THE NUMBER OF DUCCI SEQUENCES WITH GIVEN PERIOD

Ron Brown

Department of Mathematics, 2565 McCarthy Mall, University of Hawaii, Honolulu, HI 96822, USA
e-mail: ron@math.hawaii.edu

Jonathan L. Merzel

Soka University of America, 1 University Drive, Aliso Viejo, CA 92656, USA
e-mail: jmerzel@soka.edu

(Submitted July 2005-Final Revision December 2005)

ABSTRACT

The exact number of periodic Ducci sequences of vectors with arbitrary dimension but with specified period is computed, assuming natural identifications of certain sequences having the same behavior. A duality theory is developed which shows that this computation is equivalent to a result of A. Ludington Young on the number of periodic Ducci sequences of specified dimension but arbitrary period.

1. THE MAIN THEOREM

For any integer $n > 0$ define $T = T_n : \mathbb{R}^n \to \mathbb{R}^n$ by the rule

$$T((a_i)_{0\le i<n}) = (|\, a_i - a_{(i+1)\bmod n}|)_{0\le i<n}$$

where for any $s \in \mathbb{Z}$ we let $s \bmod n$ denote the remainder when s is divided by n (so that $0 \le s \bmod n < n$). If $v \in \mathbb{R}^n$ then the sequence $(T^i(v))_{i\ge 0}$ is called an *n–number game* [4, p. 259] or *Ducci sequence* [5, p. 145], or *Diffy game* [6]. We say that a Ducci sequence $(T^i(v))_{i\ge 0}$ has *period* $k > 0$ (and that the vector v has *Ducci period* k) if $T^k(v) = v$. Two basic themes in the study of Ducci sequences are the behavior of the periodic ones and the convergence of arbitrary ones to periodic ones (e.g., see [2, 4, 7]). In this paper we count, after making some natural identifications, the exact number of Ducci sequences with a specified period k.

We now make some standard reductions in the study of periodic Ducci sequences. It is well–known that if $a \in \mathbb{R}^n$ has some Ducci period, then $a \in \{0,\gamma\}^n$ for some positive $\gamma \in \mathbb{R}$ (e.g., see [1, Claim 2, p. 48] or [3, Lemma 3, p. 256]). Since $T^i(\gamma^{-1}a) = \gamma^{-1}T^i(a)$ for all $i \ge 0$, we may as well assume that $\gamma = 1$ and that $a \in \{0,1\}^n$. Moreover since $|e-f| = (e+f) \bmod 2$ for all $e, f \in \{0,1\}$, we may identify $\{0,1\}$ with $\mathbb{Z}_2$ and regard T_n as the linear map $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$ with $T_n((a_i)_{0\le i<n}) = (a_i + a_{(i+1)\bmod n})_{0\le i<n}$.

It is natural to identify a vector such as $v = (0,1,1)$ with its iterates, say for example $w = (0,1,1,0,1,1,0,1,1)$, since both give rise to Ducci sequences with the same behavior. (For each $i \ge 0$, $T_9^i(w)$ is obtained by iterating the coordinates of $T_3^i(v)$.)

Definition 1: Call vectors $a = (a_i)_{0\le i<m} \in \mathbb{Z}_2^m$ and $b = (b_i)_{0\le i<n} \in \mathbb{Z}_2^n$ *similar* if $a_{i\bmod m} = b_{i\bmod n}$ for all $i \in \mathbb{Z}$.

Similarity is clearly an equivalence relation on $\bigcup_{n>0} \mathbb{Z}_2^n$. We will see in Lemma 1 below that vectors a and b as above are similar if and only if we have

$$a = (a_0, \dots, a_{r-1}, a_0, \dots, a_{r-1}, \dots, a_0, \dots, a_{r-1}) \in \mathbb{Z}_2^m$$

and

$$b = (a_0, \ldots, a_{r-1}, a_0, \ldots, a_{r-1}, \ldots, a_0, \ldots, a_{r-1}) \in \mathbb{Z}_2^n$$

where $r = (m, n)$ is the greatest common divisor of m and n. It follows easily that if a and b are similar, then their Ducci sequences have essentially the same behavior; in particular, one has Ducci period k if and only if the other does also (see Lemma 2).

