GAME OF DUCCI SEQUENCES

A THESIS

submitted in partial fulfillment of the requirements

for the award of the dual degree of

Bachelor of Science-Master of Science

in

MATHEMATICS

by

VIKAS

(18311)

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH BHOPAL
BHOPAL - 462066

April 2023

भारतीय विज्ञान शिक्षा एवं अनुसंधान संस्थान भोपाल

Indian Institute of Science Education and Research Bhopal

(Estb. By MHRD, Govt. of India)

CERTIFICATE

This is to certify that **VIKAS**, BS-MS (Dual Degree) student in Department of Mathematics has completed bonafide work on the thesis entitled **'GAME OF DUCCI SEQUENCES'** under my supervision and guidance.

April 2023
IISER Bhopal

Dr. Nikita Agarwal

Committee Member	**Signature**	**Date**
Dr. Nikita Agarwal		
Dr. Atreyee Bhattacharya		
Dr. Karam Deo Shankhadhar		

ACADEMIC INTEGRITY AND COPYRIGHT DISCLAIMER

I hereby declare that this project report is my own work and due acknowledgement has been made wherever the work described is based on the findings of other investigators. This report has not been accepted for the award of any other degree or diploma at IISER Bhopal or any other educational institution. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

I certify that all copyrighted material incorporated into this document is in compliance with the Indian Copyright (Amendment) Act (2012) and that I have received written permission from the copyright owners for my use of their work, which is beyond the scope of the law. I agree to indemnify and safeguard IISER Bhopal from any claims that may arise from any copyright violation.

April 2023 **VIKAS**
IISER Bhopal

ACKNOWLEDGEMENT

I am deeply grateful to Dr. Nikita Agarwal, my guide, for providing me with invaluable guidance and constant support during the completion of my Master's thesis. I am truly fortunate to have had the opportunity to work under her supervision. I thank Dr. Karam Deo Shankhadhar and Dr. Atreyee Bhattacharya for being in my project evaluation committee and for their valuable comments. I am always thankful to the Department of Mathematics, IISER Bhopal, for providing me with a comprehensive and enriching academic experience. I would like to thank all my friends for making my life enjoyable and memorable at IISER. I want to thank my family for their love, affection and constant support.

VIKAS

ABSTRACT

The iteration of functions has been a subject of great interest to mathematicians for a long time. Despite appearing to be a stand-alone problem, it is related to several branches of mathematics. The orbit of point x in the domain under a map f is given by $x, f(x), f \circ f(x), \ldots$. Our primary concern is to study these orbits and answer the fundamental question such as whether the orbit is periodic or chaotic. Also whether the map f has a fixed point.

The orbits generated by the *Ducci* map are called *Ducci* sequences, which are eventually periodic. In the first chapter, we will formally define the *Ducci Map* and *Ducci* sequences, along with some motivating examples. In chapter 2, we will thoroughly describe the elements in the domain whose *Ducci sequences* are terminating. In chapters 3, and 4, we first characterize the elements that are in the cycle and study the period of *Ducci* sequences and derive explicit formulas for it. In chapter 5, we will study the limit point of the *Ducci* sequence. In chapter 6, we will give an asymptotic lower bound for the period of *Ducci* sequence. We will use finite field theory to derive the results. Finally, the *Ducci* map will be studied in matrix form in chapters 7 and 8, along with a few of its variants. This thesis is based on the existing literature on *Ducci sequences*, in particular, [1], [2], [3], [4], [5], [6], [7], [8].

Contents

Chapter 1

Introduction and Motivation

1.1 Iterated function

Let X be a complete metric space. An iterated function is a function which is obtained by composing a function $f : X \to X$ with itself a certain number of times. The nth iterate of f is denoted by f^n. Here $f^n = f \circ f \circ \dots f$ (n times composition of f).
For $x \in X$, one of the main concerns of dynamics is to study the sequence, $\{x, f(x), f^2(x), .., f^n(x), ..\}$ known as the orbit of x or iterates of f on x. Iterative functions are studied in dynamical system, computer science, fractals, and many more.

1.2 Examples

- **Mandelbrot set**
  Let $X = \mathbb{C}$ and
  $$f_c(z) = z^2 + c.$$
  The Mandelbrot set is the set of complex numbers $c \in X$ such that the orbit $\{f_c(0), f_c^2(0), f_c^2(0), \dots, \}$ remains bounded in absolute value.
  For $c = -1$, its orbit is $\{-1, 0, -1, \dots\}$, which is bounded in absolute value, so

$c = -1$ will be in Mandelbrot set. The figure below is the plot of Mandelbrot set in the complex plane.

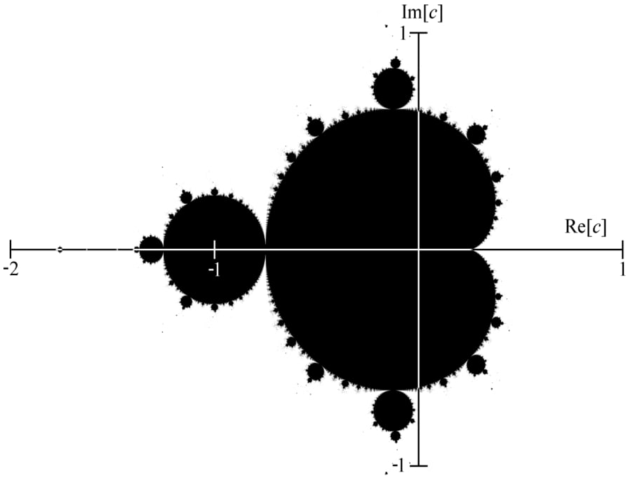


Figure 1.1: Mandelbrot Set

- **Collatz Conjecture**

  The Collatz conjecture, also known as the $3n + 1$ problem, is one of the most famous unsolved problems in mathematics. Let $X = \mathbb{N}$ and

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \equiv 0 \bmod 2, \\ 3n + 1 & \text{if } n \equiv 1 \bmod 2. \end{cases}$$

  The Collatz conjecture is: for any $n \in X$, its orbit eventually reaches 1. It has been observed that there are numbers that are sufficiently close to each other but their orbits show entirely different behavior. For example, it takes 112 iterations for $n = 27$ to reach 1, but only 11 iterations for $n = 26$. The figure below shows a few orbits in the form of a tree.

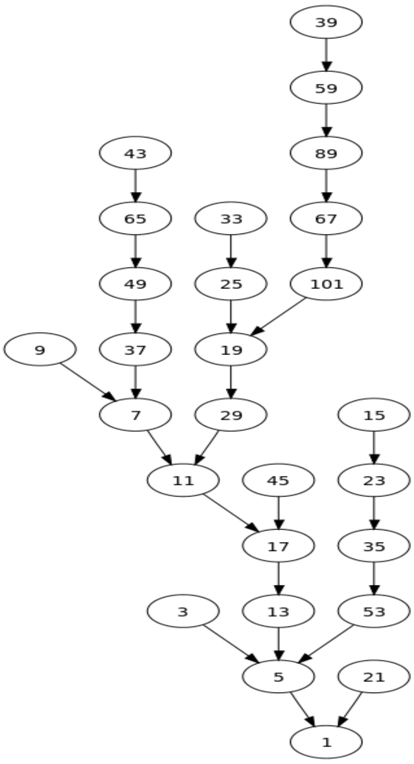


Figure 1.2: Collatz Conjecture

The above two examples show how simple orbits can create a complex structure. Upon analysis, it reveals a strong connection between these problems and branches of pure mathematics such as number theory, abstract algebra, linear algebra, and also theoretical computer science.

In this thesis, we are going to study iterates of *Ducci map* in its various forms. The orbit of a given point under this map is called a *Ducci* sequence. *Ducci* sequences are named after Enrico Ducci (1864 - 1940), the Italian mathematician who discovered this in the 1930s. In the next section, we will formally define the *Ducci* Map with and necessary concepts.

1.3 The Ducci Map

Definition 1.1. *Let $X = \mathbb{Z}^{\mathbb{N}}$, the set of infinite sequences of integers. Consider the following map $D : X \to X$ defined as*

$$D((a_i)_{i\in\mathbb{N}}) = (a'_i)_{i\in\mathbb{N}},$$

where $(a_i)_{i\in\mathbb{N}} \in X$ and for each $i \in \mathbb{N}$, $a'_i = |a_{i+1} - a_i|$. The map D is known as the Ducci map.

Definition 1.2. *Let $C = (x_i)_{i=1}^{\infty}$ be an infinite sequence of integers. We call C an $n-$cycle if and only if $x_{i+n} = x_i$ for all i. An $n-$cycle is represented as n-tuple $(x_1, x_2, \ldots, x_n)$.*

We will interchangeably use the notation $n-$cycle and $n-$tuple according to convenience and goal.

1.4 Ducci Sequence

Definition 1.3. *Let C be an integer $n-$tuple. A sequence of integer $n-$tuples obtained by iteratively applying the map D on C is known as a Ducci Sequence. For example, Ducci sequence of C is $C, D(C), D^2(C), \ldots$.*

Definition 1.4. *An integer n-tuple C is known as a repeating or periodic cycle if there exist some $N \geq 1$ such that $D^N(C) = C$. The smallest such N is known as the period of C.*

Remark 1.5. *Every $n-$cycle is also a $kn-$cycle.*

Remark 1.6. *After one application of D, all elements of the $n-$tuple become non-negative.*

Remark 1.7. *Suppose C is an $n-$cycle with non-negative entries. Then $m(D(C)) =\leq m(C)$, where $m(C)$ denotes the maximum of the entries of C.*

Remark 1.8. *The $0-$cycle given by $(0, 0, \ldots, 0)$ is the only repeating cycle with period 1.*

Remark 1.9. *Due to remark 1.7, for every integer n-tuple C, there is the first tuple which is equal to previous tuple $D^r(C)$. In this case, the tuples $D^r(C), D^{r+1}(C), \ldots, D^{s-1}(C)$ forms a repeating or periodic cycle. The length of this cycle is $s-r$ and is known as the period of C.*

Chapter 2

Terminating and Non-terminating Cycles

Definition 2.1. *An $n-$cycle is said to be terminating if its orbit eventually goes to the $0-$cycle. A cycle that is not terminating is called a non-terminating cycle.*

Example 2.2. *Consider $A = (3, 6, 2, 4)$. Then*
$D(A) = (3, 4, 2, 1),\ D^2(A) = (1, 2, 1, 2),\ D^3(A) = (1, 1, 1, 1),\ D^4(A) = (0, 0, 0, 0).$
A is a terminating 4-cycle.

