A CHARACTERIZATION FOR THE LENGTH OF CYCLES OF THE N - NUMBER DUCCI GAME

Neil J. Calkin
Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-1907

John G. Stevens
Department of Mathematical Sciences, Montclair State University, Upper Montclair, NJ 07043

Diana M. Thomas
Department of Mathematical Sciences, Montclair State University, Upper Montclair, NJ 07043

(Submitted June 2002-Final Revision September 2002)

1. INTRODUCTION

In the late 1800's, E. Ducci made a series of observations on iterations of the map $D : \mathbb{Z}^n \to \mathbb{Z}^n$,

$$D(\boldsymbol{x}) = (|x_1 - x_2|, |x_2 - x_3|, \dots, |x_n - x_1|) \tag{1}$$

where $\boldsymbol{x} = (x_1, x_2, \dots, x_n)$ [12].

The dynamics of the Ducci map have been examined for special cases of n in [7, 17, 27]. In addition, many interesting results have been developed for arbitrary n in [1, 2, 8].

One of the main results, which has been proved several times in the literature, states that for $n = 2^k$ for some positive integer k, all initial vectors converge to the zero vector [1, 5]. For the case $n \neq 2^k$, it has been proved that every initial vector converges to a periodic cycle [8]. Specific properties on the lengths of the period have been examined by Ehrlich in [8]. Ehrlich proved some divisibility conditions relating odd vector length to maximal period length. Using these relationships, he generated maximal period lengths for odd n. Due to computing limitations, the lengths were calculated only to $n = 165$.

This article will develop new insights into the period lengths for any positive integer n by considering the Ducci game as a map on the vector space $\mathbb{Z}_2^n$.

2. THE n NUMBER DUCCI AS A MAP ON THE VECTOR SPACE $\mathbb{Z}_2^n$

In order to understand the dynamics of the Ducci map on $\mathbb{Z}$, we need only understand how the map behaves on binary vectors. This observation is due to an early result that states every initial vector converges in a finite number of iterations to a periodic solution of the form $k(x_1, x_2, \dots, x_n)$ where $x_i \in \{0, 1\}$ and k is a positive constant [3].

Ehrlich noticed that the Ducci map on binary vectors can be written as

$$D\boldsymbol{x} = ((x_1 + x_2) \mod 2, (x_2 + x_3) \mod 2, \dots, (x_n + x_1) \mod 2),$$

which is clearly a linear map on $\mathbb{Z}_2^n$. The matrix representation of D in the standard basis is given by,

$$A = \begin{pmatrix} 1 & 1 & 0 & \dots & & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 \\ & & & \ddots & & \\ 0 & & \dots & 0 & 1 & 1 \\ 1 & 0 & & \dots & 0 & 1 \end{pmatrix} = I + S_L \tag{2}$$

where S_L is the left shift map on $\mathbb{Z}_2^n$. Using the formulation (2), Ehrlich proves that all vectors converge to the zero vector for $n = 2^k$. One simply expands $(I + S_L)^{2^k}$ using the binomial theorem. Since all the inner binomial coefficients are multiples of two,

$$(I + S_L)^{2^k} = I + S_L^n = I + I = 0.$$

Ehrlich attempted to find a formula for the maximal period length for odd n. He was unable to discover a concise general formula but he was able to prove some valuable divisibility relationships between vector length and the size of the maximal period. We will reprove his divisibility conditions by using the algebraic structure of the Ducci map on $\mathbb{Z}_2$. The following definitions will be used extensively in our analysis.

Definition 2.1: The *minimal annihilating polynomial* of a vector $\boldsymbol{v} \in \mathbb{Z}_2^n$ is the monic polynomial $\mu_v(\lambda)$ of least degree such that $\mu_v(A)\boldsymbol{v} = 0$.

The existence of such a polynomial is guaranteed by the Cayley-Hamilton theorem which states that the characteristic polynomial of A will annihilate A.

Definition 2.2: Suppose that $\mu_v(0) \neq 0$. Then the *order of* $\mu_v(\lambda)$, $\mathrm{ord}(\mu_v(\lambda))$, is defined to be the smallest natural number, c, such that $\mu_v(\lambda)|\lambda^c - 1$. If $\mu_v(0) = 0$, then $\mu_v(\lambda)$ can be written as $\lambda^k\tilde{\mu_v}(\lambda)$, for some positive integer k, where the polynomial, $\tilde{\mu_v}(\lambda)$, has the property, $\tilde{\mu_v}(0) \neq 0$. In this case, the order of $\mu_v(\lambda)$ is defined to be the order of $\tilde{\mu_v}(\lambda)$.