Let us now fix a positive integer k; we let 2_k denote the largest power of 2 dividing k.

Main Theorem: *The number of similarity classes of vectors in* $\bigcup_{n>0} \mathbb{Z}_2^n$ *with Ducci period* k *is* 2^{k-2_k}.

The proof of the above theorem in §2 will give a simple method of listing all the similarity classes of vectors in $\bigcup_{n>0} \mathbb{Z}_2^n$ with Ducci period k.

If $k > 0$ is least such that $v \in \bigcup_{n>0} \mathbb{Z}_2^n$ has Ducci period k, then we say that v has *minimal Ducci period* k and the Ducci sequence $(T^i(v))_{i\geq 0}$ has *minimal period* k. In §3 we will show how to compute the number of similarity classes of vectors with minimal Ducci period k.

In §4 we will develop a duality between the vectors in $\mathbb{Z}_2^n$ of Ducci period k and the vectors in $\mathbb{Z}_2^k$ of Ducci period n. This duality will show that the main theorem above is equivalent to the following observation of A. Ludington Young.

Young's Theorem: [3, p. 260, last paragraph]. *There are exactly* 2^{n-2_n} *vectors in* $\mathbb{Z}_2^n$ *with a finite Ducci period.*

The duality plus Young's Theorem yield together a second proof of the Main Theorem. In §4 we will also sketch a quick proof of Young's Theorem using linear algebra.

2. COUNTING SIMILARITY CLASSES

For each $a = (a_i)_{0\leq i<m} \in \mathbb{Z}_2^m$ let $\theta_m(a)$ denote the doubly infinite sequence $(a_{i \bmod m})_{i\in\mathbb{Z}} \in \mathbb{Z}_2^{\mathbb{Z}}$, i.e., the map $\mathbb{Z} \to \mathbb{Z}_2$ taking each $i \in \mathbb{Z}$ to $a_{i \bmod m}$. One might, for example, visualize $\theta_3((0,0,1))$ as the doubly infinite tuple $(\cdots 0,0,1,0,0,1,0,0,1 \cdots)$, although this notation does not clearly indicate the value of the doubly infinite sequence at any particular integer.

Lemma 1: *Let* $a = (a_i)_{0\leq i<m} \in \mathbb{Z}_2^m$ *and* $b = (b_i)_{0\leq i<n} \in \mathbb{Z}_2^n$; *set* $r = (m, n)$. *The following are equivalent:*

(i) a *and* b *are similar;*

(ii) $\theta_m(a) = \theta_n(b)$;

(iii) $b_{i \bmod n} = b_{i \bmod r} = a_{i \bmod r} = a_{i \bmod m}$ *for all* $i \in \mathbb{Z}$.

Proof: We prove (i) $\Rightarrow$ (iii) (that (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) is trivial). Assume that a and b are similar. Write $r = sm + tn$ and $i = rq + (i \bmod r)$ where $s, t, q \in \mathbb{Z}$. Then

$$\begin{aligned} a_{i \bmod m} &= b_{i \bmod n} = b_{(smq + i \bmod r) \bmod n} \\ &= a_{(i \bmod r) \bmod m} = a_{i \bmod r} = b_{i \bmod r} \end{aligned}$$

since $0 \leq i \bmod r < \min\{n, m\}$. □

The interpretation of similarity given after Definition 1 follows from the above lemma. The next lemma will show that similar vectors have the same Ducci period (if either has a finite Ducci period).

Note that the image of each of the maps $\theta_n : \mathbb{Z}_2^n \to \mathbb{Z}_2^{\mathbb{Z}}$ is the set of doubly infinite sequences $(c_i)_{i\in\mathbb{Z}}$ with *block length* n, i.e., with $c_{i+n} = c_i$ for all $i \in \mathbb{Z}$. (We use the term "block length" instead of "period" to avoid confusion with Ducci periods.)

