ON DUCCI SEQUENCES WITH ALGEBRAIC NUMBERS

MIHAI CARAGIU, ALEXANDRU ZAHARESCU, AND MOHAMMAD ZAKI

Abstract. In this paper we study the iterated absolute values of differences between consecutive elements of a periodic sequence of real algebraic numbers.

1. introduction

Many interesting mathematical problems and conjectures revolve around what came to be known as the *Ducci game*. Namely, if $d \geq 3$ is an integer, the traditional Ducci iteration is a map

$$D : \mathbb{Z}^d \to \mathbb{Z}^d$$

given by

$$D(x_0, x_1, \ldots, x_{d-1}) = (|x_0 - x_1|, |x_1 - x_2|, \ldots, |x_{d-1} - x_0|). \quad (1)$$

The origins of the problem may be traced back to Professor E. Ducci of Italy, who is credited in a 1937 article [8] with the discovery of the fact that the repeated application of D in the case $d = 4$ eventually leads to the null vector. Indeed, what makes this iteration even more interesting is the fact that if (and only if) d is a power of 2, the repeated application of D eventually leads to the null d-tuple. If d is not a power of 2, the dynamics induced by D always leads into cycles with the interesting property that the components of each d-tuple in a cycle are either 0 or some constant c (which is the same for all the d-tuples in the cycle), in which case it turns out that the Ducci map is essentially (up to a constant) a binary iteration $\overline{D} : \mathbb{F}_2^d \to \mathbb{F}_2^d$

$$\overline{D}(u_0, u_1, \ldots, u_{d-1}) = (u_0 + u_1, u_1 + u_2, \ldots, u_{d-1} + u_0). \quad (2)$$

The map $\overline{D}$ holds the key for the Ducci iteration in the case of integers, and is ultimately responsible for the lengths of the Ducci cycles (see [1, 4, 5, 7, 9, 10, 16]). The fact that the iteration eventually reaches the null d-tuple if $d = 2^k$ has a particularly simple explanation. Indeed, if one identifies an n-tuple $(u_0, u_1, \ldots, u_{d-1})$ with the polynomial

$$u(X) = \sum_{j=0}^{d-1} u_j X^j \in \mathbb{F}^2[X]/(X^d - 1),$$

one easily sees (2) as the multiplication by $1 + X^{-1} = 1 + X^{d-1} \in \mathbb{F}^2[X]/(X^d - 1)$. Since

$$\left(1 + X^{-1}\right)^d = \left(1 + X^{-1}\right)^{2^k} = 0 \in \mathbb{F}_2[X]/(X^d - 1),$$

it turns out that after d iterations we get a d-tuple with even entries, after $2d$ iterations we get a d-tuple with entries divisible by 4, etc. Thus their entries become divisible by higher and higher powers of 2. On the other hand, regardless of the choice of the initial d-tuple, the set of vectors generated in the Ducci process is bounded. Putting all of this together, the conclusion of the special case $d = 2^k$ follows, since an integer that is divisible by a power of 2 greater than its absolute value must necessarily be zero. The Ducci game can also be played over the rationals (in which case the same type of behavior at the limit holds for $D : \mathbb{Q}^d \to \mathbb{Q}^d$). Ducci games in a p-adic setting have been considered in which the transition rule is the multiplication by a p-adic polynomial $f(x) \in \mathbb{Z}^p[x]/(x^d - 1)$. Thus in [6] it is shown that the probability that a randomly chosen $f(x)$ generates a p-adic Ducci game with the property that the iterates converge to the zero element of $Z^p[x]/(x^d - 1)$ in the p-adic metric no matter the initial input, is p^{-t}, where t is the largest factor of d that is not divisible by p.

The Ducci iteration over the integers generated many outstanding problems [7] involving the lengths of the cycles, the asymptotic growth of the number of cycles with distinct lengths, and problems related to generalizations of the Ducci map to other mappings incorporating various "weights". Another interesting problem is in estimating the length of the Ducci game, that is the number of iterations needed in order to reach the limit cycle (see [3, 14, 17] for special case $d = 4$).