Example 2.3. *Consider $A = (1, 3, 2),\ D(A) = (2, 1, 1),\ D^2(A) = (1, 0, 1),\ D^3(A) = (1, 1, 0),\ D^4(A) = (0, 1, 1),\ D^5(A) = (1, 0, 1)$. Hence A is a non-terminating cycle.*

In this section, our focus will be on the $n-$cycles which are terminating.

Definition 2.4. *If $C = (x_1, x_2, \ldots, x_n)$ such that $x_i \in \{0, 1\}$ for all i, then C will be called primitive cycle.*

Theorem 2.5. *Every repeating $n-$cycle is a constant multiple of primitive $n-$cycle.*

Proof. If C is repeating cycle then by Remark 1.7 , $m(C) = m(D^t(C)) = m$ for $t = 1, 2, 3, \ldots$. Also, at least there is one occurrence of m in C. Let k be the period of C and C_1 be the unique repeating D preimage of C, i.e $C_1 = D^{k-1}(C)$. Since $m(C_1) = m$ there exist two entries of C_1 whose difference is m. Possible choices are

$0, m$ or $m, 0$.
In the same fashion let C_2 be the unique D repeating preimage of C_1, and $m(C_2) = m$. Thus, for occurance of $0, m$ or $m, 0$ in C_1 three entries of C_2 should be from $\{0, m\}$. Recursively doing this process nth preimage of C is C_n having each entry from $\{0, m\}$. As $C_n = D^{k-n}(C)$, we have $D^n(C_n) = D^n(D^{k-n}C) = C$. Thus $C = D^n(C_n)$. □

Theorem 2.6. *Let C be a primitive $n-$cycle with $n = 2^k L$, where L is odd. Then*

1. *C is terminating if and only if it is a 2^k-cycle.*
2. *C is repeating if and only if (as a $n-$tuple over $\mathbb{Z}_2$) it is orthogonal to every primitive terminating $n-cycle$.*

Proof. For $C = (x_1, x_2, \dots, x_n)$ be primitive. Then $|x_{i+1} - x_i| \equiv x_{i+1} + x_i \bmod 2$ for each i, If $I(x_1, x_2, \dots, x_n) = (x_1, x_2, \dots, x_n)$ and $H(x_1, x_2, \dots, x_n) = (x_2, x_3, \dots, x_n, x_1)$. Then $D = I + H$, so D becomes a linear operator on $n-$dimensional vector space over $\mathbb{Z}_2$.
Now, $D^r = (I + H)^r = \sum_{j=0}^{r} \binom{r}{j} H^j$. Denote $D^r(A) = (y_{ri})_{i=1}^{n}$, where $y_{ri} = \sum_{j=0}^{r} \binom{r}{j} x_{i+j}$.
So C is terminating if and only if $\sum_{j=0}^{r} \binom{r}{j} x_{i+j} \equiv 0 \bmod 2$ for some r and for all i. WLOG assume that r is power of 2 . Then

$$\sum_{j=0}^{r} \binom{r}{j} x_{i+j} = 0 \implies \binom{r}{0} x_i + \binom{r}{r} x_r \equiv 0 \bmod 2.$$

As $\binom{r}{j}$ when $0 < j < 2^s$ is even then, $\binom{r}{j} \equiv 0 \bmod 2$.
Thus C is terminating if and only if $x_i = x_{i+r}$, This means C is r-cycle. Now it has been given that C is $2^k L-$cycle, it is equivalent to C is $r = 2^k$-cycle as $2^k | 2^k L$.
For proof of the part 2, observe that the left shift map H is invertible and for any vectors u and v,

$$H(u).v = u.E^{-1}(v). \tag{2.1}$$

Let T be the subspace of primitive terminating n-cycles. It is trivial that H leaves invariant the subspace T. Now we claim that H leaves invariant the orthogonal

complement of T, call it R.
Let $u \in R$ and $v \in T$, If we are able to show RHS is 0 for 2.1 ,then our claim is established, but as H is invertible, so $H^{-1}(v) \in T$, so RHS is 0. Then $D = I + H$ also preserves R. But T contains the kernel of D which is $\{\{0, 0, \ldots, 0\}, \{1, 1, \ldots, 1\}\}$, and we know $T \cap R = \{0, 0, \ldots, 0\}$.
So D becomes a nonsingular linear transformation when restricted to R. This means that R must consist entirely of repeating n-cycles. □

Theorem 2.7. *Every $n-$cycle of integers or rational numbers eventually, under repeated application of D can be reduced to a repeating one.*

Proof. Suppose $C = (\frac{x_1}{y_1}, \frac{x_2}{y_2}, \ldots, \frac{x_n}{y_n})$ be a rational $n-$cycle. Since every $n-$cycle is $kn-$cycle. Choosing $k = \gcd\{y_1, y_2, \ldots, y_n\}$, we converted C into integer $kn - cycle$. Since $\max(D^{i+1}) \leq \max(D^i)$, so in *Ducci* Sequence, there are only a finite number of elements. If we consider $m = \max(C)$, $(m+1)^n$ are the total different $n-$cycle that are possible in *Ducci* sequence that can be exhausted after finite application of D. So there are only two cases left either the *Ducci* sequence eventually reaches zero(cycle of period 1) or forms a repeating cycle. □

The following theorems will give a concrete description of $n-$cycles that are terminating.

Theorem 2.8. *Every rational $n-$cycle is terminating if n is a power of 2.*

Proof. By theorem 2.7, every rational $n-$cycle will eventually be reduced to repeating one. By theorem 2.5, every repeating $n-$cycle is a constant multiple of primitive $n-$cycle. By theorem 2.6, every primitive 2^k-cycle is terminating. □

Theorem 2.9. *If n is odd, the only terminating rational $n-$cycles are trivial ones (entries are same).*

Proof. By theorem 2.6, $n-$cycle is terminating $\iff$ n is power of two. The only exception cycle is $(m, m, \ldots, m)$, for some $m \geq 0$. □

Theorem 2.10. *If n is neither power of 2 nor odd, then there are non-terminating rational $n-$cycle as well as non-trivial terminating rational $n-$cycles.*

Proof. Suppose $n = 2^k L$, L is odd greater than 1, since every $n-$cycle is $kn-$cycle, As $2^k|n$, then there must be terminating 2^k-cycles. Similarly, $L|n$, then there must be non terminating $L-$cycle. □

2.1 D-preimage

Lemma 2.11. *Let $C = (x_1, x_2, \dots, x_n)$ be an $n-$cycle. Then C has $D-$preimage if and only if there exists $A \subseteq \{1, 2, 3 \dots, n\}$ for which $\sum_{i\in A} x_i = \sum_{i\notin A} x_i$.*

Proof. $\Longrightarrow$ Let $C_1 = (y_1, y_2, \dots, y_n)$ is $n-$cycle be the $D-$preimage of C or $D(C_1) = C$. We need to construct set A.
Let $A = \{i \mid x_i = y_i - y_{i+1}\}$. Now,

$$\sum_{i\in A} x_i = \sum_{i=1}^{n} \mathcal{X}_i(A)x_i \quad , \quad \sum_{i\notin A} x_i = \sum_{i=1}^{n} \mathcal{X}_i(A^c)x_i,$$

where $\mathcal{X}_i(A)$ is 1 if $i \in A$ otherwise 0, similarly for set A^c.
Then,

$$\begin{aligned}\sum_{i\in A} x_i - \sum_{i\notin A} x_i &= \sum_{i=1}^{n} \mathcal{X}_i(A)x_i - \sum_{i=1}^{n} \mathcal{X}_i(A^c)x_i,\\ &= \sum_{i=1}^{n}(\mathcal{X}_i(A) + \mathcal{X}_i(A^c)(y_i - y_{i-1}),\\ &= \sum_{i=1}^{n}(y_i - y_{i-1}) = 0.\end{aligned}$$

Thus, $\sum_{i\in A} x_i = \sum_{i\notin A} x_i$.

$\Longleftarrow$ Given that there exist $A = \{1, 2, 3, \dots, n\}$ such that $\sum_{i\in A} x_i = \sum_{i\notin A} x_i$. We will construct a $D-$preimage of C.
Let $y_1 = \sum_{i\in A}$, and $y_{i+1} = y_i + \epsilon_i x_i$, where $\epsilon_i = 1$ when $i \in A$ and $\epsilon_i = -1$ when $i \in A^c$, then $D(C) = (y_1, y_2, \dots, y_n)$. □

Chapter 3

Tuples in a Repeating Cycle

We have already seen that *Ducci sequences* are eventually periodic. The tuples which are in the repeating cycle show interesting behavior. In this chapter, we will explicitly determine those tuples in the repeating cycle. We seek to characterize the repeating cycles of $k-$tuples for $k = 2^r k'$, where $k' > 1$ is odd. For that, we will slightly change the trivial notation for this chapter.

Notation

- Denote $A = (a_0, a_1, \ldots, a_{k-1})$ as $k-$tuple, $D(A) = \overline{A}$.
- We obtain another k-tuple $\bar{A} = (a'_0, a'_1, \ldots, a'_{k-1})$,where $a'_i = |a_{i+1} - a_i|$ and $\overline{A_i} = A_{i+1}$.
- For *Ducci map* on k-tuples, subscripts are always reduced to modulo(k), so that $a'_{k-1} = |a_{k-1} - a_0|$.

3.1 Reduction of the problem

Lemma 3.1. *For any $k-$tuple (a_i), we have*

$$(\overline{\lambda a_i + \delta}) = \lambda\overline{(a_i)} \quad \lambda \in \mathbb{Z}^+ \ , \ \delta \in \mathbb{Z}^+ \cup \{0\}.$$

This lemma narrows down the domain of study. We need to consider only those

$k-$tuples $A = (a_i)$ for which non-zero terms are relatively prime. The following result helps us characterize the tuples in the repeating cycle.