Let $T : \mathbb{Z}_2^{\mathbb{Z}} \to \mathbb{Z}_2^{\mathbb{Z}}$ be the map taking each doubly infinite sequence $a = (a_i)_{i\in\mathbb{Z}} \in \mathbb{Z}_2^{\mathbb{Z}}$ to $(a_i + a_{i+1})_{i\in\mathbb{Z}}$. We say a has *Ducci period* k if $T^k(a) = a$.

Lemma 2: *Suppose $a \in \mathbb{Z}_2^m$ and $b \in \mathbb{Z}_2^n$ are similar. If one of a, b, $\theta_m(a)$ or $\theta_n(b)$ has Ducci period k, then they all have Ducci period k.*

Proof: The lemma follows from the fact that $\theta_m(a) = \theta_n(b)$ (Lemma 1) and the fact that for all $i \geq 0$,

$$T^i(\theta_m(a)) = \theta_m(T_m^i(a)). \tag{1}$$

(Note that formula (1) follows from the easy case where $i = 1$.) □

We now prove the Main Theorem. The above lemmas show that the set of similarity classes of vectors in $\bigcup_{n>0} \mathbb{Z}_2^n$ with period k is bijective with the set $\mathcal{D}$ of doubly infinite sequences in $\mathbb{Z}_2^{\mathbb{Z}}$ which have a finite block length and Ducci period k. It therefore suffices to show that the projection map $\pi : \mathbb{Z}_2^{\mathbb{Z}} \to \mathbb{Z}_2^{k-2_k}$ taking each $(a_i)_{i\in\mathbb{Z}}$ to $(a_i)_{0\leq i<k-2_k}$ carries $\mathcal{D}$ bijectively onto $\mathbb{Z}_2^{k-2_k}$.

Let I and S denote the identity and shift operators on $\mathbb{Z}_2^{\mathbb{Z}}$, so $S((a_i)_{i\in\mathbb{Z}}) = (a_{i+1})_{i\in\mathbb{Z}}$. Then $T = S + I$ and hence for any $t \geq 0$ and $a = (a_i)_{i\in\mathbb{Z}} \in \mathbb{Z}_2^{\mathbb{Z}}$ we have

$$T^t(a) = \sum_{j=0}^{t} \binom{t}{j} S^j(a) = \left(\sum_{j=0}^{t} \binom{t}{j} a_{i+j} \right)_{i\in\mathbb{Z}}. \tag{2}$$

Suppose $1 \leq j < 2_k$; set $t = j/2_j$, so t is odd and $2_j < 2_k$. Hence $t\binom{k}{j} = \frac{k}{2_j}\binom{k-1}{j-1}$ is even, so $\binom{k}{j}$ is even. On the other hand $\binom{k}{2_k}$ is odd [9, Lemma 4.16, p. 80]. Thus $a = (a_i)_{i\in\mathbb{Z}} \in \mathbb{Z}_2^{\mathbb{Z}}$ has Ducci period k if and only if for all $i \in \mathbb{Z}$

$$a_i = \sum_{j=0}^{k} \binom{k}{j} a_{i+j} = a_i + a_{i+2_k} + \sum_{j=2_k+1}^{k} \binom{k}{j} a_{i+j}$$

or, equivalently,

$$0 = a_{i+2_k} \; + \sum_{2_k<j<k} \binom{k}{j} a_{i+j} \; + \; a_{k+i}. \tag{3}$$

Equation (3) can be reindexed to say that for all $i \in \mathbb{Z}$,

$$a_i = \sum_{j=1}^{k-2_k} \binom{k}{k-j} a_{i-j} = \sum_{j=1}^{k-2_k} \binom{k}{j+2_k} a_{i+j}, \tag{4}$$

which expresses each a_i in terms of the preceding or succeeding a_j's.

