Commun. Math. Phys. 119, 13–28 (1988)

Communications in Mathematical Physics

Linear Cellular Automata and Recurring Sequences in Finite Fields

Erica Jen
Theoretical Division, Los Alamos National Laboratory, Los Alamos, NM 87545, USA

Abstract. A one-dimensional linear cellular automaton with periodic boundary conditions consists of a lattice of sites on a cylinder evolving according to a linear local interaction rule. Limit cycles for such a system are studied as sets of strings on which the rule acts as a shift of size s/h; i.e., each string in the limit cycle cyclically shifts by s sites in h iterations of the rule. For any given rule, the size of the shift varies with the cylinder size n. The analysis of shifts establishes an equivalence between the strings of values appearing in limit cycles for these automata, and linear recurring sequences in finite fields. Specifically, it is shown that a string appears in a limit cycle for a linear automaton rule on a cylinder size n iff its values satisfy a linear recurrence relation defined by the shift value for that n. The rich body of results on recurring sequences and finite fields can then be used to obtain detailed information on periodic behavior for these systems. Topics considered here include the inverse problem of identifying the set of linear automata rules for which a given string appears in a limit cycle, and the structure under operations (such as addition and complementation) of sets of limit cycle strings.

1. Introduction

A central feature of cellular automata with periodic boundary conditions is their generation of limit cycle behavior. In one dimension, an automaton of this type may be viewed as a lattice of sites on a cylinder of specified size n evolving according to a local interaction rule of the form

$$x_i^{t+1} = f(x_{i-r}^t, \ldots, x_i^t, \ldots, x_{i+r}^t), \quad f: F_q^{2r+1} \to F_q \tag{1.1}$$

together with the condition

$$x_i^t = x_j^t, \quad i \equiv j \bmod n,$$

for all i and t. The finiteness and deterministic nature of the system then imply that, for arbitrary initial conditions, the spatial sequences generated eventually become periodic. In the case that the function f in (1.1) is linear, Martin, Odlyzko, and Wolfram [1] have provided an extensive study of transience, limit cycle

periods, and reversibility. The number of distinct attractors for rules that are additive and/or linear in the rightmost or leftmost element has been studied by Guan and He [2, 3]. The enumeration of attractors for general automata rules is also the subject of [4].

This paper builds on the results of [4] to provide information on the detailed structure of limit cycles generated by linear automata of the form (1.1). A major theme of [4] is the identification of shifts as a basic mechanism underlying periodic behavior. Clearly, any automation rule that acts as a shift (in the sense of cyclically permuting the site values in a sequence) automatically produces limit cycles. Even for general automata rules, however, shifts play a central role in generating limit cycles. In fact, it is useful to view any limit cycle for an automaton as a set of sequences on which the rule acts as a shift of size s/h; i.e., each sequence cyclically shifts by s sites in h iterations of the rule. It was shown in [4], for example, that for any rule (linear or nonlinear) of neighborhood size 2, a sequence of length n appears in a limit cycle of the rule iff the values of the sequence satisfy a relation defined using a shift value depending on n.

The analysis of shifts in generating limit cycle behavior contained in [4] indicates an equivalence between the sequences of values appearing in limit cycle for cylindrical cellular automaton, and recurring sequences in finite fields. The latter is an elegant and well-developed mathematical topic of both theoretical and practical importance. (See [5] for a definitive discussion and bibliography of the subject.) Applications of recurring sequences include the design of feedback shift registers, generation of pseudo-random sequences, and the theory of error-correcting codes.

The topic of recurring sequences has been most throughly studied in the case of a governing linear relation acting on elements of the finite field F_q, where $q = p^m$ is any prime power. As will be demonstrated in this paper, the techniques of recurring sequences are thus particularly easily applied to the analysis of cylindrical cellular automata that evolve according to a linear interaction rule with site values restricted to the set F_q. For these automata, the rich body of results for linear recurring sequences may be used to obtain extremely detailed information on periodic behavior. Topics to be considered here include the inverse problem of identifying the set of linear automata rules for which a given sequence appears in an attractor, and the structure under operations (such as addition, and complementation) of sets of limit cycles sequences. Such questions could, in theory, be considered for nonlinear automata rules, since limit cycle sequences for these systems satisfy recurrence relations as well; the nonlinearity of these relations, however, precludes a general treatment at this time.

2. Preliminaries

The analysis of the attractor structure for cylindrical cellular automata contained in [4] indicates that shift transformations are an underlying mechanism in this behavior. In particular, for any two-neighbor rule, the problem of studying limit cycle behavior can be reformulated as the problem of identifying sequences on which the rule acts as a shift. The value of the shift may be non-integer (indicating

that the shift takes place over more than one time step); and in general varies with both cylinder size and initial condition. In this section, certain results from [4] will be summarized in preparation for a discussion of shifts for linear rules of arbitrary neighborhood size.

Definition. For a given rule R defined on a cylinder size n, let $S = \{x_i^t, i = 0, \ldots, n-1; t = 0, \ldots, p-1\}$ represent a limit cycle for the rule. Then R acts on S as a *shift of size* $\sigma = s/h$, with s, h both integers and $h > 0$, if

$$x_i^t = x_{(i+s) \bmod n}^{t+h},$$

for all i and t; i.e., each sequence in the limit cycle undergoes a cyclical permutation by s sites to the right after h iterations. The shift value $\sigma = s/h$ is *fundamental* if h is the smallest positive integer for which the relation holds.