Lemma 3.2. *If $A = (a_i)$ is in repeating cycle then there is some index j such that*

1. $a_j = max(A)$,

2. $a_{j-1} = 0$ *or* $a_{j+1} = 0$.

Proof. We already know for $A = (a_i)$ in a repeating cycle, we have $\max(A) = \max(\overline{A})$. Suppose $a_j = \max(A) = m$. As $a'_j = |a_j - a_{j+1}|$, if $a'_j = m$ then $a_{j+1} = 0$, or if $a_{j+1} = \max(A) = m$ then $a_j = 0$. So at the position of the maximum element, either the left side element or the right side element to it is 0. □

Lemma 3.3. *Suppose $A_0 = (a_i)$ be $k-$tuple is in a repeating cycle such that* $\gcd\{a_i \mid a_i \neq 0\} = 1$. *Then* $\max A_0 = 1$.

Proof. The proof is by contradiction. Let $\max A_0 = m$ with some $a_i \notin \{0, m\}$. Left shift of A_0 does not change the overall properties of its orbit. Assume A_0 of the form $A_0 = (a_0, a_1, \ldots, a_{l-1}, a_l, a_{l+1})$, where $a_0 \notin \{0, m\}$; $a_i \in \{0, b\}$, $i = 1, 2, \ldots, l$ also $a_j = m$ and $a_{j+1} = 0$ for some $1 \leq j \leq l$ (such pair exist by lemma 3.2) and l is large as possible. Also, observe that $l \geq 2$ and either $a_{l+1} \notin \{0, m\}$ or else $l = k$. Applying D on A_0, we get

$$A_1 = \overline{A_0} = (a'_0, a'_1, \ldots, a'_l, a'_{l+1}, \ldots).$$

For A_1, observe that $a'_0 \notin \{0, m\}$, since $a_0 \notin \{0, m\}$ and $a_1 \in \{0, m\}$, $a'_i \in \{0, m\}$ $i = 1, 2 \ldots, l-1$ since $a_l \in \{0, m\}$ and $a_{l+1} \notin \{0, m\}$.
Continuing this process, we have

$$A_{l-1} = (a_0", a_1", \ldots, a_l", \ldots).$$

Where for A_{l-1}, $a_0" \notin \{0, m\}$; $a_1" \in \{0, m\}$ and $a_2" \notin \{0, m\}$.

Since the maximum element does not change in a repeating cycle, we have $a_1" \neq 0$. However, this is contradictory to the lemma 3.2 since on the LHS, and the RHS of $a_1" = m$ is not zero, and l is chosen as large as possible. □

As a result of lemma 3.3, we need only to consider primitive $k-$tuples.

3.2 Characterization of Tuple in a Repeating Cycle

From now on, for $A = (a_i)$ we will consider $a_i \in \{0, 1\}$, and write

$$(\overline{a_i}) = (a_i + a_{i+1}).$$

Theorem 3.4. *Let $A_0 = (a_i)$ and $A_n = (b_i^n)$, suppose the $2-$adic expansion of n is $n = \sum_{s=0}^{N} \alpha_s 2^s, \alpha_N \neq 0$. Then*

$$b_i^n = \sum_{j \in J} a_{j+i},$$

J is the set of all $j = \sum_{s=0}^{N} \beta_s 2^s$ for which $\beta = 0$ whenever $\alpha_s = 0$.

Proof. We will prove the theorem by induction on n.
Before proving the theorem following is an example. 2-adic expansion of $n = 11$ is $11 = 1 + 2 + 2^3$. Then $b_0^{11} = \beta_0 + \beta_1 2 + \beta_3 2^3$. When $\beta_i \in \{0, 1\}$ $\alpha_i = 0 \implies \beta_i = 0$, we get $J = \{0, 1, 2, 3, 8, 9, 10, 11\}$.
- When $n = 1$.

For this case set $J = \beta_0 2^0$, where $\beta_0 \in$ {0,1}, so J contain two element $\{0, 1\}$.
$\implies b_i^n = \sum_{j \in J} a_{j+i} = (a_i + a_{i+1})$.
So, our aim in this proof is to find the set J. There are three cases depending on $n = \sum_{s=0}^{N} \alpha_s 2^s$.
Assume true for $n > 1$. Thus we have

$$A_n = (b_0^n, b_1^n, \ldots, b_{k-1}^n).$$

To show:

$$A_{n+1} = \overline{A_n} = (b_0^n + b_1^n, \ldots, b_{k-1}^n + b_0^n).$$

Observe that, on RHS, we can see entries comes with the help of set J that depends on n and on LHS we can see entries comes from set say $\bar{J}$ for $n+1$. We will seek $\bar{J}$ with the help of J.

Case 1 When

$$n = \sum_{s=1}^{N} \alpha_s 2^s,$$

corresponding $J = \{j : \sum_{s=1}^{N} \beta_s 2^s, \alpha_s = 0 \implies \beta_s = 0\}$.

$$n + 1 = \sum_{s=0}^{N} \alpha_s 2^s + 1,$$

corresponding $\bar{J} = \{j : \sum_{s=0}^{N} \beta_s 2^s, \alpha_s = 0 \implies \beta_s = 0, s > 1\}$,

$$\bar{J} = J \cup J + 1.$$

verifying: $b_i^{n+1} = b_i^n + b_{i+1}^n$.
RHS:

$$b_i^n + b_{i+1}^n = \sum_{j \in J} a_{j+i} + \sum_{j \in J} a_{j+i+1}.$$

LHS:

$$\begin{aligned} b_i^{n+1} = \sum_{j \in \bar{J}} a_{j+i} &= \sum_{j \in J} a_{j+i} + \sum_{j \in J+1} a_{j+i} \\ &= \sum_{j \in J} a_{j+i} + \sum_{j \in J} a_{j+i+1}. \end{aligned}$$

RHS=LHS, hence proved.

Case 2: When

$$n = \sum_{s=0}^{N} 2^s,$$

Observe that for such n defined set $J = \{0, 1, 2, ..., n\}$.

Expanding n given above, we get

$$n = 2^N - 1,$$

$$n + 1 = 2^N.$$

So, $\bar{J} = \{0, n+1\}$.
Verifying: $b_i^{n+1} = b_i^n + b_{i+1}^n$.

$$\begin{aligned} b_i^n + b_{i+1}^n &= \sum_{j \in J} a_{j+i} + \sum_{j \in J} a_{j+i+1} \\ &= a_i + a_{i+n+1} \\ &= \sum_{j \in \bar{J}} a_{j+i} \\ &= b_i^{n+1}. \end{aligned}$$

Hence proved.

Case 3: When

$$n = \sum_{s=0}^{I-1} 2^s + \sum_{s=I+1}^{N} \alpha_s 2^S, 1 \leq I \leq N-2,$$

$$J = \{j = \sum_{s=I+1}^{N} \beta_s 2^s \mid \alpha_s = 0 \implies \beta_s = 0\}.$$

So,

$$n + 1 = 2^I + \sum_{I+1}^{N} \alpha_s 2^s, 1 \leq I \leq N-2,$$

$$\begin{aligned} \overline{J} &= \{j = \sum_{s=I}^{N} \beta_s 2^s | \alpha_s = 0 \implies \beta_s = 0, s > I\} \\ &= 2^I \beta_I + 2^{I+1} \beta_{I+1}, \ldots, 2^N \beta_N. \end{aligned}$$

So,

$$\overline{J} = J \cup J + 2^I.$$

Verifying: $b_i^{n+1} = b_i^n + b_{i+1}^n$

RHS:

$$b_i^n + b_{i+1}^n = \sum_{j \in J} a_{j+i} + \sum_{j \in J} a_{j+i+1}.$$

LHS:

$$b_i^{n+1} = \sum_{j \in \overline{J}} a_{j+i} = \sum_{j \in J} a_{j+i} + \sum_{j \in J+2^I} a_{j+i},$$

$$= \sum_{j \in J} a_{j+i} + \sum_{j \in J} a_{j+i+1}.$$

RHS=LHS, hence proved.

□

Corollary 3.5. *Let $A_0 = (a_i)$. Then*

$$A_{2^n} = (a_i + a_{i+2^n}).$$

Proof. $A_{2^n} = (b_i^{2^n})$, this falls in case 2, thus $\overline{J} = \{0, 2^n\}$, so

$$b_i^{2^n} = \sum_{j \in \overline{J}} a_{i+j} = a_i + a_{i+2^n}.$$

□

Definition 3.6. *A $k-$tuple $A = (a_i)$ and $B = (b_i)$, B is said to be inverse of A if $a_i + b_i \equiv 1 \bmod 2$ for $0 \leq i \leq k-1$. We will denote inverse of (a_i) by $(\hat{a_i})$.*

Lemma 3.7. *For (a_i), $\overline{(a_i)} = \overline{(\hat{a_i})}$ that is, successor of A and it's inverse is same.*

Proof. Let $A = (a_i)$ and $\hat{A} = (\hat{a_i})$ be the inverse of A, then $\overline{A} = (a_i + a_{i+1})$, similarly $\overline{\hat{A}} = (\hat{a_i} + \hat{a_{i+1}})$. Then

$$a_i + \hat{a_i} = 1 \bmod 2 \quad , \quad a_{i+1} + \hat{a_{i+1}} = 1 \bmod 2.$$

Adding both equations mod2, we get

$$a_i + a_{i+1} \bmod 2 = \hat{a_i} + \hat{a_{i+1}} \bmod 2,$$

$$\implies \overline{(a_i)} = \overline{(\hat{a_i})}.$$

□

Definition 3.8. *A $k-$tuple $A = A_0$ is called even tuple if $\sum_{i=0}^{k-1} a_i \equiv 0 \bmod 2$. A tuple that is not even called an odd tuple.*

Now we will proceed to characterize the successors of the $k-$tuple.

