Dynamics of finite linear cellular automata over $\mathbb{Z}_N$

F. Mendivil[*], D. Patterson[†]

September 9, 2009

Abstract

We investigate the behaviour of linear cellular automata with state space $\mathbb{Z}_N$ and only finitely many states. After some general comments about linear cellular automata over $\mathbb{Z}_N$, the general case is reduced to that of N being the power of a prime. For a prime power modulus, it is proved under fairly general conditions that the period length for "most" orbits increase by a factor of p when the modulus increases from p^k to p^{k+1}. Some specific comments about the maximal period length modulo N are also given for shift invariant linear cellular automata.

1 Introduction

An *automaton* is a simple theoretical machine which reacts in a deterministic way to its input. A *cellular automaton* (CA) is a collection of automata, where the input given to each automaton in the collection is a function of the state of the entire collection. With this view, a CA is mainly a model of individual "cells" interacting with their environment. Usually each automaton in a CA can have one of finitely many states selected from some fixed set $\mathcal{A}$ and the collection of all automata has some graph structure so that each automaton has some neighbors. The current *configuration* of the CA is

[*]Department of Mathematics and Statistics, Acadia University, Canada
[†]Department of Mathematics and Statistics, Dalhousie University, Canada

specified by giving the state of each automaton in the CA and this configuration is updated from each discrete time step to the next by simultaneously updating all the *sites* (or individual automaton) by an *update rule*. Most often this update rule has some type of local rule which generates the global behaviour. Usually the collection of sites is a grid and the update rule is defined at each site according to some function of its state and the states of its neighbors. Much of the interest in CAs lies in the fact that even with simple local update rules, the global behaviour can be very complicated. For a huge variety of examples of this, see the recent book [13].

To establish some notation, we let Λ index the collection of automata so that the configuration space is given by $\mathcal{A}^\Lambda = \{f : \Lambda \to \mathcal{A}\}$. The update rule is then a function $\Phi : \mathcal{A}^\Lambda \to \mathcal{A}^\Lambda$.

Recall that a graph G is *homogeneous* if any graph isomorphism between two finite induced subgraphs extends to an automorphism of G. An example of such a graph is the 2D infinite lattice $\mathbb{Z}^2$ or a finite lattice with periodic boundary conditions. If Λ is homogeneous as a graph, then the *neighborhood*, $\mathcal{N}(x)$, of each $x \in \Lambda$ has a structure which is independent of x. For such a CA, a *local rule* can take the form of a function $\phi : \mathcal{A}^\mathcal{N} \to \mathcal{A}$ and we use this to define the update rule by $\Phi(f)(x) = \phi(f|_{\mathcal{N}(x)})$. These CA can have especially nice structural properties.

Our attention in this paper is on *Linear Cellular Automata*. That is, a CA where the update rule is linear. In this case, the state space $\mathcal{A}$ is a commutative ring (with identity) and the configuration space $\mathcal{A}^\Lambda$ is a module over $\mathcal{A}$. The update rule is required to be an $\mathcal{A}$-module homomorphism, i.e.,

$$\Phi(af) = a\Phi(f) \quad \text{and} \quad \Phi(f+g) = \Phi(f) + \Phi(g).$$

Since $\mathcal{A}^\Lambda$ is a free $\mathcal{A}$-module, it is generated by the elements $\{\delta_x : x \in \Lambda\}$, where for $y \in \Lambda$ we have $\delta_x(y) = 1$ if $y = x$ and $\delta_x(y) = 0$ if $x \neq y$. In this situation Φ can be represented by a square matrix indexed by $\Lambda \times \Lambda$ and with entries in $\mathcal{A}$. For a very nice discussion of matrices with entries in a commutative ring, see [5]. We focus on the case where $\mathcal{A} = \mathbb{Z}_N$, the integers modulo N and where Λ a finite set.

There are a number of previous studies of linear CA with finite state space, including the early paper [10]. Some more recent work in a similar vein as the current paper are the papers [6, 11, 12] relating the Ducci n-game to linear CA. Another series of papers is [2, 3, 4] which studies the particular *Ducci map* in great detail. In particular, [2] has some general

results for (m, n)-*Binomial groups*. The paper [3] builds on [2, 4] and has precise results on period lengths based on the theory of cyclotomic fields. Notice that our Proposition 2 serves a similar role as the use of the primary decomposition in [3] and in particular equation (5) in section 4.

