Atlantic Electronic
Journal of Mathematics
Volume **2**, Number **1**, Summer **2007**

http://aejm.ca
http://aejm.ca/rema
pp. **55–63**

ALGEBRAIC DYNAMICS OF A ONE-PARAMETER CLASS OF MAPS OVER $\mathbb{Z}_2$

Luba Lidman and Diana M. Thomas

Department of Mathematical Sciences
Montclair State University
Upper Montclair, NJ 07043

Abstract. Motivated by the Ducci Map and Wolfram's Rule 90, this paper studies the relationship of the period lengths of the maps $W(n,k) = I_n + T_n^k$ as a function of n and k, where I_n is the identity map and T_n is the left shift map on $\mathbb{Z}_2^n$. It is found that $W(n,k)$ is conjugate to $W(n,1)$ for $(n,k) = 1$. A closed form expression for the minimal polynomial of $W(n,k)$ is obtained. In addition, using the language of minimal polynomials, we find that when $(n,k) \neq 1$,the period lengths of $W(n,k)$ are equal to the period lengths of $W(s,1)$ where $s \cdot (n,k) = n$.

1. **Introduction.** Interest in algebraic methods applied to dynamical systems has been steadily increasing with approaches varying by the field where the problem originated [11, 15, 18, 21, 22, 23]. The purpose of this paper is to apply algebraic techniques to study the dynamics of the class of linear maps

$$W(n,k) : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$$

defined by

$$W(n,k) = I_n + T_n^k \tag{1}$$

where I_n is the identity map and T_n is the left shift map,

$$\begin{aligned} I_n(\mathbf{x}) &= (x_1, x_2, \ldots, x_n) \\ T_n(\mathbf{x}) &= (x_2, x_3, \ldots, x_n, x_1) \end{aligned}$$

for $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$.

One important fact to notice about the iterates of $W(n,k)$ (or any other deterministic map acting on $\mathbb{Z}_2^n$) is that the forward images of any vector in $\mathbb{Z}_2^n$ must eventually cycle. This is because the vector space $\mathbb{Z}_2^n$ is a finite set consisting of 2^n elements. Forward images of any vector have only 2^n different possible range values and therefore must eventually repeat. More precisely, for any $\mathbf{x} \in \mathbb{Z}_2^n$, there exist nonnegative integers, $j \leq c$ such that

$$W^c(n,k)\mathbf{x} = W^j(n,k)\mathbf{x}.$$

Key words and phrases. Ducci, Wolfram's Rule 90, finite field, iterations.

If j and c are the first of such integers, then we say c is the *period* or the *cycle length* associated to $\mathbf{x}$ and j is the *transient* or *preperiodic length* of $\mathbf{x}$. For example, if $n=3$, $k=1$ then $W(3,1)(\mathbf{x}) = (x_1+x_2, x_2+x_3, x_3+x_1)$ where all computations are performed modulo 2. Applying $W(3,1)$ to $\mathbf{x}=(1,0,0)$ yields,

$$\begin{aligned} W(3,1)\mathbf{x} &= (1,0,1) \\ W(3,1)^2\mathbf{x} &= (1,1,0) \\ W(3,1)^3\mathbf{x} &= (1,0,1) = W(3,1)\mathbf{x}. \end{aligned}$$

So, the transient length of $(1,0,0)$ is $j=1$ and the cycle length is $c=3$.
Because all initial vectors in $\mathbb{Z}_2^n$ eventually cycle under iteration of $W(n,k)$, we seek to find a relationship between the period lengths of $W(n,k)$ as a function of n and k. The motivation for studying the dynamics of (1) follows.
For $k=1$, $W(n,k)$ is the Ducci map which has been studied extensively for over 100 years (see for example [1, 3, 5, 6, 7, 13, 17]). Although many questions on the dynamics of the Ducci map have been answered, there still exist some long standing open problems which are listed in [4].
For $k=2$, $W(n,k)$ is equal to $T_n(S_n+T_n)$ where S_n is the right shift map on $\mathbb{Z}_2^n$,

$$S_n(\mathbf{x}) = (x_n, x_1, x_2, \ldots, x_{n-1})$$

for $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$. This map is a left shift of cellular automata listed as Wolfram's Rule 90 in [24]. Interest in Wolfram's Rule 90 originated through the algebraic treatment of the map in [15] with results generalized further in [10, 11, 23]. In [18] connections between the dynamics of $W(n,1)$ and $W(n,2)$ were obtained. These relationships motivate the question addressed by this paper: Can the cyclic behavior of $W(n,k)$ in dimension n be characterized as a function of k?
The next section will introduce the language of minimal polynomials which is used to obtain cycle lengths of $W(n,k)$ as orders of minimal annihilating polynomials. In this section, data on cycle lengths, minimal and characteristic polynomials as a function of both n and k are provided. In the final section we prove results characterizing the dynamics of $W(n,k)$ as a function of n and k.

