Complex Systems **8** (1994) 151–159

A Note on Injectivity of Additive Cellular Automata

Burton Voorhees
Faculty of Science, Athabasca University,
Box 10,000, Athabasca, Alberta T0G 2R0, Canada

Abstract. Additive cellular automata on finite sequences with periodic boundary conditions are treated in terms of complex polynomials whose arguments are roots of unity. It is shown that the condition for a binary one-dimensional additive cellular automaton to be injective is that the associated complex polynomial have no zeros that are roots of unity.

1. Introduction

Cellular automata are discrete symbolic dynamical systems defined in terms of a lattice of sites, L; an alphabet of symbols, K; and an evolution rule, X, which maps configurations at any given time t to new configurations at time $t+1$. A configuration, or state, is an assignment of a symbol from K to every site of the lattice L. The set of all possible configurations is called the configuration space, denoted by E in the generic case.

Given a configuration $\mu(t)$, the evolution rule generates a new configuration $\mu(t+1)$ by assigning to every site in the lattice a symbol chosen from the alphabet on the basis of the symbols in a neighborhood at that site.

In this note the lattice is taken as a finite set of n sites located on the circumference of a circle. This gives what has been called a cylindrical cellular automaton [1], because the evolution can be visualized as occurring on a cylinder. In this case, the configuration space E_n consists of all periodic sequences of symbols with periods that divide n. In addition, consideration is restricted to binary cellular automata, for which the alphabet is the set $\{0, 1\}$.

The neighborhood of a site consists of a consecutive block of k sites within which the given site occupies a designated position. Here this position is assumed to be located at the left-hand endpoint of the neighborhood; that is, the neighborhoods are left justified.

The evolution rule is defined locally by a rule table specifying the symbols that are assigned to the designated site, for every neighborhood. This also defines a unique global operator $X : E_n \to E_n$. The global operator is represented in terms of local neighborhood maps by defining its ith component as

$$x_i = X(i_0 \ldots i_{k-1}) \tag{1.1}$$

where $i_0 \ldots i_k - 1$, the ith neighborhood, is the binary expression for the index i. The component form of X is written as a "vector" with respect to the "neighborhood basis,"

$$X = (x_0 x_1 \ldots x_{2^k-1}). \tag{1.2}$$

The map X is surjective if for every configuration β there is a configuration μ such that $X(\mu) = \beta$. If, in addition, this predecessor configuration is unique, then the map X is injective. For cellular automata, injectivity is equivalent to reversibility. Hence, if X is injective, there is another cellular automata rule X^{-1} such that if $X(\mu) = \beta$, then $X^{-1}(\beta) = \mu$.

It is known that the question of whether or not a particular cellular automaton is injective is decidable only in dimension one [2, 3]. Recent theoretical studies of reversible cellular automata have been carried out by Head [4], Toffoli and Margolus [5], McIntosh [6], and Hillman [7]. Fredkin [8] has suggested that reversible rules may provide a basis for modeling reversible physical processes.

In this paper considerations are restricted to additive cellular automata rules, that is, those that satisfy the condition

$$X(\mu + \mu') = X(\mu) + X(\mu') \tag{1.3}$$

where all sums are computed modulo 2.

Restriction of the configuration space to E_n rather than a set of infinite or half-infinite binary sequences, is not a serious constraint as far as injectivity is concerned since it is known that a cellular automata rule is injective on these larger spaces if and only if it is injective on all periodic configurations [9].

The additivity condition (1.3) requires that $x_0 = 0$. In addition, equation (1.1) for additive rules takes the form

$$X(i_0 \ldots i_{k-1}) = \sum_{s=0}^{k-1} a_s i_s \tag{1.4}$$

It also possible to give an expression for an additive rule X in terms of the left shift operator σ, defined by $[\sigma(\mu)]_i = \mu_i + \mu_i + 1$:

$$X = \sum_{s=0}^{k-1} a_s \sigma^s \tag{1.5}$$

The coefficients in (1.5) are easily determined in terms of the components of X by solving equation 1.4 with $X(i_0 \ldots i_{k-1}) = x_i$.