The structure of the rest of this paper is as follows. In Section 2, we discuss some general features of finite linear CA over $\mathbb{Z}_N$, in particular discussing the differences between cases of prime and composite modulus. Using tools from linear algebra and the Chinese Remainder Theorem, the general case is reduced to the case of when the modulus is a power of a prime. Section 3 investigates how the dynamics of the CA change when the modulus is changed from p^k to p^{k+1}, where p is a fixed prime. Finally, in Section 4 we discuss the nice special case of when the graph is homogeneous and the dynamics are shift invariant (i.e., has the same behaviour at all sites).

2 Generalities

Throughout the rest of the paper we will let A be a fixed $L \times L$ integer matrix; the matrix A is the update matrix for our Linear Cellular Automata. We will also denote the modulus by N. Thus the configuration space for the CA is $\mathbb{Z}_N^L$. For a given initial point $x \in \mathbb{Z}_N^L$, the interest is in the behaviour of the iteration sequence $x, Ax, A^2x, A^3x, \ldots$; this behaviour is completely governed by the behaviour of the powers of A.

Prime moduli

If $N = p$, a prime, then $\mathbb{Z}_p^L$ is a vector space and the behaviour of A^i can be predicted using spectral methods [10, 12]. Briefly, for each $x \in \mathbb{Z}_p^L$, the *minimal polynomial* $m_x(\lambda) \in \mathbb{Z}_p[x]$ of x is the monic polynomial of least degree for which $m_x(A)x = 0$. The polynomial $m_x(\lambda)$ is a factor of the minimal polynomial $m(\lambda)$ for the matrix A, as $m(A) = 0$ and thus $m(A)x = 0$ for any x. The *order* of $m_x(\lambda)$ is the smallest $T \in \mathbb{N}$ with $m_x(\lambda)|\lambda^k(\lambda^T - 1)$. In this case, $A^T(A^k x) = A^k x$, and thus the *period length* for $A^k x$ is T. If $m_x(0) \neq 0$, then we can take $k = 0$ and then x is in a periodic orbit of length T. For $m_x(0) = 0$, the smallest such k is the *transient length* for x as it takes k steps for x to fall into a periodic orbit. Whether x has a transient region or not we still will refer to the period length of x.

To find the set of all possible orbit lengths in this case of a prime modulus, it is only necessary to compute the minimal polynomial $m(\lambda)$ for A. Let the

prime factorization of $m(\lambda)$ in $\mathbb{Z}_p[x]$ be $m(\lambda) = f_i(\lambda)^{n_1} f_2(\lambda)^{n_1} \cdots f_m(\lambda)^{n_\ell}$. Each prime factor $f_i(\lambda)$ of $m(\lambda)$ corresponds to an invariant subspace V_i (via the Primary Decomposition Theorem) and all starting vectors in V_i will fall into a periodic orbit with length a divisor of the order of $f_i(\lambda)^{n_i}$. In particular, there is a maximal orbit length and all other orbit lengths are divisors of this maximal one (see Proposition 3).

It is possible for a linear CA over $\mathbb{Z}_p$ to have only two orbits: the orbit of 0 (which is always a fixed point) and one other orbit of length $p^L - 1$ that is the orbit of any nonzero element of $\mathbb{Z}_p^L$. One way to construct such a CA is as follows.

Recall that $GF(p^L)$, the unique finite field of order p^L, is a vector space over $\mathbb{Z}_p$ and that the collection of nonzero elements in $GF(p^L)$ is a cyclic group of order $p^L - 1$. If α is a generator for this multiplicative group, then $x \mapsto \alpha x$ is a linear function on $\mathbb{Z}_p^L \cong GF(p^L)$. The linear CA given by this linear function has only two orbits, one consisting of all nonzero elements in $GF(p^L)$ and thus of length $p^L - 1$ ([9] is a very nice introduction to finite fields).