The following theorem [4] deals with the identification of a recurrence relation satisfied by any sequence of values exhibiting shift behavior.

Theorem. *Let R be a one-dimensional rule defined on a cylinder size n, and suppose there exists for R a limit cycle of least period p for which the rule acts as a shift of size $\sigma = s/h$. Then the values of every sequence $\{x_i^t\}$ in the limit cycle satisfy*

$$x_{i-s} = f^h(x_{i-rh}, \ldots, x_i, \ldots, x_{i+rh}),$$

where f^h represents the h^{th} order composition of the rule.

Remark 1. In general, for an arbitrary recurrence relation, the solution is given by an infinite sequence of values $s_0, s_1, \ldots$ with some (not necessarily least) period n. The finite sequence $s_0, \ldots, s_{n-1}$ of length n then represents a limit cycle string for the given rule on a cylinder of size n. In the rest of this paper, the notion of an infinite sequence of period n and a finite sequence of length n on a cylinder of size n will be used interchangeably.

Remark 2. If the recurrence relation as stated in the theorem provides an explicit expression for some x_j in terms of site values with smaller indices, then it is a (generally nonlinear) recurrence relation for the values of any sequence for which the rule acts as a shift s/h. If the expression is implicit, a recurrence relation is obtained by rewriting it, for a fixed value of n, as

$$x_{i-s\pm n} = f^h(x_{i-rh}, \ldots, x_i, \ldots, x_{i+rh}).$$

The recurrence relation can then be used to generate, from arbitrary starting values, sequences of values on which the rule R acts as a shift of size s/h. See [4] for details.

The next theorem [4] uses the fundamental shift value associated with a rule R to define a relation satisfied by the values of a sequence S iff S appears in a limit cycle for R.

Theorem. *Let R be any two-neighbor automaton rule defined by a function f, and let $\sigma_n = s/h$ be the fundamental shift associated with the initial condition consisting of a single non-zero site value for R on a cylinder size n. Then a sequence $S = \{x_i^t\}$ appears in a limit cycle for R on a cylinder size n* iff *its values satisfy the relation*

$$x_{i-s} = f^h(x_{i-h}, \ldots, x_i),$$

in the case of a "left-handed" rule, or

$$x_{i-s} = f^h(x_i, \ldots, x_{i+h}),$$

in the case of a "right-handed" rule.

Remark. The proof of the above theorem requires, among other things, establishing that the spatial period of every solution exactly divides n. As will be shown in the next section, generalization to linear rules of arbitrary neighborhood size requires a modification of the above condition to ensure that the divisibility property remains true.

3. Shift Relations for Linear Automata Rules

In the remainder of this paper, the rule R will be assumed to be linear; i.e., of the form

$$\begin{aligned} x_i^{t+1} &= f(x_{i-r}, \ldots, x_{i+r}), \\ &= \sum_{j=-r}^{j=r} \alpha_j x_{i+j}^t, \end{aligned}$$

where $\alpha_j \in F_q$, q a prime power, and $r \geqq 0$ represents the radius of the rule. It will be shown that analysis of shift relations for these automata rules provides detailed information on their limit cycle behavior.

For linear rules, the shift condition is defined in all cases by

$$x_{i-s} = f^h(x_{i-rh}, \ldots, x_{i+rh}), \tag{3.1}$$

where $\sigma_n = s/h$ is a shift value associated with the initial condition consisting of a single non-zero site value on a cylinder size n, and all indices are taken modulo n if the sequence is taken to be of finite length n. Equation (3.1) can be written as

$$\sum_{j=0}^{j=K} a_j x_{i+j} = 0, \tag{3.2}$$

where addition is defined modulo q, for some K and appropriate coefficients a_j. The above represents a linear recurrence relation, and will be taken to be in standard form (and of degree K) when the indices have been shifted (modulo n) so as to minimize K. The recurrence relation can then be re-expressed as a polynomial $s(x)$ over $F_q[x]$ with

$$a(x) = \sum_{j=0}^{j=K} a_j x^j \mod(x^n - 1), \tag{3.3}$$

where $a(0) \neq 0$ due to the shifting of indices.

The following definitions are provided to avoid confusion in terminology.

Definition. The *degree* (often called *order*) of a recurrence relation $\sum_{j=0}^{j=K} a_j x_{i+j} = 0$ is K. Likewise, the *degree* of the polynomial $a(x) = \sum_{j=0}^{j=K} a_j x^j$ is K. The *order* $\operatorname{ord}(a(x))$

of the above polynomial is the smallest positive integer e such that $a(x)|x^e - 1$.

The following result is basic to the rest of this paper.