Fix a positive integer d, and consider the evolution function $D\colon \mathbb{R}^d \to \mathbb{R}^d$ defined by $D(a_1, \ldots, a_d) = (a'_1, \ldots, a'_d)$, where

$$a'_k = |a_k - a_{k+1}| \quad \text{for} \quad 1 \le k \le d-1, \text{ and } a'_d = |a_d - a_1|.$$

Alternatively, instead of the finite sequence $a_1, \ldots, a_d$, one can work with an infinite periodic sequence $(a_1, a_2, \ldots)$, where the components are defined by

$$a_k = a_{k+d}, \quad \text{for} \quad k \ge 1. \tag{3}$$

In that case the evolution function is defined by $D(a_1, a_2, \ldots) = (a'_1, a'_2, \ldots)$, with

$$a'_k = |a_k - a_{k+1}|, \quad \text{for} \quad k \ge 1. \tag{4}$$

We note in passing that this is the same map which appears in the well-known conjecture of Gilbreath (see [11, 13, 15]). While Gilbreath's conjecture is wide open, the periodicity of the sequence in the Ducci game allows one to understand the behavior of iterates of D in the long run.

Let $X = (x_1, \ldots, x_d) \in \mathbb{R}^d$, and consider the iterates $D^n(x_1, \ldots, x_d)$, $n \in \mathbb{N}$. In [2], Brown and Merzel proved that the sequence $(D^n(X))_{n\in\mathbb{N}}$ eventually stabilizes around one particular cycle, and then converges to this cycle as n tends to infinity. Given a positive integer d, $X \in \mathbb{R}^d$, we denote by E_X the set of limit points of the infinite sequence $(D^n(X))_{n\in\mathbb{N}}$. It is easy to see that for any $X \in \mathbb{R}^d$, E_X is a compact subset of $\mathbb{R}^d$. It is proved in [2] that for any $X \in \mathbb{R}^d$, E_X is finite, and the restriction $D|_{E_X}$ of D to E_X is a bijection of E_X onto itself.

It is also proved in [2] that the restriction $D|_{E_X}$ consists of exactly one cycle. Moreover, the iterates $D^n(X)$ converge to this cycle, in the sense that we have a partition of $\mathbb{N}$ as a finite union of arithmetic progressions having the same modulus, in such a way that the elements of E_X are in one-to-one correspondence with these arithmetic progressions, and $D^n(X)$ converges as $n \to \infty$ along each such arithmetic progression to the corresponding element of E_X. Thus, if L is the cardinality of E_X and $V_1, \ldots, V_L$ are the elements of E_X, then after a rearrangement of $V_1, \ldots, V_L$, one has

$$\lim_{m\to\infty} D^{j+mL}(X) = V_j, \text{ for each } 1 \le j \le L. \tag{5}$$

In the present paper, we consider the behavior of the iterates $D^n(X)$ in the case when all the components of X are algebraic numbers. We know from [2] that these iterates approach a cycle as $n \to \infty$, and we are interested to see how fast they converge to this cycle. Let us remark that there are cases when after finitely many iterates one already obtains a cycle. For example, if $d = 3$ and $X = (1, \sqrt{2}, 3\sqrt{2} - 2)$, then

$$\begin{aligned}
D(X) &= (\sqrt{2} - 1, 2\sqrt{2} - 2, 3\sqrt{2} - 3),\\
D^2(X) &= (\sqrt{2} - 1, \sqrt{2} - 1, 2\sqrt{2} - 2),\\
D^3(X) &= (0, \sqrt{2} - 1, \sqrt{2} - 1),\\
D^4(X) &= (\sqrt{2} - 1, 0, \sqrt{2} - 1),\\
D^5(X) &= (\sqrt{2} - 1, \sqrt{2} - 1, 0),
\end{aligned}$$

and

$$D^6(X) = (0, \sqrt{2} - 1, \sqrt{2} - 1) = D^3(X),$$

so we obtain a cycle of length 3.