Composite moduli and the Chinese Remainder Theorem

The Chinese Remainder Theorem is the key tool to use in the case of a composite modulus. If $N = pq$, with $gcd(p, q) = 1$, then $\mathbb{Z}_N^L \cong \mathbb{Z}_p^L \times \mathbb{Z}_q^L$ and this isomorphism extends to the action of A on $\mathbb{Z}_N^L$, $\mathbb{Z}_p^L$ and $\mathbb{Z}_q^L$. This observation is key to building up the dynamics of the CA modulo N from the separate dynamics modulo p and q. More specifically, let $x \in \mathbb{Z}_N^L$ and let $y \in \mathbb{Z}_p^L$ and $z \in \mathbb{Z}_q^L$ be the reductions of x modulo p and q respectively. Then we see that the modulus N orbit of x reduces to the orbits of y and z modulo p and q respectively, as illustrated in the equations below:

$$\begin{array}{cccccccccc}
x & Ax & A^2x & A^3x & \cdots & A^{T_p}x & \cdots & A^{T_q}x & \cdots & A^Tx = x & \mod N \\
y & Ay & A^2y & A^3y & \cdots & A^{T_p}y = y & \cdots & A^{T_q}y & \cdots & A^Ty = y & \mod p \\
z & Az & A^2z & A^3z & \cdots & A^{T_p}z & \cdots & A^{T_q}z = z & \cdots & A^Tz = z & \mod q.
\end{array}$$

In particular, this means that T is a multiple of both T_p and T_q. Because of the isomorphism given by the Chinese Remainder Theorem, in fact we have $T = \text{lcm}(T_p, T_q)$. However, it is worth noting that even if $gcd(p, q) \neq 1$ we still have $T_p | T$ and $T_q | T$ so $\text{lcm}(T_p, T_q) | T$, but we might not have equality. Since this fact will be useful, we record it as an observation.

Observation 1. *If $M|N$ then the period length of x modulo M divides the period length of x modulo N.*

Square-free moduli

For N a square-free integer, we can apply the Chinese Remainder Theorem and the linear algebra tools to compute orbit lengths and transient lengths for starting vectors $x \in \mathbb{Z}_N^L$. That is, for $N = p_1 p_2 \cdots p_\ell$ with p_i distinct primes, we can reduce the action of A on $\mathbb{Z}_N^L$ modulo p_i to obtain the action of A on $\mathbb{Z}_{p_i}^L$ and this action can be analyzed using spectral methods. If T_i and k_i are the orbit lengths and transient lengths for x modulo p_i, then $T = \text{lcm}(T_1, T_2, \ldots, T_\ell)$ and $k = \max\{k_1, k_2, \ldots, k_\ell\}$ are the orbit length and transient length of x modulo N.

General facts for any modulus

Some facts about general moduli are useful. Since $\mathbb{Z}_N^L$ is a finite set, eventually any trajectory will fall into a periodic orbit. Thus, there are minimal $k, T \in \mathbb{N}$ so that for any x, $A^T A^k x = A^k x$. This means that as a matrix $A^k(A^T - I) = 0$ modulo N and so the period length for any x will be a divisor of T.

There will be no transient regions for any x if and only if $ker(A) = \{0\}$. In any case, the submodule $\mathcal{K}$ defined by

$$\mathcal{K} = \bigcap_{n=1}^{\infty} A^n \mathbb{Z}_N^L$$

is invariant under A, $\mathcal{K} = \{x : A^n x = x \text{ for some } n \in \mathbb{N}\}$, and A restricted to $\mathcal{K}$ is invertible. Notice that the intersection in the definition of $\mathcal{K}$ is really a finite intersection as $A^n \mathbb{Z}_N^L$ will stabilize at some point. We will call $\mathcal{K}$ the *core* of the linear CA. All points eventually end up in $\mathcal{K}$. Furthermore, $A^T = I$ when restricted to $\mathcal{K}$.

Proposition 1. *For any linear CA on $\mathbb{Z}_N^L$, the transient length is no greater than $L(n_1 + n_2 + \cdots + n_\ell)$, where $N = p_1^{n_1} p_2^{n_2} \cdots p_\ell^{n_\ell}$ is the prime factorization of N.*

Proof. The sequence of submodules $A^n \mathbb{Z}_N^L$ of Z_N^L can be no longer than the length of the longest chain of distinct submodules of $\mathbb{Z}_N^L$, the *length* of $\mathbb{Z}_N^L$. However, the length of $\mathbb{Z}_N$ as a $\mathbb{Z}_N$-module is equal to $n_1 + n_2 + \cdots + n_\ell$ and the length of a product of two modules is equal to the sum of the lengths of the factors (see Proposition 6.9 in [1]). Thus the length of $\mathbb{Z}_N^L$ is equal to $L(n_1 + n_2 + \cdots + n_\ell)$. □