Lemma 3.9. *A tuple $A_0 = (a_i)$ is successor of $A_{-1} = (b_i)$ if and only if A_0 is an even tuple.*

Proof. $\implies$ Suppose A_0 is successor of A_{-1}, we will show A_0 is an even tuple. Now, $a_i = (b_i + b_{i+1}) \bmod 2$ indices mod$k$ then,

$$\sum_{i=0}^{k-1} a_i = \sum_{i=0}^{k-1}(b_i + b_{i+1}) = 2\sum_{i=0}^{k-1} b_i = 0 \bmod 2.$$

$\impliedby$ Suppose A_0 is even, we will construct predecessor A_{-1} of A_0 as follows:

$$A_0 = (a_0, a_1, \dots . a_{k-1}) \ \ , \ \ A_{-1} = (b_0, b_1, \dots . b_{k-1}).$$

$$\begin{aligned}
& b_0 = 1, \\
& b_j \equiv b_{j-1} + a_{j-1} \bmod 2, \quad 1 \leq j \leq k-1. \\
\implies & b_1 \equiv b_0 + a_0, \\
& b_2 \equiv b_1 + a_1 \equiv b_0 + a_0 + a_1, \\
& b_{k-1} \equiv b_0 + \sum_{i=0}^{k-2} a_i. \\
\text{since,} \quad & \sum_{i=0}^{k-1} a_i \equiv 0 \bmod 2 \implies a_{k-1} \equiv \sum_{i=0}^{k-2} a_i \bmod 2, \\
\text{so,} \quad & b_{k-1} \equiv b_0 + a_{k-1}.
\end{aligned}$$

Thus,

$$A_{-1} = (b_0, b_0 + a_0, b_0 + a_0 + a_1, \ldots, b_0 + a_{k-1}).$$

□

3.3 Generalized Even Tuples

Definition 3.10. *Let $A = (a_i)$ be a $k-$tuple, $k = 2^r k'$, where $k' > 1$ is odd is said to be r-even if*

$$\sum_{i=0}^{k'-1} a_{2^r i+j} \equiv 0 \bmod 2, \quad 0 \leq j \leq 2^r - 1. \tag{3.1}$$

For example, for $k = 14 = 2 \times 7$, then $A = (a_i)$ is $1-$even if

$$\sum_{i=0}^{7-1} a_{2^1 i+j} \equiv 0 \bmod 2, \quad 0 \leq j \leq 2^1 - 1.$$
$$\sum_{i=0}^{6} a_{2i+0} \equiv a_0 + a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12} \equiv 0 \bmod 2.$$
$$\sum_{i=0}^{6} a_{2i+1} \equiv a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} + a_{13} \equiv 0 \bmod 2.$$

Note: k odd, then $k-$tuple is $0-$even if and only if it is even.
In the following results, we will prove that the tuples in the cycle are $r-$even. To prove this, we need the following lemma.

Lemma 3.11. *Suppose $A_0 = (a_i)$ is $r-$ even $k-$tuple, where $k = 2^r k'$. Then A_0 have predecessor A_{-1}, which is $r-$even.*

Proof. First, Let $r = 0$ then $k = k'$ is odd, A_0 is $r-$even iff even, by lemma 3.9 we know even tuples have predecessor actually by lemma 3.7 there are two predecessors. We will show exactly one of them is *even.*
Suppose $B = (b_i)$ and $\hat{B} = (\hat{b_i})$ are predecessor of A_0 and B is not even. Then

$$\sum_{i=0}^{k'-1} b_i \equiv 1 \bmod 2.$$

$$\text{Since,} \quad b_i + \hat{b_i} \equiv 1 \bmod 2,$$
$$\implies \hat{b_i} \equiv 1 + b_i,$$
$$\implies \sum_{i=0}^{k'-1} \hat{b_i} \equiv 1 + \sum_{i=0}^{k'-1} b_i \equiv 1 + 1 \equiv 0 \bmod 2, \quad \text{k' is odd.}$$

Next, suppose $r > 0$, For existence of predecessor of A_0, first we will show that A_0 $r-$even implies it is even.

As given, A_0 is $r-$even $\implies$ equation 3.1 holds. Let

$$\sigma_j^{A_0} \equiv \sum_{i=0}^{k'-1} a_{2^r i+j}.$$

Since, for each $0 \leq j \leq 2^r - 1$ $\sigma_j^{A_0} \equiv 0 \bmod 2$, adding all $\sigma_j^{A_0}$ varying $0 \leq i \leq k' - 1$ will give $\sum_j^{2^r k'-1} a_j \equiv 0 \bmod 2$. Thus A_0 is even. Suppose $B = (b_i)$ and $\hat{B} = (\hat{b_i})$ are predecessor of A_0 that are inverse of each other. We will show one of them is $r-$even. Let

$$\sigma_j^B \equiv \sum_{i=0}^{k'-1} b_{2^r i+j}, \quad 0 \leq j \leq 2^r - 1.$$

Now, $a_i = b_i + b_{i+1}$, we will show $\sigma_j^B \equiv 0$ for all j,

$$\sigma_0^B + \sigma_1^B = \sum_{i=0}^{k'-1} (b_{2^r i} + b_{2^r i+1}),$$
$$= \sum_{i=0}^{k'-1} a_{2^r i} = \sigma_0^{A_0} \equiv 0 \bmod 2.$$

Thus, either

$$(1) \quad \sigma_0^B \equiv \sigma_1^B \equiv 0,$$

or

$$(2) \quad \sigma_0^B \equiv \sigma_1^B \equiv 1.$$

If we define $\sigma_0^{\hat{B}} \equiv \sum_{i=0}^{k'-1} \hat{b}_{2^r i+j}$, if $\sigma_0^B = 1$, since

$$\sigma_0^{\hat{B}} = \sum_{i=0}^{k'-1} \hat{b}_{2^r i} = \sum_{i=0}^{k'-1} b_{2^r i} + 1 \equiv 0 \bmod 2.$$

Thus one of them is 0. WLOG Assume $\sigma_0^B \equiv \sigma_1^B \equiv 0$.
In the same fashion $\sigma_1^B + \sigma_2^B = \sigma_0^{A_0} \equiv 0 \bmod 2$ as $\sigma_1^B \equiv 0 \implies \sigma_2^B \equiv 0$. Thus for all $0 \leq j \leq 2^r - 1$ $\sigma_j^B \equiv 0$.
Thus, $B = (b_i)$ is $r-$even, but its inverse $\hat{B}$ is not. □

Theorem 3.12. *Suppose $k = 2^r k'$, where k' is odd greater than one. A $k-$tuple is in a repeating cycle if and only if it is $r-$even.*

Proof. $\Longrightarrow$ Suppose A_0 is $r-$even, we will construct a repeating cycle in which A_0 is contained. By Lemma 3.11 it has predecessor A_{-1} which is also $r-$even. Similarly A_{-1} has predecessor A_{-2} which is also $r-$even, and so forth. As there are only a finite number of $r-$even $k-$tuples, there exist smallest n such that $A-n = A_{-j}$ where $0 \leq j \leq n-1$. Then $A_{-n}, A_{-n+1}, \ldots, A_{-j-1}$ is a repeating cycle. But $\overline{A_{-j-1}} = A_{-j}$, thus eventually, we get

$$\begin{aligned} &A_{-n} = A_{-j} \implies \overline{A_{-n}} = \overline{A_{-j}}, \\ &A_{-n+1} = A_{-j+1}. \end{aligned}$$

Thus, we get $A_{-n+j} = A_0$, $(-n+j \neq 0)$, which forms a repeating cycle.

$\Longleftarrow$ Suppose $A_0 = (a_i)$ is in a repeating cycle, then there exists

$$A_0, A_{-1}, A_{-2}, \ldots, A_{-2^r},$$

where A_i need not be different. Let $A_{-2^r} = (b_i)$. By corollary 3.5, we get

$$a_j = b_j + b_{j+2^r}.$$

Thus,

$$\begin{aligned}\sum_{i=0}^{k'-1} a_{2^r i+j} &\equiv \sum_{i=0}^{k'-1}(b_{2^r i+j} + b_{2^r(i+1)+j}),\\ &= 2\sum_{i=0}^{k'-1} b_{2^r i+j} \equiv 0 \bmod 2.\end{aligned}$$

So, A_0 is $r-$even. □

Theorem 3.13. *Suppose $k = 2^r k'$, $k' > 1$ is odd, $r \geq 0$. Let m be the order of 2 in $(\mathbb{Z}/k'\mathbb{Z})^*$. Then the maximum length of any cycle is $2^r(2^m - 1)$. If a cycle has length l then $l|2^r(2^m - 1)$.*

Proof. Given that $2^m \equiv 1 \bmod k'$, we get

$$\begin{aligned}2^m = 1 + r.k' &\implies 2^{m+r} = 2^r + r.(2^r k')\\ &\implies 2^{m+r} \equiv 2^r \bmod k.\end{aligned}$$

By corollary 3.5, since indices are mod$k$

$$A_{2^{m+r}} = (a_i + a_{i+2^{m+r}}) = (a_i + a_{i+2^m}) = A_{2^r}.$$

Thus, the period is $2^r(2^m - 1)$.
The maximum period say $p(k)$ upto multiplicity is $2^r(2^m-1)$. Since every l repeating cycle for given $k-$tuple will be multiple of it thus, $l|2^r(2^m - 1)$.

□

Chapter 4

Period of Ducci Sequences

This chapter mainly deals with the period of *Ducci sequence*. We will derive an explicit formula for the period of the *Ducci sequences*.

4.1 Maximal period

When *Ducci* sequence is periodic, it has already been proved that the component of every tuple in the sequence is either 0 or a constant C. Also, for any positive λ, $D(\lambda A) = \lambda D(A)$. Thus WLOG let $\lambda = 1$ i.e. we will restrict to $n - tuple$ with components from $\{0, 1\}$.

Definition 4.1. The *Ducci* sequence that starts with $n-$tuple $(0, \ldots, 0, 1)$ is called a basic *Ducci* sequence, period of this sequence is denoted by $P(n)$.