For another example, let us choose now, still in the case $d = 3$, $X = (1, \theta, \theta^2)$, where θ is the positive root of the equation $x^2 + x - 1 = 0$, that is, $\theta = \frac{-1+\sqrt{5}}{2}$. Then

$$D(X) = (1 - \theta, \theta - \theta^2, 1 - \theta^2) = \theta(\theta, \theta^2, 1),$$

$$D^2(X) = \theta^2(\theta^2, 1, \theta),$$

and

$$D^3(X) = \theta^3(1, \theta, \theta^2).$$

More generally,

$$D^n(X) = \begin{cases} \theta^n(1, \theta, \theta^2), & \text{if } n \equiv 0 \pmod 3,\\ \theta^n(\theta, \theta^2, 1), & \text{if } n \equiv 1 \pmod 3,\\ \theta^n(\theta^2, 1, \theta), & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

This is an example where the limiting cycle consists of the point $(0, 0, 0)$ only, and is not obtained after finitely many iterates. Also note that here the convergence is exponentially fast.

We will show that for any X with algebraic components, the convergence of the iterates $D^n(X)$ to the corresponding limiting cycle cannot be faster than exponential, unless we are in a case when the cycle is already obtained after finitely many iterates.

Theorem 1.1. *Let $X \in \mathbb{R}^d$. Let $V_1, \ldots, V_L \in E_X$ satisfying (5). Assume that all the components of X are algebraic numbers. Then one of the following holds true.*

(i) *There exists an $m_0 \in \mathbb{N}$ such that*

$$D^{j+mL}(X) = V_j,$$

for all $m \geq m_0$.

(ii) *There exist positive constants C_1, C_2 depending only on X such that*

$$\|D^{j+mL}(X) - V_j\| \geq C_1 e^{-C_2 m}$$

for all $m \in \mathbb{N}$.

2. Proof of Theorem 1.1

We start with the following lemma.

Lemma 2.1. *Given a positive integer $d \geq 1$, let $X, Y \in \mathbb{R}^d$. Then,*

$$\|D(X) - D(Y)\| \leq 2\|X - Y\|,$$

where $\|.\|$ denotes the Euclidean norm on $\mathbb{R}^d$.

Proof. Let $X = (x_1, \ldots, x_d)$ and $Y = (y_1, \ldots, y_d)$. Then,

$$\|D(X) - D(Y)\|^2 = (|x_1 - x_2| - |y_1 - y_2|)^2 + \cdots + (|x_d - x_1| - |y_d - y_1|)^2.$$

Now, for each $1 \leq j \leq d$,

$$||x_j - x_{j+1}| - |y_j - y_{j+1}|| \leq |x_j - y_j| + |x_{j+1} - y_{j+1}|.$$

Therefore,

$$\begin{aligned}
&(|x_1 - x_2| - |y_1 - y_2|)^2 + (|x_2 - x_3| - |y_2 - y_3|)^2 + \cdots + (|x_d - x_1| - |y_d - y_1|)^2 \\
&\leq 2\left(|x_1 - y_1|^2 + |x_2 - y_2|^2 + |x_2 - y_2|^2 + |x_3 - y_3|^2 + \cdots + |x_d - y_d|^2 + |x_1 - y_1|^2\right) \\
&= 4\|x - y\|^2.
\end{aligned}$$

This proves Lemma 2.1. □

The above lemma says that the map D is 2-Lipschitzian. Let us remark that there is no $\lambda < 1$ for which D is λ-Lipschitzian, since otherwise D will be a contraction, and then for each $X \in \mathbb{R}^d$, the sequence of iterates $(D^n(X))_{n\in\mathbb{N}}$ will converge to the unique fixed point of D. But this is simply not the case as we have seen in the first example from the introduction.

Let us note that for any $X \in \mathbb{R}^d$ all the components of $D^n(X)$ are nonnegative if $n \geq 1$. Let M be the maximum of the components of $D(X)$. By the definition of D, it is easy to see that for all $n \geq 1$, all the components of $D^n(X)$ are real numbers belonging to $[0, M]$, so $D^n(X) \in [0, M]^d$ for all $n \geq 1$. This shows that the set E_X of limit points of the sequence $(D^n(X))_{n\in\mathbb{N}}$ is nonempty. For any $Y = (y_1, \ldots, y_d) \in [0, \infty)^d$ we denote by $M(Y)$ the maximum of the components of Y. Observe that the maximum component function M is a continuous function. Also $(M(D^n(X)))_{n\geq 1}$ is a non-increasing sequence of nonnegative numbers, so it converges to M_0. It follows from [2] that for any element $a \in E_X$, each component of a equals either 0 or M_0.