A characterization of period lengths by Richman for odd n based on orders of polynomials was quoted in [16]. To the best of our knowledge, the paper containing the proof of this result never appeared. We now provide a general characterization for any positive integer n, and any linear map. This result was initially proved in [25] to study a similar linear map on $\mathbb{Z}_2^n$.

Theorem 2.1: *Let $\boldsymbol{v} \in \mathbb{Z}_2^n$. Let $\mu_v(\lambda)$ be the minimal annihilating polynomial of $\boldsymbol{v}$. Assume that $\mu_v(\lambda) = \lambda^k\tilde{\mu_v}(\lambda)$ where $k \geq 0$ and $\tilde{\mu_v}(\lambda)$ is a monic polynomial with $\tilde{\mu_v}(0) \neq 0$. Then the k^{th} iterate of $\boldsymbol{v}$ belongs to a periodic cycle with period length $c = \mathrm{ord}(\mu_v)$.*

Proof: Let $A^j\boldsymbol{v}$ be the first iterate that belongs to the periodic cycle. Denote the length of the cycle by c. Then by definition of periodicity,

$$\begin{aligned}
&A^c(A^j\boldsymbol{v}) = A^j\boldsymbol{v}\\
\Rightarrow &A^c(A^j\boldsymbol{v}) - A^j\boldsymbol{v} = 0\\
\Rightarrow &A^j(A^c - I)\boldsymbol{v} = 0.
\end{aligned}$$

Therefore, the polynomial $p(\lambda) = \lambda^j(\lambda^c - 1)$ has the property that $p(A)\boldsymbol{v} = 0$. Since the minimal polynomial divides any other annihilating polynomial, it follows that

$$\mu_v(\lambda)|\lambda^j(\lambda^c - 1). \tag{3}$$

Using the assumption that $\mu_v(\lambda) = \lambda^k\tilde{\mu_v}(\lambda)$, yields that $\lambda^k|\lambda^j$ and $\tilde{\mu_v}(\lambda)|\lambda^c - 1$.

We will now show that $\mathrm{ord}(\tilde{\mu_v}(\lambda))$ must equal c. To see this, assume on the contrary that $\mathrm{ord}(\tilde{\mu_v}(\lambda)) = l$ for some natural number $l < c$. This means that $\tilde{\mu_v}(\lambda)|\lambda^l - 1$ which yields, $\lambda^k(\lambda^l - 1) = \mu_v(\lambda)q(\lambda)$ for some polynomial q. Therefore,

$$A^k(A^l - I)\boldsymbol{v} = \mu_v(A)q(A)\boldsymbol{v} = q(A)\mu_v(A)\boldsymbol{v} = 0.$$

It follows that $A^l(A^k\boldsymbol{v}) = A^k\boldsymbol{v}$ and so $A^k\boldsymbol{v}$ is in a periodic cycle of length l, giving a contradiction since the period of the cycle that $\boldsymbol{v}$ converges to is c. Thus, $c = \mathrm{ord}\mu_v(\lambda)$.

Next we will prove that $k = j$. Since $\lambda^k | \lambda^j$, $k \leq j$. We will show that k cannot be strictly less than j. To see this assume on the contrary that $k < j$. Now $\tilde{\mu_v}(\lambda) | \lambda^c - 1$ by the definition of order. Therefore, $\mu_v(\lambda) | \lambda^k(\lambda^c - 1)$ and so

$$\lambda^k(\lambda^c - 1) = \mu_v(\lambda)\bar{q}(\lambda),$$

for some polynomial, $\bar{q}(\lambda)$. From the definition of minimal annihilating polynomial,

$$A^k(A^c - 1)\boldsymbol{v} = \bar{q}(A)\mu_v(A)\boldsymbol{v} = 0.$$

Therefore, $A^c(A^k\boldsymbol{v}) = A^k\boldsymbol{v}$ and so $A^k\boldsymbol{v}$ is in the periodic cycle. But $A^j\boldsymbol{v}$ is the *first* iterate on the cycle. Hence our assumption that $k < j$ is false and k cannot be strictly less than j. This shows that k must equal j. □

Since there always exists a vector whose minimal annihilating polynomial is the minimal polynomial, the period of the maximal cycle is equal to the order of the minimal polynomial. Therefore, it will be useful to obtain the exact formulation of the minimal polynomial of A, $\mu_n(\lambda)$. We do so by first computing the characteristic polynomial of A.