Now suppose $a = (a_i)_{0\leq i<k-2_k} \in \mathbb{Z}_2^{k-2_k}$. It suffices to show that there is a unique $a' \in \mathcal{D}$ with Ducci period k which under the projection π maps to a. If we define $a' = (a_i)_{i\in\mathbb{Z}}$ by the (forwards and backwards) recursion relations (4), then a' will satisfy the equations (3) for all $i \in \mathbb{Z}$ and hence a' will have Ducci period k; indeed it is the only element of $\mathbb{Z}_2^{\mathbb{Z}}$ which π maps to a having Ducci period k. It remains to show that a' has a finite block length. Since $\mathbb{Z}_2^{k-2_k}$ is finite, for some integers $u > v > 0$ we must have $(a_{u+1}, \cdots, a_{u+k-2_k}) = (a_{v+1}, \cdots, a_{v+k-2_k})$.

But then the recursion relations (4) show that $a_{u+i} = a_{v+i}$ for all $i \in \mathbb{Z}$, and hence that $a' = (a_i)_{i\in\mathbb{Z}}$ has block length $u - v$. This completes the proof of the Main Theorem. □

Note: The above argument shows that any nonzero vector in $\mathbb{Z}_2^n$ with Ducci period k is similar to one in $\mathbb{Z}_2^m$ for some $m \leq 2^{k-2_k}-1$. For example any vector in $\bigcup_{n>0}\mathbb{Z}_2^n$ with Ducci period 5 is similar to one in $\mathbb{Z}_2^m$ for some $m \leq 2^4-1 = 15$. Actually one can say more than this. A nonzero vector of Ducci period 5 has minimal Ducci period 5 and by Proposition 1 below there are exactly 15 similarity classes of such vectors. These similarily classes therefore must be exactly the similarity classes of the 15 shifts of the vector $w = (1,0,1,0,1,1,0,0,1,0,0,0,1,1,1) \in \mathbb{Z}_2^{15}$ of minimal Ducci period 5.

3. MINIMAL DUCCI PERIODS

Let μ denote the usual Moebius function and let k denote a positive integer. The Main Theorem above together with the Moebius inversion formula [8, Theorem 4.7, p. 111] give a formula for the number $N(k)$ of similarity classes of vectors with minimal Ducci period k.

Proposition 1: $N(k) = \sum_{d|k}\mu(k/d)2^{d-2_d}$.

For example if k is divisible by exactly one prime p, then the proposition says that $N(k) = 2^{k-2_k} - 2^{k/p-2_{k/p}}$. Similarly, if k has exactly two distinct prime factors p and q, then

$$N(k) = 2^{k-2_k} - 2^{k/p-2_{k/p}} - 2^{k/q-2_{k/q}} + 2^{k/pq-2_{k/pq}}.$$

When k has three or more distinct prime factors, then the summation in Proposition 1 is more complicated. The next proposition shows that in this case a truncation of the sum in Proposition 1 to just two terms gives a surprisingly good relative approximation to $N(k)$.

Proposition 2: *Let $N_0(k) = 2^{k-2_k} - 2^{k/p-2_{k/p}}$ where p is the smallest prime dividing k. Suppose that k has at least 3 distinct prime factors. If k is odd, then*

$$0 \leq 1 - \frac{N(k)}{N_0(k)} \leq \frac{1}{2^{10}-1}\frac{1}{2^{70}-1}$$

and if k is even, then

$$0 \leq 1 - \frac{N(k)}{N_0(k)} \leq \frac{16}{15}\frac{2^{14}}{2^{14}-1}\frac{1}{2^{20}}.$$

Proof: Let $p(0) < \cdots < p(r)$ be the distinct *odd* prime divisors of k, so $r \geq 1$ and if k is odd, then $r \geq 2$. Let $B = 5$ and $\delta = 0$ if $p \neq 2$ and let $B = 2$ and $\delta = 1$ if $p = 2$. Since odd primes always differ by at least 2,

$$\frac{k}{p(0)} - \frac{k}{p(i)} = \frac{k}{p(0)p(i)}\,(p(i) - p(0)) \geq B2i. \tag{5}$$