In section 2 a representation of additive cellular automata defined on E_n is given in terms of complex polynomials. Section 3 proves that an additive cellular automaton rule $X : E_n \to E_n$ is injective if and only if its associated complex polynomial has no zeros that are nth roots of unity. Finally, in section 4, a restatement is given of a theorem of Martin, Odlyzko, and Wolfram [10] relating injectivity and reachability of configurations.

2. Representations of additive rules

In their classic study of additive cellular automata, Martin, Odlyzko, and Wolfram [10] made use of a dipolynomial representation, that is, states $\mu \in E_n$ were represented as polynomials of the form

$$\mu \to \sum_{s=1}^{n} \mu_s t^{s-1}. \tag{2.1}$$

The action of the cellular automaton rule was represented as multiplication by a dipolynomial of the form

$$t^{-r} \sum_{s=0}^{k-1} c_s t^s \tag{2.2}$$

with all indices and powers reduced modulo n. This corresponds to the shift representation (1.5) when $r = 0$ since left-justified neighborhoods are being used.

Taking a different approach to additive rules, Guan and He [1] represented configurations as n-dimensional vectors and evolution rules as multiplication of these vectors by certain circulant matrices, with all terms reduced modulo 2. They also made use of left-justified neighborhoods, and the circulant representation of a rule given in the form of equation (1.5) is obtained by substitution of the circulant form for the left shift operator:

$$\sigma = \text{circ}(010\ldots0) = \begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & 0 & \ldots & 0 \end{pmatrix} \tag{2.3}$$

A connection between these different approaches can be made in terms of a complex polynomial p associated to each rule. It turns out that what is important are the values $p(w_n)$ where $w_n = \exp(2\pi i/n)$ is an nth root of unity. In what follows the subscript on w_n will generally be supressed, with the understanding that w is defined in terms of whatever value of n is under consideration.

Configurations are now represented as polynomials in the roots of unity:

$$\mu = \sum_{s=1}^{n} \mu_s w^{s-1}. \tag{2.4}$$

A cellular automaton rule X takes the form of multiplication by the complex conjugate of the polynomial

$$p(w) = \sum_{s=0}^{n-1} a_s w^s \tag{2.5}$$

where the coefficients a_s are the entries in the circulant representation of $X : \text{circ}(a_0 a_1 \dots a_{n-1})$, and all sums are taken modulo 2. Reduction modulo n, necessary in the dipolynomial approach, is automatic since $w^n = 1$.

Much is known about circulants and their relation to roots of unity, and a brief summary of results that will be useful in this note concludes this section. These results are taken from the detailed study of circulant matrices by Davis [12].

Lemma 2.1.

1. *An $n \times n$ matrix A is circulant if and only if it commutes with the shift operator.*
2. *An $n \times n$ matrix A is circulant if and only if it has the form $A = p_A(\sigma)$ where σ is the shift.*

Definition 2.2. *The Fourier matrix of order n is the matrix*

$$F = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & w^{n-1} & w^{n-2} & w^{n-3} & \dots & w \\ 1 & w^{n-2} & w^{n-4} & w^{n-6} & \dots & w^2 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^2 & w^4 & w^6 & \dots & w^{n-2} \\ 1 & w & w^2 & w^3 & \dots & w^{n-1}. \end{pmatrix} \tag{2.6}$$

The Hermitian conjugate of this matrix (i.e., the transpose of the complex conjugate) is denoted F^*. This matrix is unitary, that is, $FF^* = F^*F = I$, and its eigenvalues are ± 1 and $\pm i$ with multiplicity depending on the value of n.

Lemma 2.3. *Let $A = \text{circ}(a_0 a_1 \dots a_{n-1})$ have associated polynomial $p_A(w)$ and let $\Lambda(A)$ be the diagonal matrix*

$$\Lambda(A) = \text{diag}(p_A(1), p_A(w), \dots, p_A(w^{n-1})).$$

Then $A = F^* \Lambda(A) F$.

Corollary 2.4. *The eigenvalues of A are $\lambda_i = p_A(w^i)$.*

Remark. Since $[\sigma(\mu)]i = \mu_{i+1}$, the shift is equivalent to multiplication by w^{n-1}, the complex conjugate of w. Hence the action of a rule X, represented by circulant matrix A, on a state $\mu(w)$, is obtained by multiplying $\mu(w)$ by $p_A(w^{n-1})$, the nth eigenvalue of A.