Theorem 4.2. *For any n, the basic Ducci sequence has a maximum period among given $n-tuples$. The period of other sequences divides this maximum.*

Proof. As given for $A_1 = (0, 0, \ldots, 1)$, there exist smallest R and S such that $D^R(A_1) = D^S(A_1)$ and $P(n) = S - R$. Since we are dealing $n-$tuples in $\mathbb{Z}_2$, $D = I + H$, where H is invertible left shift map.
Claim: $D^R(H(A_1)) = D^S(H(A_1))$, that is period remains same for the n-tuple obtained by left shift.

Proof: Firstly

$$\begin{aligned}
& D \circ H = H \circ D, \\
& D \circ H = (I + H) \circ H = I \circ H + H \circ H = H \circ D \\
\Longrightarrow\ & D^R \circ H = D^{R-1}(D \circ H) = D^{R-1}(H \circ D), \\
\Longrightarrow\ & D^R \circ H = H \circ D^R \ \text{ similarly } \ D^S \circ H = H \circ D^S.
\end{aligned}$$

But, given that for basic Ducci sequence $D^R(A_1) = D^S(A_1)$ then,

$$\begin{aligned}
D^R(H(A_1)) &= H(D^R(A_1)) \\
&= H(D^S(A_1)) \\
&= D^S(H(A_1)).
\end{aligned}$$

Also, $H^n(A_1) = A_1$. Any general primitive n-tuple can written as:

$$A = c_1A_1 + c_2A_2 + \cdots + c_nA_n,$$

where $A_i = H^i(A)$ and $c_i \in \{0, 1\}$. Using the fact that D is a linear operator on $\mathbb{Z}_2$ we have

$$\begin{aligned}
D^R(A) &= c_1D^R(A_1) + c_2D^R(A_2) + \cdots + c_nD^R(A_n) \\
&= c_1D^S(A_1) + c_2D^S(A_2) + \cdots + c_nD^S(A_n) \\
&= D^S(A).
\end{aligned}$$

The period of any general $n-$tuple is bounded by $P(n)$. ■ □

4.2 Upper Bounds for P(n)

In this section, we will give results for $n-$tuple $A = (0, 0, \ldots, 1)$, i.e., results for basic *Ducci* sequence.

Lemma 4.3. *If* $2^m \equiv t \bmod (n)$, *then* $D^{2^m} = I + H^t$.

Proof. In $\mathbb{Z}_2$, $(I + H)^{2^m} = I + H^{2^m}$ since $H^n = I$ for $n-$tuple. so $H^{2^m} = H^t$, where $2^m \equiv t \bmod (n)$. □

Corollary 4.4. *If n is power of 2, then Ducci sequence have $(0, 0, \dots, 0)$.*

Proof. From Lemma 4.3, since n is the power of 2, give $t = 0$. $D^{2^m} = I + I = 2I \equiv 0 \bmod 2$. □

Corollary 4.5. *If n is not the power of 2, then the cycle of basic Ducci sequence consists of a tuple with exactly two 1's.*

Proof. Choose any m large enough such that D^{2^m} is in the periodic part of *Ducci* sequence. As given, n is not the power of 2; thus, $t \neq 0$. $D^{2^m}(0, 0, \dots, 1) = (0, 0, \dots, 1) + H^t(0, 0, \dots, 1)$ adding both give a tuple have exactly two 1's. □

Corollary 4.6. *If $2^m \equiv 1 \bmod n$, then $P(n)|2^m - 1$.*

Proof. By Lemma 4.3, $D^{2^m} = I + H = D$; thus $P(n)|2^m - 1$. □

Theorem 4.7. *If $2^M \equiv -1 (\mathrm{mod} n)$, then $P(n)$ divides $n(2^M - 1)$.*

Proof.

$$\begin{aligned} D^{2^M} &= I + H^{-1} \\ &= H^{-1}(I + H) = H^{-1}D \\ &= D^{(n2^M)} = H^{-n}D^n = D^n. \end{aligned}$$

So, $P(n)|n(2^M - 1)$. □

Abbreviations

- For an odd $n > 1$, Let $m(n)$ be the order of 2 in multiplicative group $(\mathbb{Z}/\mathbb{Z}_n)^*$.
- If for an odd $n > 1$, there is an M such that $2^M \equiv -1 \bmod n$, then n is said to be with "$a - 1$". Smallest such M is $m(n)/2$. If it does not occur, then n is said to be "without $a - 1$".

Results

- For every odd n, "without $a - 1$" from 7 to 165 except 95, $P(n) = 2^{m(n)} - 1$.
- For every odd n, with "$a - 1$" from 3 to 163 except 37 and 101, $P(n) = n(2^{m(n)/2} - 1)$.

4.3 More Properties of P(n)

Theorem 4.8. *If n is not power of 2, then $n|P(n)$.*

Proof. For a given $A = (a_1, a_2, \ldots, a_n)$, $A \in \mathbb{Z}_2^n$. Construct a regular $n-$gon and write the component of A on the $n-$gon's vertices.

Now, If a regular $n-$gon constructed by A has an axis of symmetry, that means there exists index i such that for entry x_i

$$x_{(i+N) \bmod n} = x_{(i-N) \bmod n}.$$

Call such i as an axis of point.

For example $A = (0, 0, 0, 1, 1)$, here $i = 2$, so $x_{(2+N) \bmod 5} = x_{(2-N) \bmod 5}$, this can also can be seen in figure 4.1, blue line is the axis of symmetry.

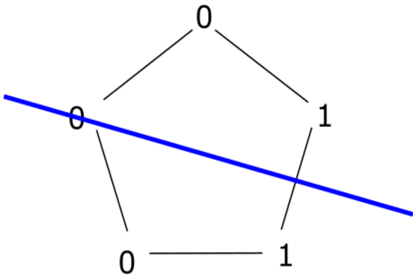


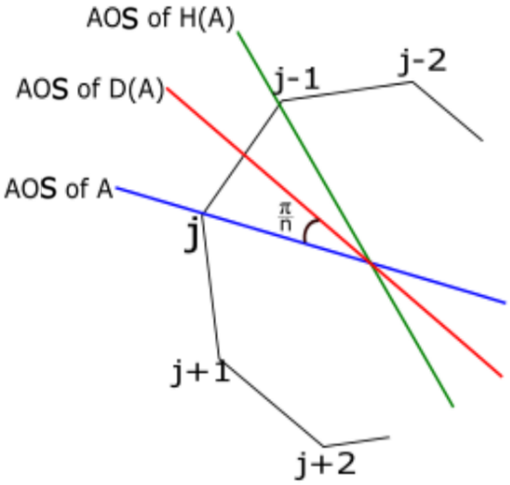
Figure 4.1:

<u>Claim:</u> If A has an axis of symmetry, then $D(A)$ also does, and its axis of symmetry is obtained by rotating the axis of symmetry(AOS) of A by $\frac{-180°}{n}$ (clockwise -ve direction).

<u>Proof:</u> With the help of the figure 4.3, we can observe that if A has an axis of the point at jth position, then $H(A)$ has an axis of the point at $j-1$th position or AOS of $H(A)$ is obtained from the AOS of A by a shift of $-\frac{2\pi}{n}$ angle.

Now let $D(A) = (b_1, b_2, \ldots, b_n)$, where $b_i = a_i + a_{i+1}$.

We will show that AOS of $D(A)$ passes as bisector of AOS of A and AOS of $H(A)$ that is,



$b_j = b_{j-1}$, $b_{j+1} = b_{j-2}$ or in general for odd n,

$$b_{j-(i+1)} = b_{j+i}, \quad 0 \leq i \leq \frac{n-1}{2} - 1.$$

on RHS

$$\begin{aligned} b_{j-(i+1)} &= a_{j-(i+1)} + a_{j-(i+1)+1} \\ &= a_{j-(i+1)} + a_{j-i}. \end{aligned}$$

on LHS

$$\begin{aligned} b_{j+i} &= a_{j+i} + a_{j+i+1} \\ &= a_{j+(i+1)} + a_{j+i}. \end{aligned}$$

Since j is the axis of point for A, So $a_{j-i} = a_{j+i}$ and $a_{j-(i+1)} = a_{j+(i+1)}$. Thus $b_{j-(i+1)} = b_{j+i}$.
For even n same equation holds but $0 \leq i \leq \frac{n}{2} - 1$.
So, the AOS of $D(A)$ is obtained from A's AOS by shifting it to angle $-\frac{180°}{n}$. ■

With the help of this claim and result from corollary 4.5 in the cycle of basic *Ducci* sequence, there is an $n-$tuple with exactly two 1 and having one AOS, so does all the tuples in repeating cycle.
Now, given n not power of 2, Let R and S, $R > S$ be the positive integer such that $D^R(A) = D^S(A)$ and $P(n) = S - R$.

To reach the Rth iterate, AOS is rotated to angle $-R\frac{180^\circ}{n}$ with respect to that of A. Similarly, reaching Sth iterate, AOS is rotated to angle $-S\frac{180^\circ}{n}$ with respect to that of A.

As $D^R(A) = D^S(A)$ their AOS is differ by multiple of 180°,

$$-R\frac{180^\circ}{n} = -S\frac{180^\circ}{n} + 180^\circ,$$

$$180^\circ\left(\frac{S-R}{n}\right) = 180^\circ$$

$$\implies n|S-R$$

$$\implies n|P(n).$$

□

For the following results, we will write $n-$tuple as a matrix. This matrix doesn't represent any kind of linear transformation. It is another way to study the *Ducci* sequences. Each row and column of this matrix is considered as tuples on their own based on that, we will define the new operation as follows:

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

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

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

These operations can be summarised as follows:

- $H_L(A)$: Each row is replaced by H(row).
- $H_C(A)$: Each column is replaced by H(column).
- $D_L(A)$: Each row is replaced by D(row).
- $D_C(A)$: Each column is replaced by D(column).