Proof of Theorem 1.1: There are two main ideas in the proof of the theorem. The first one is that, although the absolute value function $|.|$ is built into the definition of the map D, we may still write the iterates $D^n(X)$ as linear combinations of the components of X with integer coefficents, and provide bounds for these coefficents. The second idea is to multiply all the components of X by a fixed positive integer b to make them algebraic integers, and use the fact that the absolute value of the norm of any nonzero algebraic integer is at least one, in order to show that the iterates $D^n(X)$ stay away from the limiting cycle E_X, unless they belong to E_X. There is, however, a nontrivial difficulty in this approach, coming from the fact that we don't know whether or not the components of the elements of E_X are algebraic. As we will see below, this difficulty of not knowing whether M_0 is algebraic or not can be overcome by employing an argument which avoids using M_0 in the proof.

To start the proof, let K be a number field which contains all the components of $X = (a_1, \ldots, a_d)$. Let $[K : \mathbb{Q}]$ denote as usual the degree of K over $\mathbb{Q}$. Denote by O_K the ring of integers of K. From [2], we know that if L is the cardinality of E_X and $V_1, \ldots, V_L$ are the elements of E_X, then after a rearrangement of $V_1, \ldots, V_L$, one has

$$\lim_{m\to\infty} D^{j+mL}(X) = V_j, \text{ for each } 1 \le j \le L. \tag{6}$$

Next, observe that

$$\left\| D^{j+(m+1)L}(X) - D^{j+mL}(X) \right\| \le \left\| D^{j+(m+1)L}(X) - V_j \right\| + \left\| D^{j+mL}(X) - V_j \right\|.$$

By applying Lemma 2.1 repeatedly, we find that

$$\begin{aligned} \left\| D^{j+(m+1)L}(X) - V_j \right\| &\le 2 \left\| D^{j+(m+1)L-1}(X) - V_{j-1} \right\| \\ &\cdots \\ &\le 2^L \left\| D^{j+mL}(X) - V_{j-L} \right\| \\ &= 2^L \left\| D^{j+mL}(X) - V_j \right\|. \end{aligned}$$

Thus,

$$\left\| D^{j+(m+1)L}(X) - D^{j+mL}(X) \right\| \le (2^L + 1) \left\| D^{j+mL}(X) - V_j \right\|.$$

Let $Y = D^{j+(m+1)L}(X) - D^{j+mL}(X)$. So, $\|Y\| \le (2^L + 1) \left\| D^{j+mL}(X) - V_j \right\|$.

Next, fix a positive integer b such that $ba_1, \ldots, ba_d \in O_K$. Denote $D^n(X) = (a_{1,n}, \ldots, a_{d,n})$ for all n. In particular, $a_{1,0} = a_1, \ldots, a_{d,0} = a_d$. By induction on n, one finds that $ba_{1,n}, \ldots, ba_{d,n} \in O_K$ for all n. In order to see this, it is enough to note that, for any n and any $1 \le r \le d$, $a_{r,n+1} = a_{r,n} - a_{r+1,n}$ or $a_{r,n+1} = a_{r+1,n} - a_{r,n}$. Thus, $ba_{r,n+1} \in O_K$.

Also, by induction on n, each $a_{r,n}$, $r = 1, \ldots, d$ can be written as

$$a_{r,n} = c_{1,r,n}a_1 + c_{2,r,n}a_2 + \cdots + c_{d,r,n}a_d$$

with $c_{1,r,n}, \ldots, c_{d,r,n} \in \mathbb{Z}$, and $\max\{|c_{1,r,n}|, \ldots, |c_{d,r,n}|\} \le 2^n$.