2. **Characterization of cycle lengths as orders of polynomials.**

Although it is possible to iterate all initial vectors on $\mathbb{Z}_2^n$ under the map $W(n,k)$ for small values of n (see for example Figure 2), this procedure is too computationally complex for large values of n. In [20], Stevens developed an algorithm based on minimal annihilating polynomials to determine cycle lengths without iteration. In order to apply this technique, we will need the following definitions.

Definition 1. Let A be an $n\times n$ matrix over the field $\mathbb{F}$ and let $\mathbf{v} \in \mathbb{F}^n$. The polynomial $\mu_v(\lambda)$ is the minimal annihilating polynomial of the vector $\mathbf{v}$ under A if $\mu_v(\lambda)$ is the monic polynomial of least degree such that $\mu_v(A)\mathbf{v} = 0$.

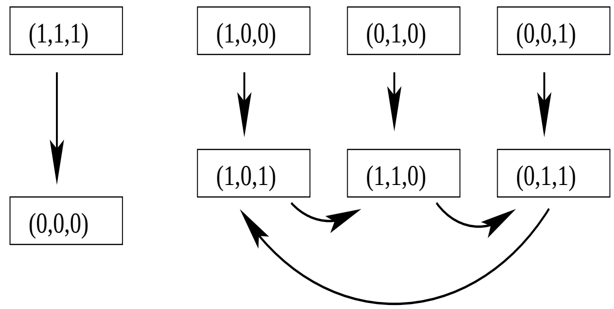

FIGURE 1. Complete dynamics under iteration of $W(3,1)$ on $\mathbb{Z}_2^3$

A minimal annihilating polynomial is not to be confused with the *minimal polynomial* of an $n \times n$ matrix A. The minimal polynomial, $\mu(\lambda)$ of a $n \times n$ matrix A with entries from the field $\mathbb{F}$ is the monic polynomial of least degree with the property that $\mu(A) = 0$. Notice that μ is not dependent on one particular vector $\mathbf{v}$. This difference is illustrated in the next example.

Example 1. *Consider the map $W(6,1)$ which equals*

$$W(6,1)(\mathbf{x}) = (x_1 + x_2, x_2 + x_3, x_3 + x_4, x_4 + x_5, x_5 + x_6, x_6 + x_1)$$

where the addition is computed modulo two.
The matrix representation of $W(6,1)$ in the standard basis of $\mathbb{Z}_2^n$ is

$$A_{W(6,1)} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

which has minimal polynomial

$$\mu(\lambda) = (1+\lambda)^6 + 1.$$

However, for $\mathbf{v} = (1,1,0,1,1,0)$

$$((A_{W(6,1)} + I)^3 + I)\mathbf{v} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

It is easy to see that there can be no lower degree polynomial that annihilates $\mathbf{v}$, so $\mu_v(\lambda) = (\lambda+1)^3 + 1$.

We now define the order of a polynomial.

Definition 2. let $q(\lambda)$ be a monic polynomial defined over a finite field $\mathbb{F}$. Write $q(\lambda) = \lambda^j \tilde{q}(\lambda)$ where $\tilde{q}(0) \neq 0$ and j is a nonnegative integer. Then the order of $q(\lambda)$ is the minimal positive integer m such that

$$\tilde{q}(\lambda) | \lambda^m - 1,$$

and we write $\mathrm{ord}(q(\lambda)) = m$.

The order of a polynomial is always guaranteed to exist when defined over a finite field [12]. We compute the order of a polynomial in the next example.