Theorem 3.1. *Let R be any linear rule. Consider a cylinder of size n. Define the polynomial $B_n(x) \equiv b_0 + b_1 x^1 + \cdots b_k x^k$ in $F_q[x]$ to be*

$$B_n(x) = \gcd[a_n(x), x^n - 1], \tag{3.4}$$

where $a_n(x) \in F_q[x]$ is the polynomial defined by (3.3) for R on a cylinder size n. Then a sequence $S = \{x_i\}$ appears in a limit cycle for R on a cylinder size n iff *the values of S satisfy the linear recurrence relation*

$$\sum_{j=0}^{j=k} b_j x_{i+j} = 0, \tag{3.5}$$

where all indices are taken modulo n. Furthermore, with $n = mD$, for some integer m with $\gcd[m, p] = 1$ and D the largest power of p that divides n,

$$B_n(x) = (\gcd[a_m(x), x^m - 1])^D,$$

where $a_m(x)$ is the polynomial defined by (3.3) for R on a cylinder size m.

Proof. Let $S = s_0, s_1, \ldots$ be a finite sequence appearing in a limit cycle for a rule R on a cylinder size n. From the linearity of the rule, it follows that the action of R on S is a shift of size s/h, and hence the values of S satisfy the recurrence relation $a_n(x)$ defined by (3.2). Since the length of S must divide n, the values of the infinite sequence corresponding to S satisfy in addition the recurrence relation $x_{i+n} = x_i$. Thus they satisfy the recurrence relation corresponding to $B_n(x) = \gcd[a_n(x), x^n - 1]$.

Sufficiency is implied by the fact that any infinite sequence satisfying the recurrence relations corresponding both to $a_n(x)$ and to $x^n - 1$ must

(i) exhibit a shift of size qs/qh under the rule R for some integer $q \geqq 1$ (and hence appear in a limit cycle for the rule); and
(ii) be of a period that exactly divides n.

Finally, the last result follows from the fact that $a_m^D(x)$ is a shift polynomial on a cylinder size n.

For example, suppose that all limit cycles on a cylinder size 8 are to be found for the rule defined by

$$x_i^{t+1} = x_{i-2}^t + x_{t-1}^t + x_{i+1}^t,$$

where "+" denotes addition modulo 3. The initial steps in the evolution of the impulse response limit cycle for $n = 8$ are given by

$t = 0$	0 0 0 0 0 0 0 1
$t = 1$	1 1 0 0 0 0 1 0
$t = 2$	2 1 2 1 0 1 0 2
$t = 3$	0 0 1 0 1 1 0 0
$t = 4$	0 1 0 2 2 1 2 1

indicating that for $t \geqq 1$, each sequence in the limit cycle undergoes a shift of size

$\frac{4}{2}$. In other words,

$$\begin{aligned} x_{i-4}^t &= x_i^{t+2} \\ &= x_{i-2}^{t+1} + x_{i-1}^{t+1} + x_{i+1}^{t+1} \\ &= x_{i-4}^t + 2x_{i-3}^t + x_{i-2}^t + 2x_{i-1}^t + 2x_i^t + x_{i+2}^t. \end{aligned}$$

Thus, after shifting the indices, Eq. (3.1) has the form

$$2x_i + x_{i+1} + 2x_{i+2} + 2x_{i+3} + x_{i+5} = 0, \tag{3.6}$$

a recurrence relation of degree 5. Since the corresponding polynomial $a(x) = x^5 + 2x^3 + 2x^2 + x^1 + 2$ exactly divides $x^8 - 1$, a sequence appears in a limit cycle on cylinder size $n = 8$ iff its values satisfy (3.6). Therefore, substitution of all possible 5-tuple starting values yields all sequences appearing in limit cycles for this rule on a cylinder size 8.

The next theorem provides an alternative method of computing the shift polynomial $B_n(x)$. The notation used to describe the result follows that of [1]. Associate with any linear rule $f: x_i^{t+1} = \sum_{j=-r}^{j=r} \alpha_j x_{i+j}^t$, the polynomial

$$\Pi(x) = x^d \sum_{j=-r}^{j=r} \alpha_j x^j,$$

where x^d is a multiplicative factor used to transform the expression into an ordinary polynomial. Similarly for any sequence $s_0, s_1, \ldots$ define the polynomial

$$t(x) = \sum_{j=0}^{j=n-1} s_j x^{n-j}.$$

Then the action of the rule f on any sequence $t(x)$ is given by $\Pi(x)t(x)$, where multiplication is defined as for ordinary polynomials modulo $(x^n - 1)$.

Theorem 3.2. *Let R be any linear rule, and let $B_n(x) \in F_q[x]$ be its shift polynomial on a cylinder size n. Then for $n = mD$, with m a positive integer such that* $\gcd[m, p] = 1$, *and D the largest power of p that divides n,*

$$B_n(x) = \frac{x^n - 1}{\gcd[x^n - 1, \Pi^D(x)]} = [B_m(x)]^D. \tag{3.7}$$

Remark. In [1], it was shown that, for any sequence $S = s_0, s_1, \ldots$, S may be generated after D steps in the evolution of R iff the denominator term in (3.7) (call it $\Lambda(x)$) divides the polynomial $S(x) = s_0 x^n + s_1 x^{n-1} + \cdots$. The proof given in [1] can be restated in the present terminology as follows:

If S is generated after D steps, then for some $S^{(0)}(x)$, it must be true that

$$S(x) \equiv \Pi^D(x) S^{(0)}(x) \bmod (x^n - 1),$$

and therefore

$$x^n - 1 \mid S(x) - \Pi^D(x) S^{(0)}(x).$$

Then the definition of $\Lambda(x)$ implies that $\Lambda(x)$ divides both $x^n - 1$ and $\Pi^D(x)$, and hence

$$\Lambda(x) \mid S(x).$$

Thus, in the language of finite fields, limit cycle sequences belong to the ideal generated by the reciprocal polynomial of $\Lambda(x)$. The above theorem represents an alternative derivation of this result.