Theorem 4.9. *For $n = 2^m k$, where $k > 1$ is odd, then $P(n) = 2^m P(k)$.*

Proof. Write $A_1 = (0, 0, \dots, 1)$ in form of $k \times 2^m$ matrix, thus each row of A_1 has 2^m components. A_1 is one of the cases of A, By the above-defined operation, we can observe that $H^{2^m}(A) = H_c(A)$, Now this holds for D also as

$$D^{2^m}(A) = (I + H)^{2^m}(A) = I(A) + H^{2^m} = I + H_c(A) = D_c(A). \tag{4.1}$$

Writing basic tuple in the form of a matrix:

$$A_1 = \begin{bmatrix} 0 & \dots & 0 & 0 \\ . & \dots & 0 & 0 \\ . & \dots & 0 & 0 \\ 0 & \dots & 0 & 1 \end{bmatrix}.$$

We will focus on operation $D_c(A_1)$. For matrix, A_1 considering each column as an individual tuple apply $D_c(A_1)$ means that each column in itself forms a basic *Ducci* sequence, but except the last column, all are zero. The last column is $k-$tuple. Assume its period is $P(k)$. That is, its orbit is

$$A, D_c(A_1), D_c^2(A_1), ..., D_c^{P(k)}(A_1) = A_1,$$

by (4.1), $D^{2^m}(A_1) = D_c(A_1) \implies D^{2^m P(k)}(A_1) = D_c^{P(k)}(A_1) = A_1$, thus period of entire sequence is $2^m P(k)$. □

Theorem 4.10. *If $k|n$, then $P(k)|P(n)$.*

Proof. From Theorem 4.2, the maximal period of *Ducci* sequence of $n-$tuple is $P(n)$ and the period of other sequences divide $P(n)$.

Thus, it is sufficient to find a $n-$tuple having a period $P(k)$. We claim that $n/k \times k$ matrix

$$\begin{bmatrix} 0 & \dots & 0 & 1 \\ . & \dots & 0 & 1 \\ 0 & \dots & 0 & 1 \end{bmatrix}$$

have period $P(k)$.

The above matrix is a special case of A where all rows are equal to each other, $H(A) = H_L(A)$ then $D(A) = D_L(A)$, but each row in itself having length k form a basic *Ducci* sequence by operation $D_L(A)$. Assume its period is $P(k)$, as $D(A) = D_L(A) \implies D^{P(k)}(A) = D_L^{P(k)}(A) = A$. Hence, its period is $P(k)$. $\square$

Chapter 5

Periodic Orbits of Ducci Sequences

5.1 Limit Points

This chapter will primarily discuss the eventual behavior of *Ducci sequence* obtained by iteratively applying *Ducci map.* To study this, we will slightly change the notion. Let n be the length of the vector $\mathbf{a} = \mathbf{a}(0) = [a_1(0), a_2(0), \ldots, a_n(0)] \in \mathbb{R}^n$ and $\mathbf{a}(t) = [a_1(t), a_2(t), \ldots, a_n(t)]$, denote $a(t) = D^t(a)$ be the $t-$th iterate of D, where $a_i(t+1) = |a_i(t) - a_{i+1}(t)|$.
We already observed that for any vector $a = [a_1, a_2, \ldots, a_n]$. We set $|a| = \max_{1 \leq i \leq N} |a_i|$,

$$|D(a)| \leq |a|.$$

This imply that for each $a \in \mathbb{R}^n_+$ the whole sequence contained in compact set

$$b \in \mathbb{R}^n_+ : |b| \leq |a|,$$

By the *Bolzano Weirstrass theorem*, every bounded sequence in $\mathbb{R}^n_+$ has a convergent subsequence. Hence the *Ducci sequence* of a has a limit point.
To prove the main theorems, we will need a few lemmas.

Lemma 5.1. *Let $p = [p_1, p_2, \ldots, p_n] \in \mathbb{R}^n_+$, $1 \leq k \leq n$ and*

$$0 < p_k < |p|,$$

Then

$$|p(n-1)| < |p|.$$

Proof. To begin with, we claim that for every iteration $i \geq 0$ with $|\mathbf{p}(i)| = |\mathbf{p}|$ there exist integers $j_i^{\pm}$ with the following properties:

$$\jmath_i^+ \geq 0 \;\;,\;\; \jmath_i^- \leq -i, \tag{5.1}$$

$$0 \leq p_{k+j}(i) < |p| \quad \text{for} \;\; j \in (j_i^-, j_i^+), \tag{5.2}$$

$$0 < p_{k+j_i^{\pm}}(i) < |p|. \tag{5.3}$$

We will prove this claim by induction, for $i = 0$, take $j_0^{\pm} = 0$.
Now assume that claim is true for certain i, i.e. $|p(i)| = |p| \implies$ there exist $j_i^+ \geq 0$ and $j_i^- \leq -i$ such that $0 < p_{k+j_i^{\pm}}(i) < |p|$. We may assume WLOG that j_i^+ and j_i^- are the greatest and least integer respectively satisfying (5.1) to (5.3). So,

$$p_{k+j_i^{\pm}\pm 1}(i) \in \{0, |p|\}. \tag{5.4}$$

For $|p(i+1)| = |p(i)|$, we need to find existence of $j's$ satisfy above equations. In that direction, take

$$j_{i+1}^+ = j_i^+ \;\;,\;\; j_{i+1}^- = j_i^- - 1.$$

Now checking the (5.1) to (5.3)
For (5.1), we get $j_{i+1}^+ = j_i^+ \geq 0$ and $j_{i+1}^- = j_i^- - 1 \leq -i - 1$.
Moreover, if $j \in (j_{i+1}^-, j_{i+1}^+) = [j_i^-, j_i^+)$ we have,

$$p_{k+j}(i+1) = |p_{k+j+1}(i) - p_{k+j}(i)| < |p|.$$

This inequality is true because $p_{k+j+1}(i) \in \{0, |p|\}$ and $0 < p_{k+j}(i) < |p|$ this is how we defined the indices $j's$ in case of $p(i)$. Same argument will satisfy (5.3) considering the end values of $j_i^{\pm}$

$$p_{k+j_{i+1}^{\pm}}(i+1) = \left| p_{k+j_{i+1}^{\pm}}(i) - p_{k+j_i^{\pm}}(i) \right| \in (0, |p|).$$

Thus, we complete the proof of the claim.
Our main result is to prove that $|p(n-1)| < |p|$.
On contrary assume that $|p(n-1)| = |p|$ by (5.1), for $i = n-1$, there exists $j^+_{n-1} \geq 0$ and $j^-_{n-1} < n-1$ such that (5.3) holds.

$$0 \leq p_{k+j}(n-1) < |p| \;\; \forall j \in [j^-_{n-1}, j^+_{n-1}].$$

But for the interval $[j^-_{n-1}, j^+_{n-1}]$, when we vary j, it will cover the every element of the tuple because, in total, there are n choices for j, giving the result that $|p(n-1)| < |p|$, which is a contradiction. □

Next, Lemma will give the description of a limit point of *Ducci Sequence.*

Lemma 5.2. *If $\boldsymbol{p} = [p_1, p_2, \ldots, p_n]$ is the limit point of the sequence then*

$$\mathit{Card}(\{p_1, p_2, \ldots, p_n\} \setminus \{0\}) \leq 1.$$

As a result, the limit point is a multiple of a primitive cycle.

Proof. Let $\mathbf{a} \in \mathbb{R}^+_n$. As $|D(a)| \leq |a|$, that means the sequence $|a(t)|$ is non increasing sequence in $\mathbb{R}$, So therefore the limit

$$c = \lim_{t\to\infty} |a(t)|, \tag{5.5}$$

exists. Now, Assume that

$$\text{Card}(\{p_1, p_2, \ldots, p_n\}) \geq 2, \tag{5.6}$$

and

$$p = \lim_{k\to\infty} a(t_k). \tag{5.7}$$

For some sequence $t_k \to \infty$. Since $\mathbf{p} \in \mathbb{R}^n$ by our assumption, from (5.1),

$$|D^{n-1}(p)| < |p| = c. \tag{5.8}$$

As, D is a continuous map 8.30, then from (5.7), after $n-1$ application of D we have

$$\lim_{k\to\infty} a(t_{k+n-1}) = D^{n-1}(p). \tag{5.9}$$

Supremum is a continuous map, according to (5.9) $\lim_{k\to\infty} |a(t_{k+n-1})| = c$, but $|D^{n-1}(p)| < c$, which is a contradiction. □

Lemma 5.3. *If* $\boldsymbol{e} = [\epsilon_1, \epsilon_2, \ldots, \epsilon_n] \in \mathbb{Z}_2^n$ *and* $2^\nu || n$ *(*2 *properly divides* n*) then,*

$$1 + x^{2^\nu} \mid \sum_{i=1}^{n} \epsilon_i(2^\nu) x^{i-1} (\text{mod} 2\ ).$$

Proof. All calculation will be done in mod2, So that $-x \equiv x \bmod 2$, indices in mod n

$$\begin{aligned}\sum_{i}^{n} \epsilon_i(t+1)x^i &\equiv \sum_{i=1}^{n} (\epsilon_i(t) + \epsilon_{i+1}(t))x^i \bmod 2 \\ &\equiv \sum_{i=1}^{n} \epsilon_i(t)x^i + \epsilon_1(t) + \epsilon_1(t) + \sum_{i=1}^{n} \epsilon_{i+1}(t)x^i \bmod 2 \\ &\equiv (1+x)\sum_{i=1}^{n} \epsilon_i(t)x^{i-1} + \epsilon_1(t)(1+x^n) \bmod 2.\end{aligned}$$

Now, we already know,

$$\begin{aligned}&(1+x)^{2^\nu} \equiv 1 + x^{2^\nu} \bmod 2. \\ &\text{As } \ 2^\nu || n \implies n = 2^\nu k, \quad k > 1. \\ &(1+x)^{2^\nu} | (1+x)^{2^\nu k} \implies (1+x^{2^\nu}) | (1 + x^{2^\nu k}) \bmod 2 \\ &(1+x^{2^\nu}) | (1+x^n) \bmod 2.\end{aligned}$$

so,

$$x\sum_{i}^{n} \epsilon_i(t+1)x^{i-1} \equiv (1+x)\sum_{i=1}^{n} \epsilon_i(t)x^{i-1} \bmod (2, 1 + x^{2^\nu}).$$

Take $t = 0, t = 1, \ldots, t = j-1$. By recursive relation of above equation we get

$$x^j \sum_i^n \epsilon_i(t+1)x^{i-1} \equiv (1+x)^j \sum_{i=1}^n \epsilon_i(0)x^{i-1} \bmod (2, 1+x^{2^\nu}).$$

By taking $j = 2^\nu$,

$$x^{2^\nu} \sum_i^n \epsilon_i(t+1)x^{i-1} \equiv (1+x^{2^\nu}) \sum_{i=1}^n \epsilon_i(0)x^{i-1} \equiv 0 \bmod (2, 1+x^{2^\nu}).$$

But on RHS, $x^{2^\nu} \not\equiv 0 \bmod (2, 1+x^{2^\nu})$, so $\sum_i^n \epsilon_i(t+1)x^{i-1} \equiv 0 \bmod (1+x^{2^\nu})$. □

Based on the previous three Lemmas, we will prove an important theorem describing the limit point of *Ducci sequence.*

Theorem 5.4. *For every vector in $a \in \mathbb{R}^n$ and limit point p of the sequence $a(t)$ we have,*

1. *$p = ce$, where $c = \lim_{t\to\infty} |a(t)|$ and $\mathbf{e} = [\epsilon_1, \epsilon_2, \ldots, \epsilon_n] \in \{0,1\}^n$.*
2. $$1 + x^{2^\nu} | \sum_{i=1}^n \epsilon_i x^{i-1} (\text{mod} 2), \ \textit{where} \ 2^\nu || n. \tag{5.10}$$

Proof. From first part, we obtained that $c = \lim_{t\to\infty} |a(t)|$ exist and proof follows from Lemma 5.2.