Since every Ducci sequence with minimal period k has period k but not k/p, $N_0(k) \geq N(k)$. Since every Ducci sequence of period k but not of minimal period k has period k/q for some prime q dividing k,

$$\begin{aligned}
N(k) &\geq 2^{k-2_k} - \delta 2^{(k-2_k)/2} - \sum_{i=0}^{r} 2^{k/p(i)-2_k} \\
&= N_0(k) - \sum_{i=0}^{r} 2^{k/p(i)-2_k} + (1-\delta)2^{k/p(0)-2_k} \\
&= N_0(k) + (1-\delta)2^{k/p(0)-2_k} - 2^{k/p(0)-2_k} \sum_{i=0}^{r} \frac{1}{2^{k/p(0)-k/p(i)}} \\
&\geq N_0(k) + (1-\delta)2^{k/p(0)-2_k} - 2^{k/p(0)-2_k} \frac{2^{2B}}{2^{2B}-1}
\end{aligned}$$

(applying inequality (5) and summing the infinite series $\sum(\frac{1}{2B})^i$). Thus

$$0 \leq 1 - \frac{N(k)}{N_0(k)} \leq \frac{2^{k/p(0)-2_k}}{2^{k-2_k} - 2^{k/p-2_{k/p}}} \left(\frac{2^{2B}}{2^{2B}-1} - 1 + \delta \right).$$

When k is odd we have $p = p(0)$ and $2_k = 1$, so

$$\begin{aligned}
0 \leq 1 - \frac{N(k)}{N_0(k)} &\leq \frac{2^{k/p-1}}{2^{k-1} - 2^{k/p-1}} \left(\frac{2^{2B}}{2^{2B}-1} - 1 \right) \\
&= \frac{1}{2^{k-k/p}-1} \, \frac{1}{2^{10}-1} \leq \frac{1}{2^{10}-1} \, \frac{1}{2^{2k/3}-1} \leq \frac{1}{2^{10}-1} \, \frac{1}{2^{70}-1}
\end{aligned} \tag{6}$$

since $p \geq 3$ and $k \geq 3 \cdot 5 \cdot 7$.

Now suppose k is even, so that $k \geq 2_k p(0)p(1) \geq (30)(2_k/2) \geq 30$ and hence $14 \leq 7k/15 = k/2 - k/30 \leq (k-2_k)/2$. Then

$$\begin{aligned}
0 \leq 1 - \frac{N(k)}{N_0(k)} &\leq \frac{2^{2B}}{2^{2B}-1} \, \frac{2^{k/p(0)-2_k}}{2^{k-2_k} - 2^{(k-2_k)/2}} \\
&= \frac{2^{2B}}{2^{2B}-1} \, \frac{1}{2^{k-k/p(0)}} \, \frac{1}{1 - \frac{1}{2^{(k-2_k)/2}}} \\
&\leq \frac{2^4}{2^4-1} \, \frac{2^{14}}{2^{14}-1} \, \frac{1}{2^{2k/3}} \leq \frac{2^4}{2^4-1} \, \frac{2^{14}}{2^{14}-1} \, \frac{1}{2^{20}}.
\end{aligned} \tag{7}$$

This completes the proof of Proposition 2. □

Remark: One can show that $1 - \frac{N(k)}{N_0(k)} < \frac{1.07}{2^{2k/3}}$. If k has at least 3 distinct prime divisors, then this follows from the formulas (6) and (7) above. If k has exactly two distinct prime divisors, then it is easy to show that $1 - \frac{N(k)}{N_0(k)} \leq 2^{-\frac{2}{3}k}$. Of course, if k has a unique prime divisor, then $N(k) = N_0(k)$.