Proof. The polynomial $\Pi(x)$ represents both the action of the rule R and the spatial sequence generated at time $t = 1$ from an initial condition consisting of a single non-zero site value.

For any m, with $\gcd[m, p] = 1$, it must be true (see preceding remark) that $\Pi(x)$ reoccurs (in some cases, first in cyclically permuted form, and in all cases eventually in unpermuted form) in the evolution of the automaton. Hence, there exist integers σ and ρ such that

$$\Pi^{\sigma}(x)\Pi(x) \equiv x^{\rho}\Pi(x) \bmod (x^m - 1),$$

since the left-hand side represents the spatial sequence generated after $\sigma + 1$ iterations, and the right-hand side represents the sequence $\Pi(x)$ shifted by ρ sites to the left. Thus

$$[\Pi^{\sigma}(x) - x^{\rho}]\Pi(x) \equiv 0 \bmod (x^m - 1),$$

or

$$\Pi^{\sigma}(x) - x^{\rho} = \frac{h(x)(x^m - 1)}{\gcd[x^m - 1, \Pi(x)]}, \tag{3.8}$$

where the left-hand side of (3.8) corresponds to the shift relation $a(x)$ defined by (3.3). Hence

$$\begin{aligned} B_m(x) &= \gcd[a(x), x^m - 1] \\ &= \gcd\left[\frac{h(x)(x^m - 1)}{\gcd[x^m - 1, \Pi(x)]}, x^m - 1\right]. \end{aligned}$$

But $d(x) \equiv \gcd[h(x), \Pi(x)] = 1$ since otherwise $d(x)$ divides the right-hand side of (3.8), but not the left-hand side, and therefore

$$B_m(x) = \frac{x^m - 1}{\gcd[x^m - 1, \Pi(x)]}.$$

For $n = mD$, with D the largest power of p that divides n, the first sequence in the impulse response limit cycle that reoccurs in the evolution of R is that generated at $t = D$, and hence $B_n(x) = B_m^D(x)$.

The following definitions describe properties of polynomials that will be shown to imply certain characteristics for limit cycle sequences associated with those polynomials.

Definitions. (i) A polynomial $p(x) \in F_q[x]$ is *irreducible* if $p(x) = c(x)d(x)$ with $c(x), d(x) \in F_q[x]$ implies that either $c(x)$ or $d(x)$ is a constant polynomial.

(ii) The *characteristic polynomial* of a sequence satisfying a recurrence relation of the form $x_k = a_{k-1}x_{k-1} + \cdots + a_0 x_0$ is the polynomial $x^k - a_{k-1}x^{k-1} - \cdots - a_0$.

(iii) A monic polynomial $m(x) \in F_q(x)$ is the *minimal polynomial* of a sequence $s_0, s_1, \ldots$ if $m(x)$ has the following property: a monic polynomial $g(x) \in F_q[x]$ of positive degree is a characteristic polynomial of $s_0, s_1, \ldots$ iff $m(x)$ divides $g(x)$.

Theorem 3.3. *Let $S = s_0, s_1, \ldots$ be any sequence appearing in an impulse response limit cycle for a linear rule R. Then the polynomial $B_n(x)$ defined by (3.4) is the minimal polynomial for S.*

Proof. Given any sequence $s_0, s_1, \ldots$ of period n satisfying the recurrence relation corresponding to a polynomial $B(x)$, the minimal polynomial is

$$m(x) = \frac{B(x)}{\gcd[B(x), h(x)]},$$

where

$$h(x) = \frac{B(x)s(x)}{x^n - 1},$$

and $s(x) = \sum_{j=0}^{j=n-1} s_j x^{n-j-1}$ [6]. Let $n = mD$, where D is the largest power of p that divides n. If the sequence $s_0, s_1, \ldots$ is taken to be the sequence generated by a rule R at time $t = D$, and if $B_n(x)$ is the shift polynomial for R on a cylinder size n, then (3.7) implies that, letting $d(x) = \gcd[x^n - 1, \Pi^D(x)]$,

$$h(x) = \frac{\Pi^D(x)}{d(x)},$$

and

$$m(x) = \frac{B_n(x)}{\gcd\left[\dfrac{x^n - 1}{d(x)}, \dfrac{\Pi^D(x)}{d(x)}\right]}$$

$$= B_n(x).$$

Thus, $B(x)$ is the minimal polynomial for the sequence generated at $t = D$ and hence for all other sequences in the impulse response limit cycle.

4. Arithmetic of Limiting Cycle Sequences

The theory of linear recurring sequences in finite fields provides the basic tools for the study of families of limit cycle sequences for linear automata rules.