Denote

$$P = \{ce \ : \ e = [\epsilon_1, \ldots, \epsilon_n] \in \{0,1\}^n\},$$
$$Q = \{ce \ : \ e = [\epsilon_1, \ldots, \epsilon_n] \in \{0,1\}^n \ \text{ and } \ 5.10 \ \text{ holds.}\}$$

Since $D(cv) = cD(v)$ for all $v \in \mathbb{R}^n$, Also for any $u \in P$ from lemma 5.3 we get

$$D^{2^\nu}(P) \subset Q. \tag{5.11}$$

The whole sequence $a(t)$ lies in compact set also $\lim_{t\to\infty} |a(t)|$ exist we have,

$$\lim_{t\to\infty} (\min_{p\in P} |a(t) - p|) = 0.$$

By continuity of D map and equation 5.11 we get

$$\lim_{t\to\infty}(\min_{\mathbf{p}\in Q}|a(t)-p|)=0.$$

Therefore, all limit points of the sequence $a(t)$ lie in Q. □

Corollary 5.5. *If $n = 2^\nu$, the only vector e that satisfy Lemma 5.3 condition is $e = [0, 0, \ldots, 0]$.*

Theorem 5.6. *If $a = ce$, where $c \in \mathbb{R}_+$ and $e = [\epsilon_1, \epsilon_2, \ldots, \epsilon_n] \in \{0, 1\}^n$ and satisfy equation 5.10 then $a(N) = a$ for some $N > 0$, i.e. the orbit of a is periodic.*

Proof.

$$Q = \{ce \ : \ e = [\epsilon_1, \ldots, \epsilon_n] \in \{0, 1\}^n \text{ and } 5.10 \text{ holds}\}.$$

Set Q is finite, we will prove that $D : Q \to Q$ is a surjective map.
From the proof of lemma 5.3, we can deduce that $D(Q) \subset Q$. As D is also a linear transformation on Q. We will show that it is an injective map by *Rank-Nullity theorem* we will get the desired result.
Let $e = [\epsilon_1, \ldots, \epsilon_n]$ and $d = [\delta_1, \ldots, \delta_n]$ belong to Q such that $e \neq d$. On the contrary to *one-one*, assume that $D(e) = D(d)$, then for each indices i we have

$$\epsilon_i + \epsilon_{i+1} = \delta_i + \delta_{i+1}.$$

So, $\epsilon_i = \delta_i$ iff $\epsilon_{i+1} + \delta_{i+1}$. We assumed that $e \neq d$ so for some j we have $\epsilon_j \neq \delta_j$ by induction we have $\epsilon_i \neq \delta_i$ for all i. From result 5.10 for $e, d \in Q$ and we have

$$1 + x^{2^\nu} \mid \sum_{i=1}^{n} \epsilon_i(2^\nu)x^{i-1}(\mathrm{mod}2\ ) \quad , \quad 1 + x^{2^\nu} \mid \sum_{i=1}^{n} \epsilon_i(2^\nu)x^{i-1}(\mathrm{mod}2\ ).$$

Since $\epsilon_i, \delta_i \in \{0, 1\}^n$ and also not equal, we have $\epsilon_i + \delta_i = 1\ \forall\ i$, so adding above equation we have,

$$1 + x^{2^\nu} \mid \sum_{i=1}^{n} x^{i-1}(\mathrm{mod}2\ ).$$

Choose $n = 2^\nu m, \;\; m > 1$. As

$$\sum_{i=1}^{n} x^{i-1} = 1 + x + x^2, \ldots, +x^{n-1} = \frac{1+x^n}{1+x}(\text{mod} 2).$$

$$\implies (1 + x^{2^\nu})(1+x) \mid 1 + x^{2^\nu m}.$$

Now, consider

$$\sum_{i=1}^{m-1} x^{j2^\nu} = \frac{1 + x^{2^\nu m}}{1 + x^{2^\nu}}(\text{mod} 2).$$

Thus

$$1 + x \mid \sum_{i=1}^{m-1} x^{j2^\nu} \bmod 2.$$

For $x = 1$ denominator is even, but the numerator is odd as m is odd, which is a contradiction. So D is one-one, D is surjective on Q. □

Chapter 6

Lower Bounds For Periods of Ducci Sequences

6.1 Multiplicative orders and partitions

In chapter 4, we derived lower bound for $P(n)$ that depends on nature of n, whether it is *"with* $a-1$" or *"without* $a-1$". In this chapter, we will use finite field theory to prove new asymptotic lower bounds for $P(n)$. As we have proved that for $n = 2^m k$, $P(n) = 2^m P(k)$, thus we always take n to be an odd integer.
Let $1 \leq a < n$ be an integer prime to n.
Let t be the order of 2 in $(\mathbb{Z}/n\mathbb{Z})^*$. Then $\mathbb{F}_{2^t}$ is the finite field of charaterstic 2. Consider the coset $a < 2 > \subseteq (\mathbb{Z}/\mathbb{Z}_n)^*$ of the multiplicative group $< 2 >$ generated by 2 in the residue ring modulo n, that is

$$S_{a,n} := \{j \in \mathbb{Z}_{>0} : j \in (\mathbb{Z}/\mathbb{Z}_n)^*, \exists\, e_j \in \mathbb{Z}_{\geq 0}, j \ \equiv a2^{e_j} \bmod n\}.$$

For a given a, $S_{a,n}$ is the coset having cardinality $\#S_{a,n} = t$, where $t = | < 2 > |$. Next, consider the set of partitions of numbers $\leq t-1$ into distinct parts from $S_{a,n}$: that is;

$$\mathcal{P}_{a,n} := \{(u_j)_{j\in S_{a,n}} \in \{0,1\}^t : \sum_{j\in S_{a,n}} ju_j \leq t-1\}.$$

Theorem 6.1. *For odd n and $a \in (\mathbb{Z}/\mathbb{Z}_n)^*$, then $P(n) \geq \#\mathcal{P}_{a,n}$.*

Proof. We will use the following fact from [8] in this proof: $P(n)$ is the lowest common multiple of the multiplicative orders of $\zeta + 1$, where $\zeta \neq 1$ ranges over all nth roots of unity $\zeta \in \mathbb{F}_{2^t}$.

Let $\zeta \in \mathbb{F}_{2^t}$ be the primitive nth root of unity. Our Idea is to show that every partition in $\mathcal{P}_{a,n}$ leads to the distinct value of $\zeta+1$. This implies that the cardinality of set $\#\mathcal{P}_{a,n}$ is not more than the order of $\zeta+1$.

The existence of such ζ to be primitive comes from the fact that $\mathbb{F}^*_{2^t}$ is cyclic also, $\zeta^n = 1 \iff n|2^t-1$, but such condition follows from the fact that $t := ord_{(\mathbb{Z}/\mathbb{Z}_n)^*}(2)$

Let $u = (u_j)_{j\in S_{a,n}} \in \mathcal{P}_{a,n}$ and set

$$\mathcal{Q}_u = \sum_{j\in S_{a,n}} ju_j,$$

where $j \equiv a2^{e_j} \bmod n$. Now

$$(\zeta+1)^{\mathcal{Q}_u} = (\zeta+1)^{\sum_{j\in S_{a,n}} ju_j}$$

$$= \prod_{j\in S_{a,n}} (\zeta+1)^{u_j 2^{e_j}} = \prod_{j\in S_{a,n}} ((\zeta+1)^{2^{e_j}})^{u_j}.$$

As above expression can be considered a polynomial in $\mathbb{F}_{2^t}$ having characteristic 2, so $(\zeta+1)^{2^{e_j}} = \zeta^{2^{e_j}} + 1$ from 8.31. Then

$$(\zeta+1)^{\mathcal{Q}_u} = \prod_{j\in S_{a,n}} (\zeta^{2^{e_j}} + 1)^{u_j}.$$

Also, choose an integer b such that $ab \equiv 1 \bmod n$ that is b is inverse of a.

As $j \equiv a2^{e_j} \bmod n$. Multiply both sides by b gives $bj \equiv 2^{e_j} \bmod n$. Then

$$(\zeta+1)^{\mathcal{Q}_u} = \prod_{j\in S_{a,n}} (\mathcal{V}^j + 1)^{u_j},$$

where $\mathcal{V} = \zeta^b \in \mathbb{F}_{2^t}$.