Sometimes we will use the notation T_x for the period length of the vector x. Furthermore, we define the *orbit space of* x to be the set

$$\mathcal{S}_x = \{ \sum_{i=0}^{T_x+k-1} \alpha_i A^i x : \alpha_i \in \mathbb{Z}_N\} \quad \text{(where } k \text{ is the transient length for } x\text{)},$$

the submodule of $\mathbb{Z}_N^L$ that is generated by the orbit of x. Clearly $\mathcal{S}_x$ is invariant under A. If $x \in \mathcal{K}$ then $\mathcal{S}_x \subset \mathcal{K}$ and $A^{T_x} y = y$ for all $y \in \mathcal{S}_x$. The orbit spaces form the finest subspace decomposition of $\mathbb{Z}_N^L$ into A-invariant subspaces.

Proposition 2. *If* $\mathcal{S}_x \cap \mathcal{S}_{x'} = \{0\}$ *for some* $x, x' \in \mathbb{Z}_N^L$, *then* $T_{x+x'} = \mathrm{lcm}(T_x, T_{x'})$.

Proof. It is clear that for $n = \mathrm{lcm}(T_x, T_{x'})$ we have $A^n(x + x') = x + x'$. Suppose $A^n(x + x') = x + x'$. Then $A^n x - x = x' - A^n x' \in \mathcal{S}_x \cap \mathcal{S}_{x'}$ and thus $A^n x - x = 0$ and $x' - A^n x = 0$. But this means that $T_x | n$ and $T_{x'} | n$ and so $\mathrm{lcm}(T_x, T_{x'}) | n$. □

For the case of a prime modulus, a bit more can be said.

Proposition 3. *For* p *a prime modulus, there is some point* $x \in \mathbb{Z}_p^L$ *whose period length* T *is maximal and all other points* y *fall into an orbit whose length is a divisor of* T.

Proof. Since the possible period lengths for A on $\mathbb{Z}_p^L$ are the same as those for A restricted to the core $\mathcal{K}$, there is no loss in generality in assuming that A is invertible.

Let the prime factorization in $\mathbb{Z}_p[x]$ of the minimal polynomial of the matrix A be $m(\lambda) = f_1(\lambda)^{n_1} f_2(\lambda)^{n_2} \cdots f_m(\lambda)^{n_\ell}$. Then by the Primary Decomposition theorem, each $f_i(\lambda)$ corresponds to an A-invariant subspace $V_i \subset \mathbb{Z}_p^L$. Let T_i be the order of $f_i(\lambda)$. Then the order of $m(\lambda)$ is $T = \mathrm{lcm}(T_1, T_2, \ldots, T_\ell)$. We need to show that there is some element $x \in \mathbb{Z}_p^L$ whose order is T.

The Primary Decomposition Theorem gives that $V_i \cap V_j = \{0\}$, so by Proposition 2 if $x_i \in V_i$, then the period length of $x = x_1 + x_2 + \cdots + x_\ell$ is the least common multiple of the period lengths of the x_i. Thus we show that there is some $x_i \in V_i$ with the period length of x_i equal to T_i.

For all $x \in V_i$, we have that $m_x(\lambda)$ divides $f_i(\lambda)^{n_i}$ and thus $m_x(\lambda) = f_i(\lambda)^{k_x}$ for some $0 \le k_x \le n_i$, as $f_i(\lambda)$ is irreducible. If no such $x \in V_i$ with

period length T_i exists, then for all $x \in V_i$, we have $k_x < n_i$, but then this means that $f_i(A)^k y = 0$ for all $y \in V_i$ where $k = \max\{k_x : x \in V_i\} < n_i$, which contradicts the fact that the minimal polynomial for A restricted to V_i is $f_i(\lambda)^{n_i}$.

□

Another useful fact is the following simple proposition.

Proposition 4. *If $y \in \mathcal{S}_x \cap \mathcal{S}_{x'}$ for some $x, x' \in \mathbb{Z}_N^L$, then $T_y | \gcd(T_x, T_{x'})$.*

Proof. We have $y \in \mathcal{S}_x$ so $T_y | T_x$ and similarly $T_y | T_{x'}$ and thus $T_y | \gcd(T_x, T_{x'})$.

