PERIODS IN DUCCI'S n-NUMBER GAME OF DIFFERENCES

Amos Ehrlich
Tel-Aviv University, Tel-Aviv, Israel

(Submitted September 1988)

1. Introduction

Let $A = (a_1, a_2, \ldots, a_n)$ be an n-tuple of nonnegative integers, and define

$$D(A) = (|a_1 - a_2|, |a_2 - a_3|, \ldots, |a_{n-1} - a_n|, |a_n - a_1|).$$

Note that in the definition of D the n-tuple A is regarded as written in a circle, so Ludington's title "Cycles of Differences" [3] is more suggestive than my "Columns of Differences" [1].

Sequences of the form A, $D(A)$, $D^2(A)$, $D^3(A)$, ... are called Ducci sequences here (see [5] and [7]). Some authors call them n-number games.

Since applying D does not increase the maximum of the components of a tuple it follows that in a Ducci sequence there are just a finite number of different tuples. Let $D^s(A)$ be the first tuple which is equal to a previous tuple $D^r(A)$, then the tuples $D^r(A)$, $D^{r+1}(A)$, ..., $D^{s-1}(A)$ form a repeating cycle. The length of this cycle, $s - r$, is called the period of the sequence. If R and S are any two natural numbers such that $D^R(A) = D^S(A)$, then $s - r | S - R$.

This article deals mainly with the periods of Ducci sequences. (Authors who deal with the length of the part that precedes the cycle refer to that length as the length of the game.)

2. Maximal Periods

The components of every tuple in the periodic part of a Ducci sequence are all equal to either 0 or a constant C which depends on the first tuple of the sequence (see [1], Th. 1 in [2], Lem. 3 in [3], item I in [7]). Since for every positive λ, $D(\lambda A) = \lambda D(A)$, one may assume without loss of generality that $C = 1$. In other words, let us restrict our attention to n-tuples with components from $\{0, 1\}$. In particular, the Ducci sequence that starts with the n-tuple $(0, \ldots, 0, 1)$ will be called a *basic* Ducci sequence, and the length of its period is denoted $P(n)$.

Let $H(a_1, a_2, \ldots, a_n) = (a_2, \ldots, a_n, a_1)$, then H is a linear transformation over Z_2. Since $|x - y| \equiv x + y \pmod 2$, it follows that $D = I + H$, and D is also a linear transformation over Z_2^n.

Theorem 1: For any n, the maximal period of Ducci's sequence of n-tuples is $P(n)$. Periods of other sequences divide this maximum.

If $D^R(A) = D^S(A)$ holds for $A = (0, 0, 0, \ldots, 0, 1)$, it holds also for $A = (0, 0, \ldots, 0, 1, 0)$, for $A = (0, \ldots, 0, 1, 0, 0)$, etc. This follows from the cyclic character of D (or, alternatively, from the commutativity of D with H). Since D is linear, it holds also for sums of these A's. □

3. Upper Bounds for $P(n)$

Lemma 1: If $2^m \equiv t \pmod n$, then $D^{(2^m)} = I + H^t$.

Proof: By Induction on m, $(I + H)^{(2^m)} = I + H^{(2^m)}$. $H^{(2^m)} = H^t$ since, by the definition of H, $H^n = I$. □

Note that Lemma 1 suggests an effective way to compute $D^r(A)$ for big r's: Write r as $\Sigma 2^{m_1}$, then compute $(\Pi(I + H^{t_1}))(A)$.

Corollalry 1: If n is a power of 2, then the cycle of Ducci's sequences consists of a single n-tuple $(0, 0, \ldots, 0)$.

Proof: In this case, $D^n = I + H^0 = I + I = 0$. □

Corollary 2: If n is not a power of 2, then the cycle of the basic Ducci sequence contains an n-tuple with exactly two 1's.

Proof: Take any m which is big enough to assure that $D^{(2^m)}(0, 0, \ldots, 0, 1)$ is in the periodic part of the sequence. Reducing 2^m modulo n gives a $t \neq 0$. $H^t(0, 0, \ldots, 0, 1)$ has exactly one 1, but it is not $(0, 0, \ldots, 0, 1)$. Thus, the result follows from Lemma 1. □

Corollary 3: If $2^m \equiv 1 \pmod{n}$ then $P(n)$ divides $2^m - 1$.