Corollary 2.5. *If A is non-singular, then $A^{-1} = F^* \Lambda^{-1}(A) F$.*

3. Injectivity of additive rules

Since reversibility and injectivity are equivalent, an additive cellular automaton rule $X : E_n \to E_n$ represented by a circulant matrix A will be injective if and only if A^{-1} exists. From Corollary 2.5 we see that this will be the case if and only if none of the diagonal entries of $\Lambda(A)$ are zero. Recalling that these entries are reduced modulo 2, and noting that $p_A(1) = \sum_{s=0}^{n-1} a_s$, this yields the conditions for injectivity of additive cellular automata rules.

Theorem 3.1. *Let $X : E_n \to E_n$ be an additive cellular automaton represented by a circulant matrix $A = \text{circ}(a_0 a_1 \ldots a_{n-1})$. The rule X is injective if and only if no nth root of unity is a root of the complex polynomial p_A modulo 2.*

Remark: Since $w^n = 1$ is an nth root of unity, this condition requires that an odd number of the coefficients a_s be nonzero. We also note that the roots of complex polynomials come in complex conjugate pairs. Hence if w^r is a root, then so is w^{-r}.

The condition in Theorem 3.1 requires that p_A be irreducible with respect to the nth roots of unity. If we are only interested in whether or not p_A has roots that are nth roots of unity for some n, rather than for specified values of n, this can be determined from the contour integral

$$N_0 = \lim_{\epsilon \to 0} \frac{1}{2\pi i} \oint_{C(\epsilon)} \frac{p'_A(z)}{p_A(z)}\, dz \tag{3.1}$$

where $p'_A(z)$ is the derivative of $p_A(z)$, and $C(\epsilon)$ is the annular curve indicated in Figure 1.

It is a well-known result of complex function theory that for any closed contour C this integral counts the number of zeros minus the number of poles of $p_A(z)$ that lie inside of C. Since p_A is a polynomial, it has no poles and only isolated zeros. Hence N_0 given in (3.1) is the number of zeros that lie on the unit circle, and the rule represented by p_A is injective for all n if an only if $N_0 = 0$.

Since an additive cellular automaton is injective on a configuration space of infinite or half-infinite binary sequences if and only if it is injective on all periodic sequences we have as an immediate result.

Corollary 3.2. *An additive cellular automaton $X : E \to E$ represented by a circulant matrix $A = \text{circ}(a_0 a_1 \ldots a_{n-1})$ will be injective if and only if $p_A(z)$ is irreducible with respect to all roots of unity.*

As an example, consider the well-known three-site rule 150 defined by $[X(\mu)]_i = \mu_i + \mu_{i+1} + \mu_{i+2}$. The action of this rule on a configuration $\mu(w)$ is obtained by multiplication of $\mu(w)$ by $p_A(w^{n-1}) = 1 + w^{n-1} + w^{n-2}$. For this rule $p_A(z) = 1 + z + z^2$, which has roots given by $z = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$. These are powers of $w = \exp(2\pi i/3)$. Hence rule 150 is not injective when $3 \mid n$, and is injective on all periodic sequences for which $n \neq 3m$ for any integer m. The next theorem extends this well-known result [11,13].

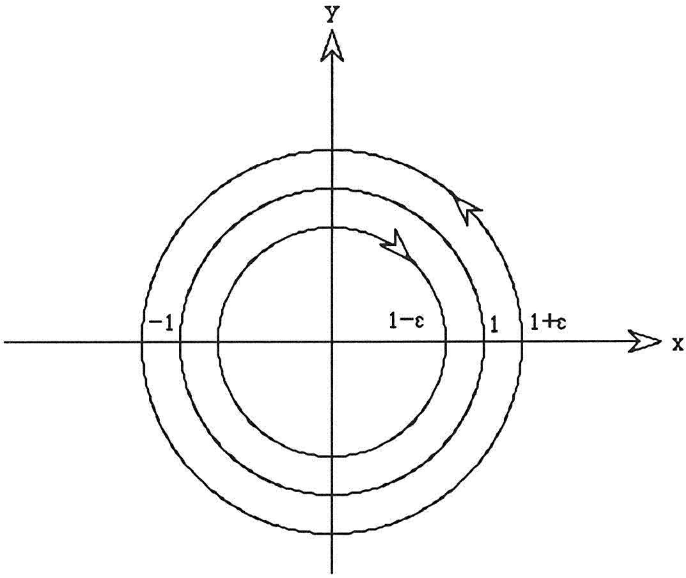

Figure 1: Contour for computation of N_0 in equation (3.1). Integration is counterclockwise around the circle of radius $1+\epsilon$, and clockwise around the circle of radius $1-\epsilon$.