Definition. For any recurrence relation of the form

$$x_{i+k} = \sum_{j=0}^{j=k-1} b_j x_{i+j},$$

corresponding to a monic polynomial

$$B_n(x) = \sum_{j=0}^{j=k} b_j x^j,$$

denote by $S[B_n(x)]$ the family of sequences $s_0, s_1, \ldots$ that satisfy the relation.

It is well-known [5] that $S[B_n(x)]$ represents a vector space over F_q with operations for sequences in the space being defined termwise. Thus, for example, the sum of two sequences $s_0, s_1, \ldots$ and $t_0, t_1, \ldots$ is defined to be the sequences

$s_0 + t_0, s_1 + t_1, \ldots$. The next three theorems are given in [6], and are stated here without proof.

Theorem (a). *Let $f(x)$ and $g(x)$ be two nonconstant monic polynomials over F_q. Then* $S[f(x)] \subseteq S[g(x)]$ iff $f(x) | g(x)$.

Theorem (b). *Let $f_1(x), \ldots, f_h(x)$ be nonconstant monic polynomials over F_q. Then*

$$S[f_1(x)] \cap \cdots \cap S[f_h(x)] = S\left[\gcd_i f_i(x)\right],$$

and

$$S[f_1(x)] + \cdots + S[f_h(x)] = S\left[\operatorname{lcm}_i f_i(x)\right].$$

Theorem (c). *For each $i = 1, 2, \ldots, h$ let S_i be a sequence satisfying a linear recurring relation in F_q with minimal polynomial $m_i(x)$. If the polynomials $m_i(x)$ are pairwise relatively prime, then the minimal polynomial of the sum $S_1 + \cdots + S_h$ is given by the product $m_1(x) \ldots m_h(x)$.*

The following results use the above theorems to describe the behavior produced by the composition of sequences appearing in limit cycles for (possibly different) linear automata rules.

Theorem 4.1. *Let S_i be a set of sequences of lengths n_i that appear in limit cycles for rules R_i:$\Pi_i(x)$. Set $n = \operatorname{lcm}_i n_i$ and D to be the largest power of p that divides n;* i.e., $n = mD$, *where* $\gcd(m, p) = 1$. *Then*

$$S^* = \sum_i S_i$$

appears in a limit cycle for any rule R: $\Pi(x)$ such that

$$\gcd[x^m - 1, \Pi(x)] \mid \gcd\left[x^m - 1, \gcd_i \Pi_i(x)\right]. \tag{4.1}$$

Proof. To prove the result, note that Theorem 3.2 implies that the shift polynomial for a rule $\Pi(x)$ on a cylinder size n is given by

$$B_n(x) = \frac{x^n - 1}{\gcd[x^n - 1, \Pi^D(x)]}.$$

Since $\Pi(x)$ satisfies condition (4.1), it follows that

$$B_n(x) = h(x) \frac{x^n - 1}{\gcd\left[x^n - 1, \gcd_i \Pi_i^D(x)\right]}.$$

for some $h(x)$. Further note that the period of each sequence S_i divides n, and S_i satisfies the recurrence relation corresponding to

$$\frac{x^n - 1}{\gcd[x^n - 1, \Pi_i^D(x)]}.$$

Theorem (b) above then implies that S^* satisfies the relation

$$B^*(x) = \operatorname*{lcm}_i \frac{x^n - 1}{\gcd[x^n - 1, \Pi_i^D(x)]},$$

$$= \frac{x^n - 1}{\gcd\left[x^n - 1, \gcd_i \Pi_i^D(x)\right]}.$$

Since $B^*(x) | B_n(x)$, it follows from Theorem (a) above that S^* must appear in a limit cycle for $\Pi(x)$.

In the special case that $p = q = 2$, the effect of "toggling" on the values of a limit cycle sequence is described in the following result.

Definition. Let S be a sequence $s_0, s_1, \ldots$. Then its *binary complement* $\bar{S}$ is defined to be the sequence $\bar{s}_0, \bar{s}_1, \ldots$, with $\bar{s}_i = 1 - s_i$.

Theorem 4.2. *Let S be a finite sequence of length n, and let $n = mD$, where m is odd. Suppose S appears in a limit cycle for a rule $R = f(x)$. Then $\bar{S}$, its binary complement, appears in a limit cycle for R* iff $(x+1)^D \nmid f(x)$.

Proof. Let ε be the sequence in F_2 all of whose terms are 1. First suppose that $(x+1)^D | f(x)$. Theorem 3.2 implies that $x + 1 \nmid m(x)$, where $m(x)$ is the minimal polynomial for any sequence that appears in a limit cycle for R. Since $\bar{S} = S + \varepsilon$, and the minimal polynomial of ε is $x + 1$, the Theorem (c) above implies that the minimal polynomial of $\bar{S}$ is given by $m(x)(x+1)$, and hence $\bar{S}$ cannot appear in a limit cycle for R.

Conversely, if $(x+1)^D \nmid f(x)$, then $(x+1) | m(x)$ and therefore the minimal polynomial of S divides $m(x)$. Hence $\bar{S}$ appears in a limit cycle for R.