The structure of the matrix $A - \lambda I$ provides some important observations:

$$A - \lambda I = \begin{pmatrix} 1-\lambda & 1 & 0 & \ldots & & 0 \\ 0 & 1-\lambda & 1 & 0 & \ldots & 0 \\ & & & \ddots & & \\ 0 & 0 & \ldots & 0 & 1-\lambda & 1 \\ 1 & 0 & & \ldots & 0 & 1-\lambda \end{pmatrix} \tag{4}$$

The $n-1^{\text{st}}$ minor determinant of $A-\lambda I$ is equal to one. Therefore, the characteristic polynomial is

$$p_n(\lambda) = (1 - \lambda)^n + 1.$$

A result in [13] states that $\mu_n(\lambda) = p_n(\lambda)\left[q_{n-1}(\lambda)\right]^{-1}$ where $q_{n-1}(\lambda)$ is the greatest common factor of the $n - 1$ rowed minor determinants of $A - \lambda I$. Since we already know that one of the $n - 1$ minor determinants is equal to one,

$$\mu_n(\lambda) = p_n(\lambda) = (1 - \lambda)^n + 1.$$

Since we are working over a field of characteristic 2, combining these observations with Theorem 2.1 yields the following corollary,

Corollary 2.2: *Let n be a positive integer. Then the period of the maximal cycle under A is equal to the order of the minimal polynomial of A,*

$$\mu_n(\lambda) = (1 + \lambda)^n + 1.$$

Moreover, for n odd, $\mu_n(\lambda) = \lambda\tilde{\mu_v}(\lambda)$ and so any v that converges to the maximal cycle does so in at most one iteration.

Define $c_1 = 2^j - 1$ where j is the order of 2 modulo n. If $n|2^l + 1$, for some l, then let $m = \min\{l : n|2^l + 1\}$ and define $c_2 = n(2^m - 1)$. Note that the existence of c_1 is always guaranteed by Euler's Theorem. Ehrlich proved that $c|c_1$ and $c|c_2$ if c_2 exists. We now provide alternate algebraic proofs of this divisibility condition. The structure of these arguments give insight into the connection between Ehrlich's results and the minimal polynomial of A.

Proposition 2.3: *Let c be the period length for the maximal cycle and define $c_1 = 2^j - 1$ where j is the order of 2 modulo n. For odd n, c divides c_1.*

Proof: Since the roots of the minimal polynomial, $\mu_n(\lambda)$ are simple, a result from [14] states that

$$c = \text{ord}(\mu_n(\lambda)) = \min\{s|z_i^s = 1\},$$

where z_i is a root of $\mu_n(\lambda)$. Now if z_i is a root of $\mu_n(\lambda)$ then

$$(1 + z_i)^n = 1.$$

Let $x_i = 1 + z_i$. Then $x_i^n = 1$ and $z_i = 1 + x_i$. Therefore, we seek,

$$\min_s (1 + x_i)^s = 1$$

where x_i is an n^{th} root of unity.

We will show that $(1 + x_i)^{c_1} = 1$ which will prove that $c|c_1$. To see this, observe that

$$\begin{aligned}(1 + x_i)^{c_1} &= (1 + x_i)^{2^j-1} \\ &= 1 + x_i + \ldots + x_i^{2^j-1} \\ &= \frac{1 + x_i^{2^j}}{1 + x_i}.\end{aligned}$$

We know $x_i^{2^j-1} = 1$, since $n|2^j - 1$. Therefore, $x_i^{2^j} = x_i$ and so

$$\frac{1 + x_i^{2^j}}{1 + x_i} = 1. \quad \square$$

Proposition 2.4: *Let n be odd and suppose that $n|2^l+1$, for some l. Let $m = \min\{l : n|2^l+1\}$ and define $c_2 = n(2^m - 1)$. If c is the length of the maximal cycle, then $c|c_2$.*

Proof: Similar to Proposition 2.3, we compute $(1 + x_i)^{c_2}$,

$$\begin{aligned}(1 + x_i)^{c_2} &= \left[(1 + x_i)^{2^m-1}\right]^n \\ &= \left[1 + x_i + \ldots + x_i^{2^m-1}\right]^n \\ &= \left[\frac{1 + x_i^{2^m}}{1 + x_i}\right]^n\end{aligned}$$

Since $x_i^{2^m+1} = 1$, $x_i^{2^m} = x_i^{-1}$ so

$$\left[\frac{1+x_i^{2^m}}{1+x_i}\right]^n = x_i^{-n}\left[\frac{x_i+1}{1+x_i}\right]^n = 1.$$

This proves $c|c_2$. □

The next lemma relates c_2 to c_1 when c_2 exists.