□

3 Prime power moduli

The Chinese Remainder Theorem allows us to construct a description of the dynamics of a linear CA modulo N from descriptions of the dynamics of this same linear CA modulo the prime power factors of N. Thus, understanding the dynamics of A modulo p^k is the main step in understanding the dynamics of A with a general modulus. On the other hand, the modulus p^1 is easy, as linear algebra tools are applicable and this case is the basic building block. Thus, in this section our goal will be to examine how the dynamics change when we change the modulus from p^k to p^{k+1}. The main idea used in this section is an adaptation of ideas from [8, 7]. It is implicit in the solutions to problems in Section 3.2.2 (particularly #8) in [8] and is explicit in [7].

We start with a simple observation which points out that the dynamics become more "complicated" as you move from modulo p^k to modulo p^{k+1}.

Proposition 5. *The dynamics of A modulo p^k are embedded as a subset of the dynamics of A modulo p^{k+1}.*

Proof. Define the map $\phi : \mathbb{Z}_{p^k}^L \to \mathbb{Z}_{p^{k+1}}^L$ by $\phi(x) = px$. Clearly $A\phi(x) = \phi(Ax)$ and thus the orbit of $x \in \mathbb{Z}_{p^k}^L$ matches the orbit of $px \in \mathbb{Z}_{p^{k+1}}^L$.

□

3.1 Lifting orbits and the Ψ function

Consider now an element $x \in \mathbb{Z}_{p^k}^L$ in a periodic orbit of length T modulo p^k. This means that $A^T x = x \mod p^k$ and thus $A^T x - x = p^k y$ for some $y \in \mathbb{Z}^L$.

We will now investigate the possible orbit lengths modulo p^{k+1} for elements $\hat{x} \in \mathbb{Z}_{p^{k+1}}^L$ which satisfy $\hat{x} = x \mod p^k$. That is, $\hat{x} = x + p^k z$ with $z \in \mathbb{Z}_p^L$. Clearly for any such z, we get a corresponding $\hat{x}$, so the set of all "lifts" of x can be identified with $\mathbb{Z}_p^L$. We are free to choose which lift we identify as the origin in $\mathbb{Z}_p^L$, however the choice of that $\hat{x} \in \mathbb{Z}_{p^{k+1}}^L$ all of whose coordinates satisfy $0 \leq \hat{x}_i < p^k$ is a natural choice.

Another way of thinking about this is that we have the projection $\pi : \mathbb{Z}_{p^{k+1}}^L \to \mathbb{Z}_{p^k}^L$ given by $\pi(\hat{x}) = \hat{x} \mod p^k$ and the set of all lifts of x is the fiber $\mathbb{F}_x = \pi^{-1}(x) \subset \mathbb{Z}_{p^{k+1}}^L$ and this fiber is naturally identified with $\mathbb{Z}_p^L$ with $0 \in \mathbb{Z}_p^L$ being identified with x.

Now any $\hat{x} \in \mathbb{F}_x$ has period a multiple of T, since the orbit of $\hat{x}$ modulo p^{k+1} reduces to that of x modulo p^k. Thus, the orbit length of a lift can either stay the same or increase by some factor.

Since $A^T x = x \mod p^k$, we know that A^T maps any lift of x to another lift of x and thus corresponds to a map $\Psi : \mathbb{F}_x \to \mathbb{F}_x$. Now, $A^T x = x + y p^k$ and thus

$$A^T(x + z p^k) = A^T(x) + p^k A^T(z) = x + p^k y + p^k A^T(z) = x + p^k(y + A^T z). \quad (1)$$

Now, in (1) we only care about $y + A^T z$ up to modulus p (as we are only interested in the behaviour of this iteration modulo p^{k+1}). Thus, we define the Ψ *function associated with* x *and going from the modulus* p^k *to the modulus* p^{k+1} as

$$\Psi_k : \mathbb{Z}_p^L \to \mathbb{Z}_p^L, \quad \Psi_k(z) = A^T z + y \mod p. \quad (2)$$

The function Ψ_k completely describes the way the dynamics of the lifts of x are different from the dynamics of x. For instances if $\Psi_k(z) = z$, then we see that $\hat{x} = x + p^k z$ has the same period length as x as then $A^T(x + p^k z) = x + p^k \Psi_k(z) = x + p^k z$. In particular, if $y \neq 0$ then $\Psi_k(z) \neq z$ and so the period length of $x + p^k z$ is strictly greater than T.