Proof: In this case $D^{(2^m)} = I + H^1 = D^1$. □

Remark: Both Corollaries 1 and 3 are not new. Corollary 1 is item D_1 in [7] and appears in at least 19 of the 22 articles referred to there, sometimes only for $n = 4$. The present proof is considerably shorter than the ones in [7] and in [6]. Corollary 3 is written without proof in [1] and is the "further" part of Theorem 3 in [3], restricted to odd n's.

Theorem 2: If $2^M \equiv -1 \pmod{n}$, then $P(n)$ divides $n(2^M - 1)$.

Proof: $D^{(2^M)} = I + H^{-1} = H^{-1}(H + I) = H^{-1}D$; hence, $D^{(n2^M)} = H^{-n}D^n = D^n$. □

Let us use the following abbreviations:

a. For an odd $n > 1$, let $m(n)$ be the smallest $m > 0$ such that $2^m \equiv 1 \pmod{n}$. [By Euler's theorem, such an m does exist and $m(n) | \phi(n)$.]
b. If for an odd $n > 1$ there is an M such that $2^M \equiv -1 \pmod{n}$, then n will be said to be "with a -1." When this occurs, the smallest such M is $m(n)/2$. If this does not occur, then we say that n is "without a -1."

Facts:

For every odd n with a -1, from 3 to 163 except for 37 and 101,

$$P(n) = n(2^{m(n)/2} - 1).$$

For every odd n without a -1, from 7 to 165 except for 95 and 111,

$$P(n) = 2^{m(n)} - 1.$$

For all of the four exceptions, $P(n)$ is 1/3 of the "expected" value. I do not know whether any deeper thing is hidden behind this divisor 3.

These data were computed in the following way. Since for every odd n there is an m such that $2^m \equiv 1 \pmod{n}$, and since $(0, \ldots, 0, 1, 1) = D(0, \ldots, 0, 1)$, it follows from the proof of Corollary 3 that, for such an n, $(0, \ldots, 0, 1, 1)$ is in the periodic part of the basic Ducci sequence. The note just after Lemma 1 gives a fast way for checking whether $D^r(0, \ldots, 0, 1, 1) = (0, \ldots, 0, 1, 1)$. By Corollary 3 and Theorem 2, one has to check only r's which divide $2 \quad - 1$, and in many cases only the divisors of $n(2^{m(n)/2} - 1)$.

As an example, let us see how $P(37)$ is found. 18 is the smallest M such that $2^M \equiv -1 \pmod{37}$. [In other words, 37 is with a -1 and $m(37) = 36$.] By Theorem 2,

$$P(37) | 37 \cdot (2^{18} - 1) = 9699291. \quad 9699291 = 3 \cdot 3 \cdot 3 \cdot 7 \cdot 19 \cdot 37 \cdot 73.$$

A subroutine based on Lemma 1 is now called, and outputs $D^r(0, \ldots, 0, 1, 1)$ for $r = 9699291/3$, $9699291/7$, $9699291/19$, $9699291/37$, and $9699291/73$. The first of these r's returns $(0, \ldots, 0, 1, 1)$, while the other ones do not. Running this subroutine for $r = 9699291/9$ does not return $(0, \ldots, 0, 1, 1)$

either; hence,

$$P(37) = 9699291/3 = 3233097.$$

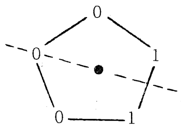
Remark: The D^r subroutine is quite fast. The reason for stopping the calculations at $P(165)$ was the time needed for the factoring. I thank Yehuda Kats of Levinsky College for Teachers, Tel-Aviv, for factoring the numbers that were needed in calculating $P(131)$, $P(139)$, and $P(149)$.

4. More Properties of $P(n)$

Having seen that $P(n)$ may be a proper divisor of $2^{m(n)} - 1$ or of $n(2^{m(n)/2} - 1)$ there is an interest in the following theorem.

Theorem 3: If n is not a power of 2, then $n|P(n)$.

Proof: Write the components of an $A \in Z_2^n$ on the vertices of a regular n-gon in a counterclockwise order, starting, say, at the highest vertex. For example, write (0, 0, 0, 1, 1) as follows:



If A has an axis of symmetry, then $D(A)$ also does, and its axis is obtained from that of A by a rotation of $-180/n$ degrees. [It is the bisector of the axis of A and the axis of $H(A)$.] If A has more than one axis, then each of the axes is transferred to the followers of A in the same way.