4. DUALITY

We begin with an example. The vector $v = (1,1,0,0,0) \in \mathbb{Z}_2^5$ has minimal Ducci period 15 and $w = (1,0,1,0,1,1,0,0,1,0,0,0,1,1,1) \in \mathbb{Z}_2^{15}$ has minimal Ducci period 5. These facts turn out to be related. Consider the 5×15 matrix whose rows are the vectors $T^i(w)$, $0 \le i < 5$ (of course $T^5(w) = w$):

$$\begin{bmatrix} w \\ T(w) \\ T^2(w) \\ T^3(w) \\ T^4(w) \end{bmatrix} = \begin{bmatrix} 1&0&1&0&1&1&0&0&1&0&0&0&1&1&1 \\ 1&1&1&1&0&1&0&1&1&0&0&1&0&0&0 \\ 0&0&0&1&1&1&1&0&1&0&1&1&0&0&1 \\ 0&0&1&0&0&0&1&1&1&1&0&1&0&1&1 \\ 0&1&1&0&0&1&0&0&0&1&1&1&1&0&1 \end{bmatrix}.$$

The columns of the above matrix are exactly the transposes of the vectors $T^i(v), 0 \le i < 15$. We now show that this kind of behavior is not anomalous.

It is convenient for us to develop some terminology parallel to that in §2 that lets us deal simultaneously with an entire similarity class of vectors; we will use sequences here in place of the doubly infinite sequences of §2. (The use of doubly infinite sequences facilitated the analysis of similarity and the recursion arguments of §2.)

For each integer $m > 0$ let $\pi_m : \mathbb{Z}_2^m \to \mathbb{Z}_2^\omega$ be the map assigning to each vector $(a_i)_{0 \le i < m} \in \mathbb{Z}_2^m$ the sequence

$$(a_{i \bmod m})_{i \ge 0} = (a_{0 \bmod m}, a_{1 \bmod m}, a_{2 \bmod m}, \cdots) \in \mathbb{Z}_2^\omega.$$

One checks that vectors $a \in \mathbb{Z}_2^m$ and $b \in \mathbb{Z}_2^n$ are similar if and only if $\pi_m(a) = \pi_n(b)$. The image of π_m is the set of sequences $(a_i)_{i \ge 0}$ of *block length* m, i.e., with $a_{i+m} = a_i$ for all $i \ge 0$. We let $T : \mathbb{Z}_2^\omega \to \mathbb{Z}_2^\omega$ map each sequence $(a_i)_{i \ge 0}$ to $(a_i + a_{i+1})_{i \ge 0}$ and say that a sequence $a \in \mathbb{Z}_2^\omega$ has *Ducci period* k if $T^k(a) = a$.

For all $i \ge 0$, $m > 0$ and $a \in \mathbb{Z}_2^m$ we have $T^i(\pi_m(a)) = \pi_m(T_m^i(a))$. Therefore a vector $a \in \mathbb{Z}_2^m$ has Ducci period k if and only if $\pi_m(a)$ has Ducci period k.

We call a sequence $a = (a_i)_{i \ge 0} \in \mathbb{Z}_2^\omega$ a *Ducci list* if it has a finite block length and a finite Ducci period, and hence if and only if for some $m > 0$ it is the image under π_m of a vector in $\mathbb{Z}_2^m$ which is the initial term of a periodic Ducci sequence. The *infinite Ducci matrix* of a Ducci list $a \in \mathbb{Z}_2^\omega$ is the infinite matrix $[a_{ij}]_{i \ge 0, j \ge 0}$ such that for all $i \ge 0$, $T^i(a) = (a_{i0}, a_{i1}, \cdots)$. By the *transpose* of any infinite matrix $A = [a_{ij}]_{i \ge 0, j \ge 0}$ we mean the infinite matrix $A^{tr} = [a_{ji}]_{i \ge 0, j \ge 0}$.

Duality Theorem: *Let $a \in \mathbb{Z}_2^\omega$ be a Ducci list with block length m, Ducci period k, and infinite Ducci matrix A. Then the transpose of the first column of A is a Ducci list with block length k, Ducci period m, and infinite Ducci matrix A^{tr}.*