We write $Y = (h_1, \ldots, h_d)$. Then for each $1 \le r \le d$, $h_r = a_{r,j+(m+1)L} - a_{r,j+mL}$. On one hand, we know that $bh_r = ba_{r,j+(m+1)L} - ba_{r,j+mL} \in O_K$. On the other hand,
$h_r = (c_{1,r,j+(m+1)L} - c_{1,r,j+mL})a_1 + \cdots + (c_{d,r,j+(m+1)L} - c_{d,r,j+mL})a_d$.

Therefore,

$$\begin{aligned} |h_r| &\le (|c_{1,r,j+(m+1)L}| + |c_{1,r,j+mL}|)|a_1| + \cdots + (|c_{d,r,j+(m+1)L}| + |c_{d,r,j+mL}|)|a_d| \\ &\le (2^{j+(m+1)L} + 2^{j+mL})(|a_1| + \cdots + |a_d|). \end{aligned}$$

Next, for any embedding σ of K into $\mathbb{C}$, we have that $\sigma(h_r) = (c_{1,r,j+(m+1)L} - c_{1,r,j+mL})\sigma(a_1) + \cdots + (c_{d,r,j+(m+1)L} - c_{d,r,j+mL})\sigma(a_d)$. Thus, as above we find that

$$|\sigma(h_r)| \le (2^{j+(m+1)L} + 2^{j+mL})(|\sigma(a_1)| + \cdots + |\sigma(a_d)|).$$

It follows that

$$|\sigma(bh_r)| \le b(2^{j+(m+1)L} + 2^{j+mL})(|\sigma(a_1)| + \cdots + |\sigma(a_d)|).$$

Let $R = (2^{j+(m+1)L} + 2^{j+mL}) \max_{\sigma} |\sigma(a_1)| + \cdots + |\sigma(a_d)|$, where the maximum is taken over all the embeddings σ of K into $\mathbb{C}$. Then

$$|\sigma(bh_r)| \le bR,$$

for all embeddings σ.

Now, for each $r \in \{1, \ldots, d\}$, we distinguish two cases. Either $h_r = 0$ in which case $N_{K/\mathbb{Q}}(bh_r) = 0$, or $h_r \neq 0$, and then $|N_{K/\mathbb{Q}}(bh_r)| \geq 1$ since $bh_r \in O_K$ is nonzero. In the second case we further deduce that

$$|bh_r| \geq \frac{1}{(bR)^{[K:\mathbb{Q}]-1}},$$

and so

$$|h_r| \geq \frac{1}{b^{[K:\mathbb{Q}]}R^{[K:\mathbb{Q}]-1}}.$$

Next, if $h_r = 0$ for all $1 \leq r \leq d$, then $Y = 0$, and hence

$$D^{j+mL}(X) = D^{j+(m+1)L}(X).$$

In this case it follows that

$$D^{j+mL}(X) = D^{j+(m+1)L}(X) = D^{j+(m+2)L}(X) = \ldots.$$

Therefore, $D^{j+mL}(X)$ belongs to E_X, and then it must coincide with V_j. Note that if this holds for one particular pair (j, m), then $D^n(X)$ belongs to E_X for any $n \geq j + mL$, and then one is on case (i) of the theorem. The other alternative is when there is no pair (j, m) for which $D^{j+mL}(X) \in E_X$. In this second case, we have that for any choice of j and m, at least one component h_r of the corresponding Y is nonzero. Then the Euclidean norm of Y satisfies

$$\|Y\| = \left(\sum_{1\leq j\leq d} |h_j|^2\right)^{\frac{1}{2}} \geq |h_r| \geq \frac{1}{b^{[K:\mathbb{Q}]}R^{[K:\mathbb{Q}]-1}}.$$

Since $\|Y\| \leq (2^L + 1)\left\|D^{j+mL}(X) - V_j\right\|$, we have that

$$\left\|D^{j+mL}(X) - V_j\right\| \geq \frac{1}{(2^L+1)b^{[K:\mathbb{Q}]-1}R^{[K:\mathbb{Q}]-1}}.$$

In this case we conclude the

$$\|D^{j+mL}(X) - V_j\| \geq C_1 e^{-C_2 m}$$

for all pairs (j, m), for some positive constants C_1 and C_2 depending on X only. This completes the proof of Theorem 1.1. □