5. Enumeration of Limit Cycle Sequences

This section considers the enumeration of limit cycle sequences for linear automata rules. Given the equivalence between limit cycle sequences and recurring sequences, the problem of enumeration is easily solved using standard results from finite fields. This section presents these results in the context of cellular automata behavior. For a thorough discussion of the results themselves, as well as their proofs, see [5, 6].

The basic theorem on the length of limit cycle sequences for linear automata rules is given below.

Definition. A sequence $s_0, s_1, \ldots$ is *primitive* of length n if its spatial period is exactly equal to n; i.e., there is no $m < n$ such that, for all i,

$$s_{i+m} = s_i.$$

Theorem 5.1. *Let R be a linear rule, and let $B_n(x)$ be its shift polynomial of degree k on a cylinder size n. Let α be a root in F_{q^k} of $B_n(x)$, and let r be the order of α;* i.e., *r is the smallest positive integer such that $\alpha^r = 1$. Then associated with α is a sequence of length r that appears in a limit cycle for R on a cylinder size n, and $r | \operatorname{ord}[B_n(x)]$, and thus $r | n$.*

Proof. For any root α of $B_n(x)$, consider the powers of α computed using multiplication with residue reduction modulo $B_n(x)$. For $j = 0, 1, \ldots, r-1$, and $\alpha^j = \sum_i \beta_{i,j}\alpha^i$, construct the k-tuple $(\beta_{k-1,j}, \beta_{k-2,j}, \ldots, \beta_{0,j})$. Then any vector $\vec{\beta} = (\beta_{i,j}, j = 0, 1, \ldots, r-1)$ consists of components that satisfy the linear recurrence relation, and thus represents a limit cycle sequence.

For example, consider the rule defined on F_2 by

$$x_i^{t+1} = x_{i-1}^t + x_{i+2}^t$$

on a cylinder size 9. Then the shift polynomial is found to be $B_9 = x^6 + x^3 + 1$, of degree 6. For α a root of B_9, the powers of α and the corresponding 6-tuples are given by

power	polynomial	tuple
0	1	000001
1	x	000010
2	x^2	000100
3	x^3	001000
4	x^4	010000
5	x^5	100000
6	$x^3 + 1$	001001
7	$x^4 + x$	010010
8	$x^5 + x^2$	100100
9	1	000001

The next theorem enumerates the number of sequences appearing in limit cycles for rules with shift relations represented by powers of irreducible polynomials.

Theorem 5.2. *Let R be a linear rule. For any m with $\gcd[m, p] = 1$, let $B_m(x)$ be the shift polynomial of R on a cylinder size m. Suppose $B_m(x)$ is irreducible of degree k and order e. Then for $n = mD$, where $D = p^t$ is a power of p, the number of distinct sequences appearing in limit cycles for R and their spatial lengths are given by*

$$\begin{array}{rll} 1 & \text{primitive sequences of length} & 1 \\ q^k - 1 & \text{primitive sequences of length} & e \\ q^{kp^j} - q^{kp^{j-1}} & \text{primitive sequences of length} & ep^j \\ q^{kD} - q^{kp^{t-1}} & \text{primitive sequences of length} & eD. \end{array} \quad ; \quad j = 1, 2, \ldots, t-1$$

Remark. The enumeration (as distinct from the length) of limit cycle sequences can also be derived from results obtained by Guan and He [2]. (See, in particular, Eq. (3.15) of [2].) Their focus is dual to that of the above theorem in that they consider the enumeration of limit cycle periods for linear automata rules. Their technique involves reducing a matrix representing the linear automaton rule to Jordan canonical form. In the language of shift analysis, this is equivalent to finding a power of the rule's transformation matrix equal to the identity matrix with cyclically non-zero entries, and whose action on any sequence is therefore to generate a shift.

Proof. The first theorem in this section states that the period of every sequence

that satisfies $B_m(x)$ must divide $e = \mathrm{ord}(B_m(x))$. Since $B_m(x)$ is irreducible, every nonunit period must be equal to e, and there are exactly $q^k - 1$ such solutions. For $n = mD$, Theorem 3.2 and Theorem (a) cited from [6] imply that

$$S[B_m(x)] \subseteq S[B_m^2(x)] \subseteq \cdots \subseteq S[B_n(x)],$$

and the result follows from simple counting arguments.

Using the above result and that of the previous section on the products of shift polynomials, it is thus possible to apply in straightforward fashion the results of [5, 6] to enumerate limit cycle sequences for arbitrary linear automata rules.

The final theorem in this section discusses the number of distinct equivalence classes of limit cycle sequences, with "equivalence" defined using concepts of shift-invariance and "reduced" periodicity.

Definition. Two sequences $S = s_0, s_1, \ldots$ and $S' = s'_0, s'_1, \ldots$ are *cyclically equivalent* if there exists an integer j such that

$$s'_i = s_{i+j}$$

for all i. S and S' are *projectively cyclically* equivalent if there exist integers j and λ such that

$$s'_{i+j} = \lambda s_i \tag{5.1}$$

for all i.