Odd Prime Powers

Lemma 1. *Suppose that* p *is an odd prime,* $ker(A) = \{0\}$ *modulo* p*,* M *is the maximum period length modulo* p*,* x *has period* T *modulo* p^k*, and* $M|T$*. Then*

$$x + A^T x + A^{2T} x + \cdots A^{(p-1)T} x = px \mod p^{k+1}.$$

Proof. We see that $A^T x = x \mod p^k$ implies that $A^T x = x + p^k y$ for some $y \in \mathbb{Z}^L$.

Now suppose that p is an odd prime. Doing all our calculations modulo p^{k+1} we see

$$A^{2T}x = A^T(x + p^k y) = x + p^k y + p^k A^T y.$$

Now since $M|T$ we know $A^T y = y \mod p$ and thus $A^T y = y + pz$ for some $z \in \mathbb{Z}^L$. But then

$$A^{2T}x = x + p^k y + p^k A^T y = x + p^k y + p^k(y + pz) = x + 2p^k y + p^{k+1} z$$

which equals $x + 2p^k y$ modulo p^{k+1}. In a similar way using a simple induction we can show that

$$A^{jT}x = x + jp^k y \mod p^{k+1}$$

and thus

$$\begin{aligned} x + A^T x + A^{2T} x + \cdots A^{(p-1)T} x &= px + (1 + 2 + \cdots + p - 1)p^k y \\ &= px + \frac{(p-1)p}{2} p^k y = px, \end{aligned}$$

recalling that we are operating modulo p^{k+1}. □

Lemma 2. *Suppose that p is an odd prime, $ker(A) = \{0\}$ modulo p, M is the maximum period length modulo p, x has period T modulo p^k, and $M|T$. Then*

$$A^T x = x + yp^k \mod p^{k+1} \quad \Rightarrow \quad A^{pT} x = x + yp^{k+1} \mod p^{k+2}.$$

Proof. Since $A^T x = x \mod p^k$, we know that $A^T x = x + yp^k + zp^{k+1}$ for some $y \in \mathbb{Z}_p^L$ and $z \in \mathbb{Z}^L$. But then

$$A^{2T}x = A^T(x + yp^k + zp^{k+1}) = x + p^k(y + A^T y) + p^{k+1}(z + A^T z)$$

and by induction

$$A^{jT} = x + p^k(y + A^T y + \cdots + A^{(j-1)T} y) + p^{k+1}(z + A^T z + \cdots + A^{(j-1)T} z)$$

for each j. Thus

$$A^{pT}x = x + p^k \left(\sum_{j=0}^{p-1} A^{jT} y \right) + p^{k+1} \left(\sum_{j=0}^{p-1} A^{jT} z \right).$$

By Lemma 1 we have

$$\sum_{j=0}^{p-1} A^{jT} y = py \mod p^2 \quad \text{and} \quad \sum_{j=0}^{p-1} A^{jT} z = pz \mod p^2.$$

Therefore

$$\sum_{i=0}^{p-1} A^{jT} y = py + p^2 y', y' \in \mathbb{Z}^L \quad \text{and} \quad \sum_{i=0}^{p-1} A^{jT} z = pz + p^2 z', z' \in \mathbb{Z}^L,$$

and thus

$$\begin{aligned} A^{pT} x &= x + p^k \left(\sum_{j=0}^{p-1} A^{jT} y \right) + p^{k+1} \left(\sum_{j=0}^{p-1} A^{jT} z \right) \\ &= x + p^k (py + p^2 y') + p^{k+1} (pz + p^2 z') \\ &= x + p^{k+1} y \mod p^{k+2}. \end{aligned}$$

□

Putting these lemmas together, we see that in a fairly generic situation the period length of an element x goes up by a factor of p for each increase in the power of p in the modulus.

Theorem 1. *Suppose that p is an odd prime, $ker(A) = \{0\}$ modulo p, M is the maximum period length modulo p, x has period T modulo p^k, and $M|T$. Further suppose that $\Psi_k(z) = A^T z + y$ with $y \neq 0$. Then*

$$\Psi_{k+\ell}(z) = A^{p^\ell T} z + y.$$

In particular, the period of any lift $\hat{x} \in \mathbb{Z}^L_{p^{k+\ell}}$ of $x \in \mathbb{Z}^L_{p^k}$ is $p^\ell T$.