3. Comments

The value of the exponent C_2 which is achieved by our proof above is

$$C_2 = (\log 2)\left([K : Q] - 1\right) L.$$

As was pointed out by the referee, when M_0 is algebraic, Roth's Theorem (see p. 304 in [12]) gives $C_2 = (\log 2)\,(2 + \epsilon)\, L$ for any ϵ. Here one uses the fact that the height of h_r is bounded by a constant times 2^{mL}. It may be interesting to ask if one can obtain the optimal value for the exponent C_2 in the main result.

One may also ask whether the fact that the convergence of the Ducci iterates to the corresponding limiting cycle cannot be faster than exponential unless the limit cycle is effectively reached holds in general for all X with arbitrary real components.

4. Acknowledgement

The authors are grateful to the referee for many useful comments and suggestions.

References

[1] F. Breuer, E. Lotter, and B. van der Merwe, *Ducci-sequences and cyclotomic polynomials*, Finite Fields Appl., **13.2** (2007), 293–304.

[2] R. Brown and J. L. Merzel, *Limiting behavior in Ducci sequences*, Period. Math. Hungar., **47.1-2** (2003), 45–50.

[3] R. Brown and J. L. Merzel, *The length of Ducci's four-number game*, Rocky Mountain J. Math., **37.1** (2007), 45–65.

[4] N. J. Calkin, J. G. Stevens, and D. M. Thomas, *A characterization for the length of cycles of the N-number game*, The Fibonacci Quarterly, **43.1** (2005), 53–59.

[5] J. P. Campbell, *Reviews*, Mathematics Magazine, **69.4** (1996), 311–313.

[6] M. Caragiu and N. Baxter, *A note on p-adic Ducci games*, JP J. Algebra Number Theory Appl., **8.1** (2007), 115–120.

[7] M. Chamberland and D. M. Thomas, *The N-number Ducci game*, J. Difference Equations and Applications, **10.3** (2004), 339–342.

[8] C. Ciamberlini and A. Marengoni, *Su una interessante curiosita numerica*, Periodiche di Matematiche, Ser. 4, 17 (1937), 25–30.

[9] C. I. Cobeli, M. Crâşmaru, and A. Zaharescu, *A cellular automaton on a torus*, Portugal. Math., **57.3** (2000), 311–323.

[10] A. Ehrlich, *Periods in Ducci's N-number game of differences*, The Fibonacci Quarterly, **28.4** (1990), 302–305.

[11] R. K. Guy, *Unsolved Problems in Number Theory*, Third edition, Problem Books in Mathematics, Springer-Verlag, New York, (2004), 42–43.

[12] M. Hindry and J. H. Silvermann, *Diophantine Geometry. An Introduction*, Graduate Texts in Mathematics, Vol. 201, Springer-Verlag, New York, 2000.

[13] R. B. Killgrove and K. E. Ralston, *On a conjecture concerning the primes*, Math. Tables Aids Comput., **13** (1959), 121–122.

[14] A. Ludington-Young, *Length of the N-number game*, The Fibonacci Quarterly, **28.3** (1990), 259–265.

[15] A. M. Odlyzko, *Iterated absolute values of differences of consecutive primes*, Math. Comp., **61.203** (1993), 373–380.

[16] B. Thwaites, *Two conjectures or how to win £1100*, Mathematical Gazette, **80** (1996), 35–36.

[17] W. A. Webb, *The length of the four-number game*, The Fibonacci Quarterly, **20.1** (1982), 33–35.

MSC2010: 11B85

Department of Mathematics, Ohio Northern University, 525 S Main Street, Ada, Ohio 45810
E-mail address: m-caragiu1@onu.edu

Institute of Mathematics of the Romanian Academy, P.O.Box 1-764, Bucharest 014700, Romania, and Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 W. Green Street, Urbana, IL 61801
E-mail address: zaharesc@math.uiuc.edu

Department of Mathematics, Ohio Northern University, 525 S Main Street, Ada, Ohio 45810
E-mail address: m-zaki@onu.edu