Proposition 2.5: *Let n be odd and suppose that c_2 exists. Then $c_2|c_1$.*

Proof: We will first show that $j = 2m$. Since $2^m \equiv -1 \pmod{n}$, $2^{2m} \equiv 1 \pmod{n}$, which implies that $j \leq 2m$. Now, if $j < m$, then $2^{m-j} \equiv -1 \pmod{n}$, contradicting the minimality of m. Moreover, by definition, $m \neq j$, and if $m < j < 2m$, then $2^{j-m} \equiv -1 \pmod{n}$, again contradicting the minimality of m. Hence $j = 2m$ as claimed.

It follows that, $c_1 = (2^m+1)(2^m-1)$ is divisible by c_2. □

Ehrlich provided four examples to show that c does not necessarily have to equal c_1 or c_2, namely $n = 37, 95, 101$ and 111. Obviously, the maximal period in these cases was a proper common divisor of c_1 and c_2 and is also a multiple of n.

The next section provides data for cycles of the Ducci map up to $n = 40$, obtained using Theorem 2.1.

3. PERIODS OF THE n-NUMBER DUCCI GAME

In addition to cycles with the maximal period c, there can exist cycles with shorter periods that are proper divisors of c. If $g(\lambda)$ is a proper divisor of $\tilde{\mu}(\lambda)$, then there exists a vector with $g(\lambda)$ as its minimal annihilating polynomial. As Theorem 2.1 states, the vector is in a cycle with period equal to the order of $g(\lambda)$. In fact, all possible periods can be obtained by examining $\tilde{\mu}$ and all of its divisors.

For example, for $n = 17$, $\tilde{\mu}(\lambda) = g_1(\lambda)g_2(\lambda)$ where,

$$g_1(\lambda) = \lambda^8 + \lambda^7 + \lambda^5 + \lambda^4 + \lambda^3 + \lambda^2 + 1$$

and

$$g_2(\lambda) = \lambda^8 + \lambda^5 + \lambda^3 + \lambda^2 + 1.$$

The order of g_1 is 85 and the order of g_2 is 255. Although the majority of cycles are of length 255, there do exist three cycles of length 85. The algorithm to obtain the complete cyclic structure (state diagram) for a linear map on $\mathbb{Z}_p^n$ based on this approach is given in [25].

The output of this procedure applied to the Ducci map for vector lengths up to $n = 40$ are provided in Table 1. In addition to the information in Table 1, the program also generates the number of vectors in each cycle, the maximum number of iterations needed to arrive in the cycle, and the irreducible factors of the minimal polynomial. We note that fixed points are considered a cycle of length one.

Many interesting questions remain on the Ducci map. For example, is there a way to predict when $c = c_1$ or c_2? If so, is there a method of determining the period for the cases when $c \neq c_1, c_2$? The even case has been looked at but not as extensively as the odd case. Are there similar divisibility conditions connected to the minimal polynomial in the even case? We believe that the algebraic structure may provide some answers to these questions.

Vector Length	Number of Cycles of Different Lengths	Cycle Lengths	Vector Length	Number of Cycles of Different Lengths	Cycle Lengths
n=3	2	1,3	n=22	3	1,341,682
n=4	1	1	n=23	2	1,2047
n=5	2	1,15	n=24	5	1,3,6,12,24
n=6	3	1,3,6	n=25	3	1,15,25575
n=7	2	1,7	n=26	3	1,819,1638
n=8	1	1	n=27	4	1,3,63,13797
n=9	3	1,3,63	n=28	4	1,7,14,28
n=10	3	1,15,30	n=29	2	1,475107
n=11	2	1,341	n=30	7	1,3,5,6,10,15,30
n=12	4	1,3,6,12	n=31	2	1,31
n=13	2	1,819	n=32	1	1
n=14	3	1,7,14	n=33	4	1,3,341,1023
n=15	4	1,3,5,15	n=34	5	1,85,170,255,510
n=16	1	1	n=35	6	1,7,15,105,819,4095
n=17	3	1,85,255	n=36	7	1,3,6,12,63,126,252
n=18	5	1,3,6,63,126	n=37	2	1,3233097
n=19	2	1,9709	n=38	3	1,9709,19418
n=20	4	1,15,30,60	n=39	6	1,3,455,819,1365,4095
n=21	5	1,3,7,21,63	n=40	5	1,15,30,60,120

Table 1. Period lengths under iterations of the Ducci map.