Example 2. *From the previous example we know that for $A_{W(6,1)}$ and $\mathbf{v} = (1,1,0,1,1,0)$, that the minimal annihilating polynomial is $\mu_v(\lambda) = (\lambda+1)^3 + 1$. To illustrate how to compute order, we shall find the order of $\mu_v(\lambda)$. Expanding $\mu_v(\lambda)$ modulo 2 yields,*

$$(\lambda+1)^3 + 1 = \lambda^3 + \lambda^2 + \lambda = \lambda(\lambda^2 + \lambda + 1).$$

So $\tilde{\mu}_v(\lambda) = \lambda^2 + \lambda + 1$. Because $\lambda^3 - 1 = (\lambda - 1)\tilde{\mu}_v(\lambda)$ by the difference of cubes formula, we have $\tilde{\mu}_v(\lambda)|\lambda^3 - 1$. It is clear that $\tilde{\mu}_v(\lambda)$ does not divide $\lambda^m - 1$ for $m < 3$ and therefore the order of $\mu_v(\lambda)$ is 3.

The characterization of cycle lengths as orders of polynomials first appeared for circulant matrices in [11] and was later generalized for any matrix defined over a finite field in [20]. The proof of the next theorem appears in [2].

Theorem 2.1. *Let A be an $n \times n$ matrix with entries from a finite field $\mathbb{F}$ and let $\mathbf{v} \in \mathbb{F}^n$. If $\mu_v(\lambda) = \lambda^j \tilde{\mu}(\lambda)$ where $\tilde{\mu}(0) \neq 0$, is the minimal annihilating polynomial of $\mathbf{v}$ under A, then $A^j\mathbf{v}$ belongs to a cycle of length $c = ord(\mu_v(\lambda))$.*

The characterization formulated by Theorem 2.1 provides a method to compute the cycle length and preperiod length of a vector without iteration. To understand how to implement Theorem 2.1, we look to previous examples. We know that $\mathbf{v} = (1,1,0,1,1,0)$ has minimal annihilating polynomial with order 3. Indeed iterating $\mathbf{v} = (1,1,0,1,1,0)$ under $W(6,1)$ yields,

$$\begin{aligned} W(6,1)\mathbf{v} &= (0,1,1,0,1,1) \\ W(6,1)^2\mathbf{v} &= (1,0,1,1,0,1) \\ W(6,1)^3\mathbf{v} &= (1,1,0,1,1,0) = \mathbf{v} \end{aligned}$$

Therefore, $\mathbf{v}$ belongs to a cycle with period 3 equal to the order of its minimal annihilating polynomial.

A program in Maple was developed by Stevens in [20] to determine all minimal annihilating polynomials and their corresponding orders for an $n \times n$ matrix A defined over $\mathbb{Z}_p$ where p is prime. Using this program, we are able to generate the cycle lengths of $W(n,k)$ and data is provided for $n = 3, \ldots, 20$ and $k = 1, \ldots, 6$ in Table 2. Several patterns emerge from the cyclic information in Table 2. One of the questions that has

n	k = 1	k = 2	k = 3	k = 4	k = 5	k = 6
$n = 3$	$1, 3$	$1, 3$	1	$1, 3$	$1, 3$	1
$n = 4$	1	1	1	1	1	1
$n = 5$	$1, 15$	$1, 15$	$1, 15$	$1, 15$	1	$1, 15$
$n = 6$	$1, 3, 6$	$1, 3$	1	$1, 3$	$1, 3, 6$	1
$n = 7$	$1, 7$	$1, 7$	$1, 7$	$1, 7$	$1, 7$	$1, 7$
$n = 8$	1	1	1	1	1	1
$n = 9$	$1, 3, 63$	$1, 3, 63$	$1, 3$	$1, 3, 63$	$1, 3, 63$	$1, 3$
$n = 10$	$1, 15, 30$	$1, 15$	$1, 15, 30$	$1, 15$	1	$1, 15$
$n = 11$	$1, 341$	$1, 341$	$1, 341$	$1, 341$	$1, 341$	$1, 341$
$n = 12$	$1, 3, 6, 12$	$1, 3, 6$	1	$1, 3$	$1, 3, 6, 12$	1
$n = 13$	$1, 819$	$1, 819$	$1, 819$	$1, 819$	$1, 819$	$1, 819$
$n = 14$	$1, 7, 14$	$1, 7$	$1, 7, 14$	$1, 7$	$1, 7, 14$	$1, 7$
$n = 15$	$1, 3, 5, 15$	$1, 3, 5, 15$	$1, 15$	$1, 3, 5, 15$	$1, 3$	$1, 15$
$n = 16$	1	1	1	1	1	1
$n = 17$	$1, 85, 255$	$1, 85, 255$	$1, 85, 255$	$1, 85, 255$	$1, 85, 255$	$1, 85, 255$
$n = 18$	$1, 3, 6, 63, 126$	$1, 3, 63$	$1, 3, 6$	$1, 3, 63$	$1, 3, 6, 63, 126$	$1, 3$
$n = 19$	$1, 9709$	$1, 9709$	$1, 9709$	$1, 9709$	$1, 9709$	$1, 9709$
$n = 20$	$1, 15, 30, 60$	$1, 15, 30$	$1, 15, 30, 60$	$1, 15$	1	$1, 15, 30$