Proof: Write $A = [a_{ij}]_{i \ge 0, j \ge 0}$ and let $b = (a_{00}, a_{10}, a_{20}, \cdots)$ be the transpose of the first column of A. By the definition of T (and of A) for all $i \ge 0$ and $j \ge 0$ we have

$$a_{i+1,j} = a_{ij} + a_{i,j+1}$$

and hence $a_{i,j+1} = a_{ij} + a_{i+1,j}$. This says that for all $j \ge 0$, $T(a_{0j}, a_{1j}, a_{2j}, \cdots) = (a_{0,j+1}, a_{1,j+1}, a_{2,j+1}, \ldots)$ and hence that

$$T^j(b) = (a_{0j}, a_{1j}, a_{2j}, \cdots), \tag{8}$$

so the j-th column of A is just the transpose of $T^j(b)$, for all $j \geq 0$. Since a, and hence $T^i(a)$ for each $i \geq 0$, has block length m, the columns of A repeat with period m, so b has Ducci period m. Similarly, since a has Ducci period k, the rows of A repeat with period k and hence b has block length k. The formula (8) further tells us that A^{tr} is exactly the infinite Ducci matrix of b, as claimed. □

Remark: With a and b as in the above proof we call b the *dual* of a. Since $(A^{tr})^{tr} = A$, the dual of the dual of a is a. Note that if m is the minimal block length and k is the minimal Ducci period of a, then k is the minimal block length and m is the minimal Ducci period of the dual of a.

The set $\mathcal{S}_1$ of periodic n–number games (with vectors in $\mathbb{Z}_2^n$) is bijective with the set $\mathcal{S}_2$ of Ducci lists with block length n. By duality, $\mathcal{S}_2$ is bijective with the set $\mathcal{S}_3$ of Ducci lists with Ducci period n. The Main Theorem says that $\mathcal{S}_3$ has 2^{n-2_n} elements and Young's Theorem says that $\mathcal{S}_1$ has 2^{n-2_n} elements. Thus the two theorems are equivalent. We end this section by sketching a quick proof of Young's Theorem using linear algebra.

Proof of Young's Theorem: Write $n = 2^r t$ with t odd (so $2_n = 2^r$). The characteristic polynomial of T_n is

$$(x+1)^n + 1 = ((x+1)^t + 1)^{2^r} = x^{2^r} p(x)$$

for some $p(x) \in \mathbb{Z}_2[x]$ not divisible by x. (Note that 0 is a simple root of $(x+1)^t + 1$.) Then $\mathbb{Z}_2^n$ decomposes into a direct sum $V \oplus W$ of T_n–invariant subspaces where V and W denote the null spaces of $T_n^{2^r}$ and of $p(T_n)$, respectively. But $T_n|_V$ is nilpotent and $T_n|_W$ is invertible. It follows that W is exactly the set of vectors in $\mathbb{Z}_2^n$ with a finite Ducci period (clearly this set is contained in W and if $w \in W$ then $T_n^i(w) = T_n^j(w)$ for some positive integers $i > j \geq 0$, whence $T_n^{i-j}(w) = w$). Since $\dim V = 2^r = 2_n$, therefore $\dim W = n - 2_n$, i.e., W has 2^{n-2_n} elements. □

REFERENCES

[1] R. Brown and J. L. Merzel. "Limiting Behavior in Ducci Sequences." *Periodica Math. Hungarica* **47** (2003): 45-50.

[2] R. Brown and J. L. Merzel. "The Length of Ducci's 4–number Game." *Rocky Mountain J. Math.* **37** (2007): 45-66.

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

[4] A. Ludington–Young. "Length of the n–number Game." *Fibonacci Quart.* **28** (1990): 259-265.

[5] A. Ludington–Young. "Even Ducci Sequences." *Fibonacci Quart.* **37** (1999): 145-153.

[6] K. R. McLean. "Playing Diffy with Real Sequences." *Math. Gazette* **83** (1999): 58-68.

[7] M. Misiurewicz and A. Schinzel. "On n Numbers on a Circle." *Hardy-Ramanujan J.* **11** (1988): 30-39.

[8] I. Niven and H. S. Zuckerman. *An Introduction to the Theory of Numbers*, 4th ed., Wiley, 1980.

[9] J. Rotman. *An Introduction to the Theory of Groups*, 4th ed., Springer, 1995.

AMS Classification Numbers: 11B99, 40A05

✠✠✠