Proof. If $y \neq 0$, then the period of a lift $\hat{x} \in \mathbb{Z}^L_{p^{k+1}}$ of x is pT by Lemma 2. Furthermore, Lemma 2 also shows that the y in the definition of Ψ_{k+1} is the same y in the definition of Ψ_k. By induction the result follows. □

Powers of Two

The situation for powers of two is more complicated, mainly because Lemma 1 doesn't work out the same. If $A^T x = x$ modulo 2^k, then $A^T x = x + 2^k y$ for some $y \in Z^L$ and so

$$A^{2T} x = A^T (x + 2^k y) = x + 2^k y + 2^k A^T y.$$

Supposing that T is a multiple of the maximal period length modulo 2, then $A^T y = y$ modulo 2 and thus $A^T y = y + 2y'$ for some $y' \in \mathbb{Z}^L$. But then

$$A^{2T}x = x + 2^k y + 2^k y + 2^{k+1}y' = x \mod 2^{k+1}.$$

This proves the following proposition.

Proposition 6. *Suppose that $ker(A) = \{0\}$ modulo 2, M is the maximum period length modulo 2, x has period T modulo 2^k, and $M|T$. Then modulo 2^{k+1}, either every lift of x has period T or every lift of x has period $2T$.*

As for the relationship between Ψ_k and Ψ_{k+1} in this case, it is a little bit more complicated. The proof of the following is similar to that of Lemmas 1 and 2 and we omit it.

Proposition 7. *Suppose that $ker(A) = \{0\}$ modulo 2, M is the maximum period length modulo 2, $A^T x = x + 2^k y$ modulo 2^{k+1} (so x has period T modulo 2^k), and $M|T$. Then*

$$A^{2T}x = x + 2^{k+1}(y + y') \mod 2^{k+2}$$

where $A^T y = y + 2y'$. Thus if T is a multiple of all the period lengths for modulo 4,

$$A^{2T}x = x + 2^{k+1}y \mod 2^{k+2}.$$

As a consequence, if T is a multiple of all the period lengths for modulo 4, then we know that Ψ_k has the same y vector as Ψ_{k+1} and thus the period length goes up the same factor for each increase in exponent.

4 Circulant Matrices

The special case of a linear CA with A a circulant matrix has nice additional structure which is worth mentioning. In particular, these CA have an update rule which is *shift invariant*. That is, if $S(x_1, x_2, \ldots, x_L) = (x_2, x_3, \ldots, x_L, x_1)$ is the left shift operation, then $AS = SA$ and so the dynamical behaviour of x and Sx is the same. When Λ as a graph has the structure of a finite cycle, this will occur exactly when the update rule has the same (relative) definition at each site.

A particular example of interest is the $L \times L$ Wolfram Rule 90 matrix

$$W_L = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

We can compute that

$$det(W_L) = \begin{cases} 0, & \text{if} \quad \text{L} = 4\text{k} \\ 2, & \text{if} \quad \text{L} = 4\text{k} + 1 \\ -4, & \text{if} \quad \text{L} = 4\text{k} + 2 \\ 2, & \text{if} \quad \text{L} = 4\text{k} + 3, \end{cases} \tag{3}$$

and thus $ker(W_L) = \{0\}$ modulo any odd N if $L \neq 4k$. In particular, a linear CA based on W_L has no transient states if and only if N is odd and $L \neq 4k$.

Proposition 8. *For a shift invariant linear CA the maximal period length is the period length of the vector $x = (1, 0, 0, \ldots, 0)$ and all other period lengths divide this period length.*

Proof. First suppose that x is in a periodic orbit of period T. Then for any $y \in \mathbb{Z}_N^L$ there are coefficients $\alpha_i \in \mathbb{Z}_N$ with

$$y = \sum_{i=0}^{L-1} \alpha_i S^i x$$

as the set $\{x, Sx, S^2x, \ldots, S^{L-1}x\}$ is a generating set for $\mathbb{Z}_N^L$. But then

$$A^T y = \sum_{i=0}^{L-1} \alpha_i A^T S^i x = \sum_{i=0}^{L-1} \alpha_i S^i x = y.$$

This means that the period length for y is a divisor of T. □

Proposition 8 remains true for any x as long as $\{x, Sx, S^2x, \ldots, S^{L-1}x\}$ is a generating set for $\mathbb{Z}_N^L$.