TABLE 1. Cycle lengths under iterations of $W(n, k)$ for $n = 1, \ldots, 20$ and $k = 1, \ldots, 6$.

appeared often in the literature about the Ducci map is to identify for which values of n do all initial vectors eventually vanish. It has been proved and reproved that this occurs when n is a power of two [3]. Examining Table 2 for $k = 1$, we see that there is only one cycle of period one whenever n is a power of two. Because the zero vector is a fixed point for all values of n, this implies that the only cycle that exists when n is a power of two, is the zero fixed point. We generalize this result for the maps $W(n, k)$.

Theorem 2.2. *Let $n = k2^j$ where j is any nonnegative integer. Then for any $\mathbf{x} \in \mathbb{Z}_2^n$, the forward iterates of $\mathbf{x}$ under $W(n, k)$ converge to zero.*

Proof:
We will prove that the map itself vanishes in $k2^j$ iterates.
Because shifting a vector left n times shifts the vector back to its original configuration, $T_n^n = I$. Using this fact and expanding modulo 2 yields

$$W(n, k)^{2^j} = (I_n + T_n^k)^{2^j} = I_n^{2^j} + T_n^{2^j k} = I + T_n^n = I + I = 2I = 0$$

■

Several other patterns are also quickly identified. For example, when n and k are relatively prime, it appears that the cycle lengths of $W(n, k)$ are equal. To prove this result, it would be beneficial to determine a closed form expression for the minimal annihilating polynomials of $W(n,k)$ as function of n and k.

Each minimal annihilating polynomial is a factor of the minimal polynomial [9]. In Example 1, we see this result illustrated by expansion modulo 2:

$$\mu_v(\lambda)^2 = ((1+\lambda)^3+1)^2 = (1+\lambda)^6+1 = \mu(\lambda).$$

In addition, there exists at least one vector, $\mathbf{v} \in \mathbb{Z}_2^n$ whose minimal annihilating polynomial is the minimal polynomial [9]. In fact, in [13] it was proved that the minimal annihilating polynomial of the standard basis vectors in $\mathbb{Z}_2^n$ under any linear circulant matrix is the minimal polynomial. Moreover, the $\text{ord}(\mu_v(\lambda)) \leq \text{ord}(\mu(\lambda))$ for all $\mathbf{v} \in \mathbb{Z}_2^n$. Therefore, the maximal period length is given by $\text{ord}(\mu(\lambda))$ [12]. Due to all the information we can gather from the minimal polynomial, *determining a closed form expression for the minimal polynomial of $W(n,k)$ as a function of n and k is of interest.*

In the next section, we determine the minimal polynomials of $W(n,k)$ and then use the closed form expressions to prove cyclic relationships we see in Table 2.

3. The relationship of cycle lengths of $W(n,k)$ as a function of n and k.

Some of the patterns we see in Table 2 are due to the structure of $W(n,k)$. For example, if $n|k$, then $W(n,k) = I_n + T_n^k = I_n + I_n = 0$. Thus when $n|k$ all vectors converge to the zero vector, which is reflected in Table 2. Another observation is that $W(n,n+1) = I_n + T_n^{n+1} = I_n + T_n = W(n,1)$. Thus, the maps $W(n,k)$ are cyclic of period l in k and $l|n$. This fact is also reflected in Table 2.

In fact, not just the cycle lengths are equal when $(n,k)=1$, but the maps themselves are connected in this case. We describe this relationship in the next example.

Example 3. *Consider $n=5, k=3$ and define the permutation function*

$$\pi : (1,2,3,4,5) \to (1,2,3,4,5)$$

by $\pi(jk+1) = j+1,\ j=0,1,2,3,4$, where the addition is performed modulo 5. That is,

$$\begin{aligned}
&\pi(1)=1,\ \pi(1\cdot 3+1)=\pi(4)=2,\\
&\pi(2\cdot 3+1)=\pi(7)=\pi(2)=3,\ \pi(3\cdot 3+1)=\pi(10)=\pi(5)=4\\
&\pi(4\cdot 3+1)=\pi(13)=\pi(3)=5.
\end{aligned}$$

Notice that π is a permutation because $(5,3)=1$.