Theorem 3.3. *Let $X : E_n \to E_n$ be k-site additive cellular automaton for which every coefficient a_s in equation (1.5) is equal to 1. If k is even, X is never injective. If k is odd, X is injective for all values of n which are not divisible by k.*

Proof. If all coefficients in equation (1.5) are unity, then $p_A(z) = 1+z+z^2+\cdots+z^{k-1}$. If k is even, then there are an even number of nonzero coefficients a_s, and $p_A(1) = 0 \pmod 2$. Hence X cannot be injective in this case.

If k is odd, $p_A(1) = 1 \pmod 2$, but $w = \exp(2\pi ri/k)$ is a root for $1 \leq r \leq k$. Hence for $n = mk, \exp(2\pi mi/n)$ will be a root. Further, p_A has degree $k-1$, and hence has only $k-1$ roots, so no other values of n can yield roots. Thus, so long as $n \neq mk$, the rule is injective. ∎

Table 1 lists the additive rules for up to five site neighborhoods, and indicates conditions for their reversibility.

In those cases where a rule is injective, its inverse can be computed. The example of rule 150 acting on E_4 and E_5 indicates, however, that this inverse must generally be expected to depend on the period n. For $n = 4$, the inverse of rule 150 is computed to be $I+\sigma^2+\sigma^3$, while for $n = 5$ it is $\sigma(I+\sigma+\sigma^3)$.

a_s coefficients	Shift Form of Rule	Number of Sites	Injectivity Conditions
00000	0	1	never
00001	σ^4	5	always
00010	σ^3	4	always
00011	$\sigma^3 + \sigma^4$	5	never
00100	σ^2	3	always
00101	$\sigma^2 + \sigma^4$	5	never
00111	$\sigma^2 + \sigma^3 + \sigma^4$	5	$n \neq 3m$
01000	σ	2	always
01001	$\sigma + \sigma^4$	5	never
01010	$\sigma + \sigma^3$	4	never
01011	$\sigma + \sigma^3 + \sigma^4$	5	always
01100	$\sigma + \sigma^2$	3	never
01101	$\sigma + \sigma^2 + \sigma^4$	5	always
01110	$\sigma + \sigma^2 + \sigma^3$	4	$n \neq 3m$
01111	$\sigma + \sigma^2 + \sigma^3 + \sigma^4$	5	never
10000	I	1	always
10001	$I + \sigma^4$	5	never
10010	$I + \sigma^3$	4	never
10011	$I + \sigma^3 + \sigma^4$	5	always
10100	$I + \sigma^2$	3	never
10101	$I + \sigma^2 + \sigma^4$	5	$n \neq 3m$
10110	$I + \sigma^2 + \sigma^3$	4	always
10111	$I + \sigma^2 + \sigma^3 + \sigma^4$	5	never
11000	$I + \sigma$	2	never
11001	$I + \sigma + \sigma^4$	5	always
11010	$I + \sigma + \sigma^3$	4	always
11011	$I + \sigma + \sigma^3 + \sigma^4$	5	never
11100	$I + \sigma + \sigma^2$	3	$n \neq 3m$
11101	$I + \sigma + \sigma^2 + \sigma^4$	5	never
11110	$I + \sigma + \sigma^2 + \sigma^3$	4	never
11111	$I + \sigma + \sigma^2 + \sigma^3 + \sigma^4$	5	$n \neq 5m$

Table 1: Injectivity of additive rules for five sites or less.