Proposition 9. *Let $N = p_1^{n_1} p_2^{n_2} \cdots p_\ell^{n_\ell}$ be an odd number. Furthermore, let $M_1, M_2, \ldots, M_\ell$ be the maximal period length of W_L modulo $p_1, p_2, \ldots, p_\ell$ respectively. Then the maximal period length of W_L modulo N is*

$$\mathrm{lcm}(M_1 p_1^{n_1-1}, M_2 p_2^{n_2-1}, \ldots, M_\ell p_\ell^{n_\ell-1}).$$

Proof. This is just a consequence of Proposition 8 and Theorem 1 and the comments about the Chinese Remainder Theorem. □

This behaviour of W_L is generic for shift invariant linear CA.

Theorem 2. *Let A be a shift invariant matrix with $ker(A) = \{0\}$ for the odd modulus $N = p_1^{n_1} p_2^{n_2} \ldots p_\ell^{n_\ell}$. Furthermore, let $M_1, M_2, \ldots, M_\ell$ be the maximal period length of A modulo $p_1, p_2, \ldots, p_\ell$ respectively. Then the maximal period length of A modulo N is*

$$\mathrm{lcm}(M_1 p_1^{n_1-1}, M_2 p_2^{n_2-1}, \ldots, M_\ell p_\ell^{n_\ell-1}).$$

More general shift invariant linear CAs

It is simple to generalize the idea of shift invariance to more general linear CAs. Suppose that Λ (the set of automata) has the structure of a homogeneous graph and let $\mathcal{G}$ be the set of all automorphisms of Λ. Then we have $\mathcal{G}$ acting transitively on Λ. Further, $\theta \in \mathcal{G}$ acts on $\mathcal{A}^\Lambda$ by $\theta(f)(x) = f(\theta(x))$. If Φ commutes with this action, then the matrix A which represents Φ will have a generalized form of invariance like being a circulant matrix. That is, each $\theta \in \mathcal{G}$ permutes the rows and columns of A but A remains fixed under each of these permutations. In cases like this, it is easy to see that Proposition 8 and Theorem 2 remain true.

ACKNOWLEDGMENTS

This work grew out of the second author's Honours Thesis at Acadia University. This work was supported in part by funds from NSERC and the authors would like to thank NSERC for this support; FM for a Discovery Grant and DP for an NSERC PGSM.

References

[1] Atiyah, M., MacDonald, I.G., *Introduction to commutative algebra*, Westview Press, 1994.

[2] Breuer, F. "Ducci sequences over commutative groups," *Comm. Algebra* **27**, no. 12, pp. 5999-6013, 1999.

[3] Breuer, F. "Ducci sequences and cyclotomic fields," *preprint.*

[4] Breuer, F., Lötter, E.C., van der Merwe, A.B., "Ducci sequences and cyclotomic polynomials," *Finite Fields Appl.*, **13**, pp. 293-304, 2007.

[5] Brown, W.C., *Matrices over Commutative Rings*, Marcel Dekker, New York, 1993.

[6] Calkin, N.J., Stevens, J., Thomas, D., "A characterization for the length of cycles of the n-number Ducci game," *Fibonacci Quart.*, **43**, no. 1, pp. 53-59, 2005.

[7] desJardins D.L., Zieve M.E., "On the structure of polynomial mappings modulo an odd prime power," arXiv: Number Theory `http://arxiv.org/abs/math/0103046/`, 2001.

[8] Knuth, D.E., *The art of computer programming:Seminumerical algorithms*, volume 2, Addison-Wesley, 1969.

[9] Lidl, N., Niederreiter, H., *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, 1994.

[10] Martin, O., Odlyzko, A., Wolfram, S. "Algebraic Properties of Cellular Automata," *Commun. Math. Phys.* **93**, pp. 219-258 1984.

[11] Misiurewicz, M., Stevens, J., Thomas, D., "Iterations of linear maps over finite fields," *Linear Algebra Appl.*, **413**, no. 1, pp. 218-234, 2006.

[12] Stevens, J., Lettieri, S., Thomas, D., "Characteristic and Minimal Polynomials of Linear Cellular Automata," *Rocky Mountain Journal of Mathematics*, **36**, no. 3, pp. 1077-1087, 2006.

[13] Wolfram, S. *A New Kind of Science*, Wolfram Media Inc, Illinois, 2002.