Define $\sigma(\mathbf{x}) = (x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, x_{\pi(4)}x_{\pi(5)})$, for $\mathbf{x} = (x_1,x_2,x_3,x_4,x_5)$. Then,

$$\begin{aligned}
W(5,3)\sigma(\mathbf{x}) &= W(5,3)(x_1,x_3,x_5,x_2,x_4)\\
&= (x_1+x_2, x_3+x_4, x_5+x_1, x_2+x_3, x_4+x_5)
\end{aligned}$$

Computing $\pi^{-1}(j)$ yields:

$$\pi^{-1}(1)=1,\ \pi^{-1}(2)=4,\ \pi^{-1}(3)=2,\ \pi^{-1}(4)=5,\ \pi^{-1}(5)=3$$

and so,

$$\sigma^{-1}W(5,3)\sigma(\mathbf{x}) = (x_1 + x_2, x_2 + x_3, x_3 + x_4, x_4 + x_5, x_5 + x_1) = W(5,1)(\mathbf{x}).$$

Clearly, the permutation in the above example can be generalized whenever $(n, k) = 1$ and this results in the following theorem.

Theorem 3.1. *Let $(n,k) = 1$. Then $W(n,k)$ is algebraically conjugate to $W(n,1)$.*

Proof:
Let $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$ and define $\sigma : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ by

$$\sigma(\mathbf{x}) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$$

where

$$\pi(jk+1) = j+1, \;\; j = 0, 1, 2, \ldots, n$$

with addition performed modulo n. Because $(n,k) = 1$, π is a permutation of $(1, 2, \ldots, n)$.
The components from $jk+1$ to $(j+1)k+1$ are k terms apart yielding,

$$\left(W(n,k)\sigma(\mathbf{x})\right)_{jk+1} = x_j + x_{j+1}.$$

The permutation, $\pi^{-1}(j) = (j-1)k+1$ (again with addition computed modulo n), so

$$\left(\sigma^{-1}W(n,k)\sigma(\mathbf{x})\right)_j = x_j + x_{j+1},$$

and so $W(n,k)$ is conjugate to $W(n,1)$. ■

We now move to the case where $(n,k) \neq 1$. In this situation, patterns from Table 2 seem to be less immediate. It appears that if $(n,k) = l$ then the cycle lengths for $W(n,k)$ are equal to the cycle lengths for $W(s,1)$ where $n = ls$. For example, if $n = 18$ and $k = 4$, then $l = 2$ and $s = 9$. The cycle lengths for $W(9,1)$ are $1, 3, 63$ which agree with the cycle lengths of $W(18,4)$. In the next theorem, we prove that the minimal polynomial of $W(n,k)$ in the case of $(n,k) \neq 1$ is equal to the minimal polynomial of $W(s,1)$. Because the characteristic polynomial is not equal to the minimal polynomial for $(n,k) \neq 1$, it is obvious that the maps $W(n,k)$ and $W(s,1)$ are not similar.

Theorem 3.2. *Let $gcd(n,k) \neq 1$ and let $L = lcm(n,k)$. If $L = ks$ where $s \in \mathbb{N}$, then the minimal polynomial of $A_{W(n,k)}$ is*

$$\mu(\lambda) = (1+\lambda)^s + 1.$$

Proof:
We will first show that $\mu(\lambda)$ annihilates $A_{W(n,k)}$,

$$\mu(W(n,k)) = (I_n + I_n + T_n^k)^s + I_n = T_n^{ks} + I_n.$$

Because $n | ks$, $T_n^{ks} = I_n$, and so $\mu(W(n,k)) = 0$.