4. Injectivity and reachability

A question of major interest for studies of cellular automata is whether or not a given configuration μ has a predecessor. Clearly, if a rule $X : E_n \to E_n$ is injective, then all configurations have predecessors. In general, however, this is not the case. In their classic analysis of additive cellular automata, Martin, Odlyzko, and Wolfram[10] prove a lemma specifying the conditions under which a configuration is reachable, that is, has a predecessor. Using the dipolynomial notation of equations (2.1) and (2.2) their result is given in the next lemma:

Lemma 4.1 (10, Lemma 4.4) *A configuration $\mu(t)$ is reachable in the evolution of a size n additive cellular automaton over $\mathbf{Z}_p$, as described by $\mathbf{T}(t)$, if and only if $\mu(t)$ is divisible by the greatest common divisor $\Lambda_1(t) = gcd(x^n - 1, \mathbf{T}(x))$.*

In terms of the nth roots of unity, this can be restated in a form that makes the connection to injectivity explicit. For simplicity, the alphabet is restricted to $\mathbf{Z}_2$.

Lemma 4.2. *Let $X : E_n \to E_n$ be an additive cellular automaton represented by the polynomial p_A. Further, let $p_A(w)$ be decomposed into irreducible factors*

$$p_A(w) = \prod_{i=1}^{r} \pi_i(w) \prod_{j=1}^{S} \Omega_j(w) \tag{4.1}$$

where each $\pi_i(w)$ represents an injective rule and the $\Omega_j(w)$ represent non-injective rules.

A configuration $\mu(w)$ is reachable if and only if

$$\prod_{j=1}^{S} \Omega_j(w) \mid \mu(w). \tag{4.2}$$

Proof: If $\mu(w)$ is reachable, then there is a $\mu'(w)$ such that $p_A(w)\mu'(w) = \mu(w)$ and (4.2) is satisfied as a consequence of equation (4.1).

Conversely, suppose that equation (4.2) is satisfied. Since each π_i represents an injective rule, there exists an inverse π_i^{-1} that is also a polynomial in w. Thus

$$\prod_{j=1}^{S} \Omega_j(w) = p_A(w) \prod_{i=1}^{r} \pi_i^{-1}(w). \tag{4.3}$$

But (4.2) implies that

$$\mu(w) = \prod_{j=1}^{S} \Omega_j(w)\rho(w) \text{ for some } \rho(w).$$

Hence, by (4.3),

$$\mu(w) = p_A(w) \prod_{i=1}^{r} \pi_i^{-1}(w)\rho(w), \tag{4.4}$$

which provides a predecessor for $\mu(w)$. ∎

Acknowledgments

This work was supported by NSERC Operating Grant OPG 0024817.

References

[1] E. Jen, "Cylindrical Cellular Automata," *Communications in Mathematical Physics*, **118** (1988) 569–590.

[2] S. Amoroso and Y. N. Patt, "Decision Procedures for Surjectivity and Injectivity of Parallel Maps for Tessellation Structures," *Journal of Computer and System Science*, **6** (1972) 448–464.

[3] J. Kari, "Reversibility and Surjectivity Problems of Cellular Automata," *Journal of Computer and System Science* (to appear).

[4] T. Head, "One-Dimensional Cellular Automata: Injectivity from Unambiguity," *Complex Systems*, **3** (1989) 343–348.

[5] T. Toffoli and N. Margolus, "Invertible Cellular Automata: A Review," *Physica D*, **45** (1990) 229–253.

[6] H. V. McIntosh, "Reversible Cellular Automata," *Physica D* (to appear).

[7] D. Hillman, "The Structure of Reversible One-Dimensional Cellular Automata," *Physica D*, **52** (1991) 277–292.

[8] E. Fredkin, "Digital Mechanics: An Informational Process Based on Reversible Universal Cellular Automata," *Physica D*, **45** (1990) 254–270.

[9] K. Culik II, L. P. Hurd, and S. Yu, "Computation Theoretic Aspects of Cellular Automata," *Physica D*, **45** (1990) 357–378.

[10] O. Martin, A. M. Odlyzko, and S. Wolfram, "Algebraic Properties of Cellular Automata," *Communications in Mathematical Physics*, **93** (1984) 219–258.

[11] P. Guan and Y. He, "Exact Results for Deterministic Cellular Automata," *Journal of Statistical Physics*, **43** (1986) 463–478.

[12] P. J. Davis, *Circulant Matrices* (New York: John Wiley, 1979).

[13] B. Voorhees, "Predecessors of Cellular Automata States: I. Additive Automata," *Physica D*, **68** (1993) 283–292.