ACKNOWLEDGMENTS

The authors would like to thank Marc Chamberland for generating interest in the problem and providing us with literature.

REFERENCES

[1] O. Andriychenko and M. Chamberland. “Iterated Strings and Cellular Automata.” *Mathematical Intelligencer* **22.4** (2000): 33-36.

[2] F. Breuer. “A Note on a Paper by Glaser and Schöff.” *Fibonacci Quarterly* **36.5** (1998): 463-466.

[3] M. Burmester, R. Forcade and E. Jacobs. “Circles of Numbers.” *Glasgow Math. J.* **19** (1978): 115-19.

[4] L. Carlitz and R. Scoville. In “Solutions.” *SIAM Review* **12** (1970): 247-300.

[5] M. Chamberland. “Unbounded Ducci Sequences.” *Journal of Difference Equations* , to appear.

[6] C. Ciamberlini and A. Marengoni. “Su una interessante curiosit.” *it à numerica Periodiche di Matematiche* **17** (1937): 25-30.

[7] J. Creely. “The Length of a Three-Number Game.” *Fibonacci Quarterly* **26** (1988): 141-143.

[8] A. Ehrlich. "Periods in Ducci's n-Number Game of Differences." *Fibonacci Quarterly* **28** (1990): 302-305.

[9] B. Freedman. "The Four Number Game." *Scripta Math* **14** (1948): 35-47.

[10] H. Glaser and G. Schöffl. "Ducci-Sequences and Pascal's Triangle." *Fibonacci Quarterly* **33** (1995): 313-324.

[11] J.M. Hammersley. In "Problems." *SIAM Review* **11** (1969): 73-74.

[12] R. Honsberger. *Ingenuity in Mathematics*, Yale University, (1970).

[13] N. Jacobson. *Lectures in Abstract Algebra, VII*, (1953).

[14] R. Lidl and H. Niederreiter. *Finite Fields*, Encyclopedia of Mathematics and its Applications, **20** (1983).

[15] M. Lotan. "A Problem in Difference Sets." *American Mathematical Monthly* **56** (1949): 535-541.

[16] A. Ludington Furno. "Cycles of Differences of Integers." *Journal of Number Theory* **13** (1981): 255-261.

[17] A. Ludington. "Length of the 7-Number Game." *Fibonacci Quarterly* **26** (1988): 195-204.

[18] A. Ludington-Young. "Length of the n-Number Game." *Fibonacci Quarterly* **28** (1990): 259-265.

[19] A. Ludington-Young. "Ducci-Processes of 5-tuples." *Fibonacci Quarterly* **36.5** (1998): 419-434.

[20] A. Ludington-Young. "Even Ducci-Sequences." *Fibonacci Quarterly* **37.2** (1999): 145-153.

[21] K.R. McLean. "Playing Diffy With Real Sequences." *Mathematical Gazette* **83** (1999): 58-68.

[22] R. Miller. "A Game With n Numbers." *American Mathematical Monthly* **85** (1978): 183-185.

[23] F. Pompili. "Evolution of Finite Sequences of Integers ...." *Mathematical Gazette* **80** (1996): 322-332.

[24] I.R. Sprague. *Recreation in Mathematics*, Dover, (1963).

[25] J.G. Stevens. "On the Construction of State Diagrams for Cellular Automata With Additive Rules." *Information Sciences* **115** (1999): 43-59.

[26] B. Thwaites. "Two Conjectures or How to Win £1100." *Mathematical Gazette* **80** (1996): 35-36.

[27] W. Webb. "The Length of the Four-Number Game." *Fibonacci Quarterly* **20** (1982): 33-35.

[28] F.-B. Wong. "Ducci Processes." *Fibonacci Quarterly* **20** (1982): 97-105.

[29] P. Zvengrowski. "Iterated Absolute Differences." *Mathematics Magazine* **52.1** (1979): 36-37.

AMS Classification Numbers: 11T99, 12E20, 39A11

✠ ✠ ✠