Now we will prove the minimality property of $\mu(\lambda)$. In [13, 18] it was proved that the degree of the minimal polynomial equals the minimum number of linearly independent iterates of e_1 where $e_1 = (1, 0, 0, \ldots, 0)$ is the first standard basis vector in $\mathbb{Z}_2^n$. Symbolically iterating e_1 yields the sequence, $e_1 + T_n^{jk} e_1$ for $j = 0, 1, 2, 3, \ldots$. The set of vectors

$$S = \{e_1, e_1 + T^k e_1, \ldots, e_1 + T^{jk} e_1\}$$

is linearly independent if and only if no mk equals rk modulo n for any two nonnegative integers m, r. Thus, the first such j that makes S a dependent set is $j = s$. Therefore, the set of linearly independent iterates of e_1 are:

$$\{e_1, e_1 + T^k e_1, \ldots, e_1 + T^{(s-1)k} e_1\}$$

and hence the degree of the minimal polynomial must be s. By uniqueness of the minimal polynomial, this proves

$$\mu(\lambda) = (1 + \lambda)^s + 1.$$

■

This result yields the cyclic behavior seen in Table 2 as stated in the next corollary.

Corollary 1. *Suppose that* $(n, k) = l \neq 1$ *and write* $ls = n$ *for some nonnegative integer* s*. Then the cycle lengths of* $W(n, k)$ *equal the cycle lengths of* $W(s, 1)$*.*

REFERENCES

[1] F. Breuer, F., Lőtter and B. van der Merwe, Ducci sequences and cyclotomic polynomials, preprint.

[2] N. Calkin, J. Stevens and D. Thomas, A characterization of lengths of cycles of the n-number Ducci game, Fibonacci Quarterly, in press.

[3] M. Chamberland, Unbounded Ducci sequences, J. Difference Equ. Appl., 2003, 9, 887-895.

[4] M. Chamberland and D. Thomas, The n-number Ducci game (open problems and conjectures), J. Difference Equ. Appl., 2004, 10, 339-342.

[5] C. Ciamberlini and A. Marengoni. Su una interessante curiosit, à numerica Periodiche di Matematiche, 1937, 17:25–30.

[6] A. Ehrlich, Periods in Ducci's n-number game of differences, Fibonacci Quart., 1990, 28, 302-305.

[7] H. Glaser and G. Schöffl, Ducci-sequences and Pascal's triangle, Fibonacci Quart., 1995, 33, 313-324.

[8] R. Honsberger, *Ingenuity in mathematics*,1970, Yale University.

[9] N. Jacobson, *Lectures in abstract algebra. Vol. II. Linear Algebra*, 1953, Van Nostrand Co., Toronto-New York-London.

[10] E. Jen, Cylindrical cellular automata, Comm. Math. Phys., 1988, 118, 569-590.

[11] E. Jen, Linear cellular automata and recurring sequences in finite fields, Comm. Math. Phys., 1988, 119, 13-28.

[12] R. Lidl and H. Niederreiter, *Finite fields, Encyclopedia of Mathematics and its Applications*, 1983, 20, Addison-Wesley, Reading, MA.

[13] S. Lettieri, J. G. Stevens and D. M. Thomas, Characteristic and minimal polynomials of linear cellular automata, Rocky Mountain J. Math. (in press).

[14] A. Ludington Furno, Cycles of differences of integers, J. Number Theory, 1981, 13, 255-261.
[15] O. Martin, A. Odlyzko and S. Wolfram, Algebraic properties of cellular automata, Comm. Math. Phys., 1984, 93, 219-258.
[16] J. C. P. Miller, Periodic forests of stunted trees, Philos. Trans. Roy. Soc. Lond., 1970, A266, 63-111.
[17] M. Misiurewicz and A. Schinzel, On n numbers on a circle, Hardy-Ramanujan Journal, 1988, 11, 30-39.
[18] M. Misiurewicz, J.G. Stevens, D.M. Thomas, Iterations of linear maps over finite fields, under review, 2004.
[19] J. Stevens, R. Rosensweig and A. Cerkanowicz, Transient and cyclic behavior of cellular automata with null boundary Conditions, J. Statist. Phys., 1993, 73, 159-174.
[20] J. G. Stevens, On the construction of state diagrams for cellular automata with additive rules, Inform. Sci., 1999, 115, 43-59.
[21] J. A. G. Roberts and F. Vivaldi, Arithmetical method to detect integrability in maps, Phys. Rev. Lett. 90 (2003) 034102; also Publisher's Note, Phys. Rev. Lett. 90 (2003) 079902.
[22] K. Schmidt, Dynamic systems of algebraic origin, Birkha"user 1995.
[23] F. Vivaldi, Geometry of linear maps over Finite Fields, Nonlinearity , 5, (1992), 133-147.
[24] S. Wolfram, *A new kind of science*, 2002, Wolfram Media, Champaign, IL.

Recieved 1 May 2007
E-mail address: thomasdia@mail.montclair.edu