\mu)]_{i+1}. \tag{V.1}$$

The role of $B_{(b,r)}$ indicates that this operator is analogous to integration with respect to the sequence index. This suggests the possibility of integrating more general difference equations for cellular automata. Equations of the form $(D^-_{(r,s)})^k D^k_{(r',s')}(\mu) = \beta$ can be solved by alternating between the formulas of Theorems 2 and 5. For example, the equation $D^-_{(r,s)} D_{(r',s')}(\mu) = \beta$ yields, by Theorem 5, $D_{(r',s')}(\mu) = cB_{(b,t)}(\beta)$, which can be solved by (III.6).

Restricting attention to $p = 2$, Martin et al. [12] prove that for finite automata, states μ for which $\#_1(\mu_n^*) = 1$ have no predecessors. Theorem 1 now indicates how to compute predecessors for states of (D, E_n) and (D^-, E_n) having $\#_1(\mu) = 0$. (D, E_n) is embedded in (D, E^+) and (III.4) is applied for all values of k such that $\#_1(\mu)$ remains zero, except for the final value of k . For (D^-, E_n) the space of left half-infinite sequences E^- is defined and (D^-, E_n) is embedded in (D^-, E^-) . The operator B is suitable redefined and (III.4) is applied. Predecessors for states of (D^-D, E_n) are

obtaining by alternation of the above procedures. That is, $D^-D(\mu) = \beta$ is rewritten as $D^-(D(\mu)) = \beta$ which is embedded in (D^-, E^-) and solved for $D(\mu)$. This is restricted to E_n and then embedded in (D, E^+) and solved for μ . Note that the automaton (D^-D, E_n) does not embed exactly in the automaton (D^-D, E^+) due to the difference in definition of the operator D^- on the spaces E_n and E^+ .

The period multiplying property of B indicates and B defines a one-to-many mapping $E_n \rightarrow E_{pn} \rightarrow \dots \rightarrow E_{p^sn} \rightarrow \dots$ it is an interesting question as to whether or not, in the limits $n, p \rightarrow \infty$, this exhausts all of E^+ . This is equivalent to the question of whether or not every element of E^+ lies in the basin of attraction of some cycle of $D_{(p-1, 1)}$.

References

1. von Neumann, J.: In Taub A. H. (ed.) J. von Neumann, Collected Works **5**, 288 (1963)
2. Flanigan, L. K.: An experimental study of electrical conduction in the mammalian atrioventricular node. Ph.D. Thesis, University of Michigan 1965
3. Manning, F. B.: IEEE Trans. (Computation) **C26**, 536 (1977)
4. Hillis, W. D.: Physica **10D**, 213 (1984)
5. Fischer, P. C.: J. AMC **12**, 388 (1965)
6. Rosenfeld, A.: Picture languages. NY: Academic Press, 1979
7. Sternberg, S. R.: In Gelesma E. S., Kanal L. N. (eds.) Pattern recognition in practice. Amsterdam: North-Holland 1980, p. 35.
8. Wolfram, S.: Rev. Mod. Phys. **55**, 601 (1983)
9. Wolfram, S.: Commun. Math. Phys. **96**, 15 (1984)
10. Wolfram, S.: Physica **10D**, 1 (1984)
11. Wolfram, S.: Physica **22D**, 385 (1986)
12. Martin, O., Odlyzko, A. M., Wolfram, S.: Commun. Math. Phys. **93**, 219 (1984)
13. Voorhees, B., Weiss, A.: preprint (1987)
14. Voorhees, B.: preprint (1987)
15. Shank, D.: Solved and unsolved problems in number theory (2nd ed.) NY: Chelsea 1978

Communicated by J.-P. Eckmann

Received November 30, 1987