Theorem 5.3. *Let R be a linear rule and suppose that its shift polynomial $B_n(x)$ is irreducible. Then the number N of distinct, cyclically inequivalent nonzero sequences that appear in limit cycles for R on a cylinder size n is given by*

$$N = \frac{q^k - 1}{n}, \tag{5.2a}$$

and the number N_1 of distinct, projectively cyclically inequivalent nonzero sequences that appear in limit cycles is given by

$$N_1 = \frac{q^k - 1}{\mathrm{lcm}(n, q-1)}, \tag{5.2b}$$

where $n = \mathrm{ord}(B_n(x))$, and k is the degree of $B_n(x)$. Moreover, the values of every nonzero limit cycle sequence satisfy (5.1) (setting $s'_i = s_i$), with

$$j = \frac{n}{\gcd[n, q-1]},$$

and λ an element of F_q of order $e = \gcd[n, q-1]$.

Proof. Equation (5.2a) follows immediately from the irreducibility of the shift polynomial and Corollary 5.2.1. The proof for (5.2b) is given in [8].

Corollary 5.3. *If $B_n(x)$ is irreducible and the cylinder size n is of the form $q^k - 1$ for some k, then R has only two cyclically inequivalent limit cycle sequences: the zero fixed point, and a primitive sequence of length n.*

For example, consider the rule defined over F_5 on a cylinder size 6 by

$$x_i^{t+1} = 4x_{i-2}^t + 4x_{i-1}^t + x_{i+1}^t + x_{i+2}^t.$$

From Theorem 3.1, the recurrence relation for $n = 6$ is given by

$$x_{i+2} = x_{i+1} - x_i \pmod 5.$$

Every sequence that appears in a limit cycle for the rule on a cylinder size 6 is therefore obtained by substituting one of the 5^2 possible starting values into the above relation. The polynomial corresponding to the relation is irreducible over $F_5[x]$, and hence every solution has length 6. From Theorem 5.3, it follows that there are $N = 5^2 - 1/6 = 4$ cyclically inequivalent solutions. These solutions are given by

$$\begin{array}{c} 0\,1\,1\,0\,4\,4 \\ 1\,2\,1\,4\,3\,4 \\ 0\,2\,2\,0\,3\,3 \\ 2\,4\,2\,3\,1\,3 \end{array} \tag{5.3}$$

Theorem 5.3 further states that there are in fact only $N_1 = 2$ projectively cyclically inequivalent solutions given by

$$\begin{array}{c} 0\,1\,1\,0\,4\,4 \\ 1\,2\,1\,4\,3\,4 \end{array} \tag{5.4}$$

since the last two sequences of (5.3) are equal to the first two multiplied by 2. The final part of Theorem 5.3 states that each sequence in (5.4) satisfies relation (5.1); e.g., for both sequences, the relation $s_{i+3} = -s_i$ holds.

6. Characterization of Limit Cycle Sequences for Linear Automata Rules

In Sect. 3, it was shown that the values of any sequence that appears in a limit cycle for a linear automaton rule must satisfy a linear recurrence relation. This section will use that constraint to solve the inverse problem of identifying the set of all linear automata rules for which a given sequence S appears in a limit cycle.

The first result in this section provides the degree of the minimal polynomial for any limit cycle sequence.

Definition. Let $s_0, s_1, \ldots$ be any arbitrary sequence of values. For integers $n \geqq 0$ and $j \geqq 1$, the *Hankel determinant* $D_n^{(j)}$ is defined as

$$\begin{vmatrix} s_n & s_{n+1} & \cdots & s_{n+j-1} \\ s_{n+1} & s_{n+2} & \cdots & s_{n+j} \\ \vdots & \vdots & & \vdots \\ s_{n+j-1} & s_{n+j} & \cdots & s_{n+2j-2} \end{vmatrix}.$$

Theorem 6.1. *Let $S = s_0, s_1, \ldots$ be a limit cycle sequence for some linear automaton rule. Then there exists a positive integer k such that $D_n^{(j)} = 0$ for all $j > k$ and all $n \geqq 0$. If k is the smallest positive integer for which this is true, then k is the degree of the minimal polynomial for S.*

Proof. The above is a rephrasing of a standard result in linear recurring sequences [5]. If S is a limit cycle sequence with minimal polynomial of degree k, then it follows that the $(k+1)$-st row of $D_n^{(k+1)}$ is a linear combination of the first k rows,

and therefore $D_n^{(k+1)} = 0$. Moreover, k is the smallest positive integer for which this is true.

For example, given the sequence $1,1,1,1,0,0,0$, it is easy to show that $D_0^{(j)} \neq 0$ for $j \leqq 4$, and $D_0^{(j)} = 0$ for $j > 4$. Hence, the minimal polynomial has degree 4, and in fact can be shown to be given by $x^4 + x^2 + 1$.

The next problem is the actual computation of the minimal polynomial corresponding to a sequence S. The Berlekamp–Massey algorithm [5,9] is a recursive procedure that can be used to solve this problem, assuming that the degree of the minimal polynomial is known. The inverse problem of finding all linear rules for which a sequence appears in a limit cycle is then solved using the theorem that follows.