By Corollary 2, there is an n-tuple with exactly two 1's in the cycle of the basic Ducci sequence. Since this n-tuple has just one axis of symmetry, so do all of the tuples in the repeating cycle. During one cycle, the axis rotates a whole multiple of 180 degrees, so the period is a multiple of n. □

In the proofs of the following theorems, I am going to cut a tuple into equal parts and write these parts one below the other in the form of a matrix. These matrices are not intended to represent linear transformations. They are just another way to write the tuples, and you may read them the same way you read an English text of more than one line. For example, for

$$A = (a, b, c, d, e, f, g, h, i, j, k, l),$$

$$H(A) = H\begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \end{bmatrix} = \begin{bmatrix} b & c & d & e \\ f & g & h & i \\ j & k & l & a \end{bmatrix}.$$

On the other hand, if the dimensions of the matrix form of A are given, then each row and each column of A are well defined tuples on their own, and our transformations H and D may apply to each of them. Let us define $H_L(A)$ to be the matrix obtained from A by replacing each row by H(that row), and define $D_L(A)$, $H_C(A)$, and $D_C(A)$ in similar ways, with "D" instead of "H" or with "column" instead of "row." Following our last example,

$$H_L(A) = \begin{bmatrix} b & c & d & a \\ f & g & h & e \\ j & k & l & i \end{bmatrix} \quad H_C(A) = \begin{bmatrix} e & f & g & h \\ i & j & k & l \\ a & b & c & d \end{bmatrix}.$$

Theorem 4: If $n = 2^m k$, where k is an odd number, then $P(n) = 2^m P(k)$.

Let us write each n-tuple A as a $k \times 2^m$ matrix. Since each row of A is, now, of 2^m components, $H^{(2^m)}(A) = H_C(A)$. By Lemma 1, this holds for D's too.

To find $P(n)$, it is sufficient to inspect just every 2^mth element of the basic Ducci sequence since, by Theorem 3, $2^m|P(n)$. If we start our inspections with the first element of the entire sequence, i.e., with the n-tuple whose matrix is

$$\begin{bmatrix} 0, & \dots, & 0, & 0 \\ \vdots & & & \\ 0, & \dots, & 0, & 0 \\ 0, & \dots, & 0, & 1 \end{bmatrix}$$

then the right column of the inspected elements forms a basic Ducci sequence of k-tuples, and the other columns are 0's (since $D^{(2^m)} = D_C$). The period of the inspected subsequence is, thus, $P(k)$, and the period of the entire sequence is $2^m P(k)$. □

Theorem 5: If $k|n$, then $P(k)|P(n)$.

Proof: By Theorem 1, it is sufficient to find an n-tuple whose Ducci sequence has $P(k)$ for its period. We are going to see that the $n/k \times k$ matrix

$$\begin{bmatrix} 0, & \dots, & 0, & 1 \\ \vdots & & & \\ 0, & \dots, & 0, & 1 \end{bmatrix}$$

will do.

Indeed, if all of the rows of a matrix A are equal to each other, then $H(A) = H_L(A)$; hence, $D(A) = D_L(A)$. It follows that the Ducci sequence of n-tuples which starts with the above mentioned matrix, behaves like the basic Ducci sequence of k-tuples. □

References

1. A. Ehrlich. "Columns of Differences." *Maths Teaching* (1977):42-45.
2. M. Brumeister, R. Forcade, & E. Jacobs. "Circles of Numbers." *Glasgow Math J. 19* (1978):115-19.
3. A. L. Ludington. "Cycles of Differences of Integers." *J. Number Theory 13* (1981):255-61.
4. W. Webb. "The Length of the Four-Number Game." *Fibonacci Quarterly 20* (1982):33-35.
5. F. Wong. "Ducci Processes." *Fibonacci Quarterly 20* (1982):97-105.
6. R. Miller. "A Game with n Numbers." *Amer. Math. Monthly 85* (1978):183-85.
7. L. Meyers. "Ducci's Four-Number Problem: A Short Bibliography." *Crux Mathematicorum 8* (1982):262-66.
8. K. D. Boklan. "The n-Number Game." *Fibonacci Quarterly 22* (1984):152-55.
9. J. W. Creely. "The Length of the Three Number Game." *Fibonacci Quarterly 26* (1988):141-43.
10. A. L. Ludington. "Length of the 7-Number Game." *Fibonacci Quarterly 26* (1988):195-204.

*****