Theorem 6.2. *Let $S = s_0, s_1, \ldots$ be any sequence of length n with elements in F_q, and let $m(x)$ be its minimal polynomial in $F_q[x]$ (obtained, for example, from the Berlekamp–Massey algorithm). Then S appears in a limit cycle for a linear rule $R: \Pi(x) \in F_q[x]$* iff

$$\gcd[x^n - 1, \Pi^D(x)] \Big| \frac{x^n - 1}{m(x)},$$

where $n = mD$, and D is the largest power of p that divides n.

Proof. Suppose

$$\gcd[x^n - 1, \Pi^D(x)] = m^*(x) \Big| \frac{x^n - 1}{m(x)},$$

for some polynomial $m^*(x) \in F_q[x]$. Then Theorem 3.2 implies that the shift polynomial for R on a cylinder size n is given by

$$B_n(x) = \frac{x^n - 1}{\gcd[x^n - 1, \Pi^D(x)]} = m(x)h(x),$$

where $h(x)$ is some polynomial over $F_q[x]$. Since $m(x)$ is the minimal polynomial of the sequence S, it follows that S must appear in a limit cycle for R. The converse is proved in similar fashion.

For example, consider the sequence $1,1,0,0,1,0,1$ in F_2. The Berlekamp–Massey algorithm yields $m(x) = x^3 + x + 1$ as the sequence's minimal polynomial in $F_2[x]$. The above theorem then states that the sequence appears in a limit cycle for any rule $\Pi(x)$ such that

$$\gcd[x^7 - 1, \Pi(x)] \in \{(x^4 + x^2 + x + 1), (x^3 + x^2 + 1), (x + 1), 1\}.$$

An example of such a rule is that defined by

$$x_i^{t+1} = x_{i-2}^t + x_{i-1}^t + x_i^t + x_{i+2}^t.$$

7. Summary

A rule acts upon a sequence as a shift of size $\sigma = s/h$ if, under the evolution of the automaton, the sequence shifts s sites in h iterations. It has been shown that shifts

underlie periodic behavior for all linear rules in the sense that a sequence of length n appears in a limit cycle for such a rule iff its values satisfy a linear recurrence relation defined using the shift value for a cylinder size n.

The shift-based recurrence relation not only represents a necessary and sufficient condition for sequences appearing in limit cycles for linear automata rules, but also provides information on the detailed structure of limit cycle behavior. The relation has been shown in this paper to be minimal in that any other relation characterizing a limit cycle sequence must be a multiple of this relation. Its degree and order are parameters that determine the number of limit cycles for these systems. Its reducibility (i.e., the extent to which it can be factored into terms of lower degree) determines the extent to which limit cycle sequences can be expressed as compositions of shorter sequences. Although not discussed in this paper, a number of other characteristics of limit cycle sequences, such as their distribution of site values and autocorrelation properties, can be derived in straightforward fashion [5] from the governing recurrence relation.

Based on the equivalence between limit cycle sequences and linear recurring sequences, a standard technique valid for any field can be used to determine the degree of the minimal polynomial for a sequence that appears in a limit cycle for any linear automaton rule. Moreover, the Berlekamp–Massey algorithm, a procedure for actually computing the minimal polynomial of any such sequence, then leads to the solution of the inverse problem of identifying the set of all linear automata rules for which the sequence appears in a limit cycle.

Finally, the derivation of linear recurring relations implies that limit cycle sequences for linear automata can be generated using these relations, and that this generation process can be implemented on feedback shift registers. The degree k of the recurrence relation determines the number of starting values needed to specify any limit cycle sequence, and, in general, k is smaller than the cylinder size n.

Examples indicate that nonlinear rules of arbitrary neighborhood size exhibit highly complicated shift structures. Sequences appearing in limit cycles for such systems satisfy shift relations [4], but the paucity of results for nonlinear recurrence relations makes it difficult to extend the results in this paper except on a case-by-case basis.

Acknowledgements. This work was supported in part by the NSF under Grant No. DMS-8601520 and by the DOE Office of Scientific Computing under Contract No. KC-07-01-01.

References

1. Martin, O., Odlyzko, A., Wolfram, S.: Algebraic properties of cellular automata. Commun. Math. Phys. **93**, 219–259 (1984)
2. Guan, P., He, Y.: Exact results for deterministic cellular automata. J. Stat. Phys. **43**, 463 (1986)
3. Guan, P., He, Y.: Upper bound on the number of cycles in border-decisive cellular automata. Complex Systems **1**, 181 (1987)
4. Jen, E.: Cylindrical cellular automata. Commun. Math. Phys. **118**, 569–590 (1988)
5. Lidl, R., Niederreiter, H.: Finite fields. Reading, MA: Addison–Wesley 1983
6. Zierler, N.: Linear recurring sequences. J. SIAM **7**, 31 (1959)

7. Zierler, N., Mills, W. H.: Products of linear recurring sequences. J. Algebra **27**, 147 (1973)
8. McEliece, R.: Finite fields for computer scientist and engineers. Boston, MA: Kluwer Academic 1987
9. Berlekamp, E.: Algebraic coding theory. New York: McGraw-Hill 1968

Communicated by J. L. Lebowitz

Received August 7, 1987; in revised form March 15, 1988