Claim: $\mathcal{V} = \zeta^b$ is primitive and nth root of unity.
Proof: To show ζ^b is primitive we need to show that $gcd(b, 2^t - 1) = 1$.
As $n|2^t - 1 \implies n = K(2^t - 1)$ for some constant K. We choose b as inverse of a in multiplicative group $(\mathbb{Z}/\mathbb{Z}_n)^*$ that means $gcd(b, n) = 1$, then $gcd(b, 2^t - 1) = 1$.
$\mathcal{V}$ is also nth root of unity as from the theory of finite fields we know

$$ord(\zeta^b) = \frac{ord(\zeta)}{gcd(b, n)} = n.$$

So, we proved that $\mathcal{V}$ is also the primitive nth root of unity. ■

By taking another partition $v = (v)_{j \in S_{a,n}} \in \mathcal{P}_{a,n}$ different from u, and doing the same procedure we get

$$(\zeta + 1)^{\mathcal{Q}_v} = \prod_{j \in S_{a,n}} (\mathcal{V}^j + 1)^{v_j}.$$

On the contrary, suppose that both partitions give the same value when raised to the power of $\zeta + 1$, that is

$$(\zeta + 1)^{\mathcal{Q}_u} = (\zeta + 1)^{\mathcal{Q}_v}.$$

or

$$\prod_{j \in S_{a,n}} (\mathcal{V}^j + 1)^{u_j} = \prod_{j \in S_{a,n}} (\mathcal{V}^j + 1)^{v_j}.$$

Let $f(X) \in \mathbb{F}_2[x]$ be the minimal polynomial of $\mathcal{V}$. Since $\mathcal{V}$ is primitive; $f(X)$ is of degree t. Then $f(X)$ must divide $U(X) - V(X)$, where

$$U(X) = \prod_{j \in S_{a,n}} (X^j + 1)^{u_j} \quad \text{and} \quad V(X) = \prod_{j \in S_{a,n}} (X^j + 1)^{v_j}$$

Since $u, v \in \mathcal{P}_{a,n}$, we have $\sum_{j \in S_{a,n}} ju_j \leq t - 1$ and $\sum_{j \in S_{a,n}} jv_j \leq t - 1$, thus the degree of $U(X)$ and $V(X)$ is $\leq t - 1.$, which is less than the degree of minimal polynomial $f(X)$, it follows that $U(X) = V(X)$.

Removing the common factors from both sides of polynomials (corresponding to $u_j = v_j$), Then we obtain identity

$$\prod_{h \in \mathcal{H}} (X^h + 1)^{u_h} = \prod_{k \in \mathcal{K}} (X^k + 1)^{v_k}.$$

Where $\mathcal{H}$ and $\mathcal{K}$ are a disjoint subset of $S_{a,n}$ but for e to be the smallest element in $\mathcal{H} \cup \mathcal{K}$, so the term of smallest degree x^e appears on only one side of the identity makes the different degree of both side which is a contradiction.
So, each partition gives a different value when raised to the power of $\zeta + 1$. □

6.2 Counting Partitions

In this section, we will construct lower bounds for $\mathcal{P}_{a,n}$, but they will only be useful if t is not very small, specifically, $t > \sqrt{2\pi}$.

Corollary 6.2. *Let $n = p$ be an odd prime and two be primitive root modulo p. Then, as $n \to \infty$,*

$$P(n) \geq \exp\left[\left(\frac{\pi}{\sqrt{3}} + o(1)\right)\right].$$

Corollary 6.3. *Suppose 2 is primitive root modulo odd non-Wieferich prime p that is $2^{p-1} \not\equiv 1 \bmod p^2$. For $n = p^k$, as $k \to \infty$.*

$$P(n) \geq exp\left[\left(\frac{\pi}{\sqrt{3}}\sqrt{\frac{p-1}{p}} + o(1)\right)\sqrt{n}\right].$$

If $t < \phi(n)$. Let $2 \leq N < t$ be an integer and set $S_{a,n}(N) = S_{a,n} \cap [1, N]$. Each subset $\tau \subseteq S_{a,n}$ of $\#\tau < t/N$ produces a valid partition $u \in \mathcal{P}_{a,n}$, where $u_j = 1$ if $j \in J$ else 0 as follows:

$$\text{for } \tau \subseteq S_{a,n} \text{ and } \#\tau < t/N,$$

$$\sum_{j \in S_{a,n}(N)} j u_j = \sum_{j in \tau} j < t/N \max(\tau).$$

But, N is the maximum value τ can attain

$$\implies \sum_{j\in\tau} j < t/NN = t.$$

Because $\#\mathcal{P}_{a,n}$ is the partition of $t-1$, whose indicies varying in the whole set $S_{a,n}$. Thus

$$\#\mathcal{P}_{a,n} \geq \sum_{J\leq t/N} \binom{\#S_{a,n}(N)}{J}. \tag{6.1}$$

Now it remains to find $\#S_{a,n}$ and choose suitable a and N.
Claim: Among the cosets of $< 2 > \subseteq (\mathbb{Z}/n\mathbb{Z})^*$, one of the coset contain at least the average number of representative in $[1, N]$. So there exist an integer a, prime to n such that

$$\#S_{a,n}(N) \geq \frac{t}{\varphi(n)}\#\{j : 1 \leq j \leq N, \gcd(j, n) = 1\}.$$

Proof: On contrary, Assume that for any $a < n$, prime to n,

$$\#S_{a,n}(N) < \frac{t}{\varphi(n)}\#\{j : 1 \leq j \leq N, \gcd(j, n) = 1\}.$$

Denote $\alpha_N = \#\{j : 1 \leq j \leq N \mid \gcd(j, n) = 1\}$.
Now, observing that $\alpha_N = \#\dot{\bigcup} S_{a,n}(N)$ as it is the cardinality of disjoint union of cosets intersecting with sub-interval $[1, N]$. As coset's union cover the whole elements less than n that are relatively prime to it, there are total $\varphi(n)/d$ cosets available, say d to be the order of the element whose cosets we are taking. That means

$$\alpha_N = \#\dot{\bigcup} S_{a,n}(N) = \#\dot{\bigcup} S_{a_1,n}(N) + \#\dot{\bigcup} S_{a_2,n}(N) + \cdots + \#\dot{\bigcup} S_{\frac{\varphi(n)}{d},n}(N),$$

by assumption

$$\alpha_N = \#\dot{\bigcup} S_{a,n}(N) < \frac{t}{\varphi(N)}\frac{\varphi(N)}{t}\alpha_N = \alpha_N.$$

This contradiction provides us an element a for which one of its coset holds,

$$\#S_{a,n}(N) \geq \frac{t}{\varphi(n)}\#\{j : 1 \leq j \leq N, \gcd(j, n) = 1\}.$$

■

It is a well-known result,

$$\alpha_N = \#\{j : 1 \leq j \leq N \mid \text{gcd(j,n)} = 1\} = N\frac{\varphi(n)}{n} + O(n^{o(1)}).$$

Proceeding further, we will show:

$$\#S_{a,n}(N) \geq \frac{t}{\varphi(n)}(N\frac{\varphi(n)}{n} + O(n^{o(1)})) = (1 + o(1))\frac{tN}{n},$$

$$\frac{t}{\varphi(n)}(N\frac{\varphi(n)}{n} + O(n^{o(1)})) = \frac{tN}{n}\left(1 + \frac{n}{N\varphi(n)}O(n^{o(1)})\right).$$

In another way, our goal is to show that

$$\frac{n}{N\varphi(n)}O(n^{o(1)}) = o(1).$$

As $n \to \infty$, provided $N > n^\epsilon$ for some fixed $\epsilon > 0$ we have;

$$\frac{n}{N\varphi(n)}O(n^{o(1)}) < \frac{C.n.n^{o(1)}}{n^\epsilon\varphi(n)} \tag{6.2}$$

$$= \frac{C.n^{1-\epsilon+o(1)}}{\varphi(n)}. \tag{6.3}$$

for $1 - \epsilon \leq 0$ or $\epsilon > 1$ makes $\frac{n}{N\varphi(n)}O(n^{o(1)}) = o(1)$.

Thus,

$$\#S_{a,n}(N) \geq \frac{t}{\varphi(n)}(N\frac{\varphi(n)}{n} + O(n^{o(1)})) = \frac{tN}{n}\left(1 + o(1)\right)).$$

For $N = [\sqrt{2n}]$ and since $t > N$, so $t \geq n^{\frac{1}{2}+\epsilon}$.

In such a setting, again, we will show that;

$$\frac{tN}{n}\left(1 + o(1)\right)) = (2 + o(1))\frac{t}{N}.$$

$$\begin{aligned}\frac{tN}{n}\left(1+o(1)\right)) &= \left(\frac{N^2}{n}+\frac{N^2}{n}o(1)\right)\frac{t}{N}\\ &= \left(2+2*o(1)\right)\frac{t}{N}\\ &= \left(2+o(1)\right)\frac{t}{N}.\end{aligned}$$

From the above calculation, we get

$$\#S_{a,n} \geq (2+o(1))\frac{t}{N}.$$

Stirling formula: For large n

$$n! \approx \frac{n^n}{e^n}\sqrt{2\pi n}.$$

Putting all values in 6.1 we get:

$$\begin{aligned}\#\mathcal{P}_{a,n} \geq \sum_{J\leq t/N}\binom{\#S_{a,n}(N)}{J} &\geq \binom{\#S_{a,n}}{[t/N]}.\\ &= \frac{(\#S_{a,n})!}{(r!)(\#S_{a,n}-r)!}\ , \qquad \text{Where}\quad r=\left[\frac{t}{N}\right]\\ &\geq \exp((\log(4)+o(1))\frac{t}{N}).\end{aligned}$$

Corollary 6.4. *Let n be odd, and t is the order of two modulo n.Then*

$$P(n) \geq \exp\left((\log(4)+o(1))\frac{t}{\sqrt{2n}}\right).$$

Proof. **Specific Case:** When $n = p^k$, p is odd prime.
Claim: $t \geq c(p)p^k$, Where $c(p) > 0$ depends only on p

This claim will help us to compare our result and the results of corollary 6.2 and corollary 6.3.

Proof: **Case 1 :** 2 is primitive root modulo n.
In this case $t = \varphi(n) = \varphi(p^k) = p^{k-1}(p-1) \implies t = (\frac{p-1}{p})p^k$, Here $c(p) = \frac{p-1}{p}$.

Case 2 : 2 is not primitive root modulo n.
Suppose d be the order of 2 mod$p$. If 2 is not primitive mod p, $\implies d|p-1$. Now we will prove that 2 has order dp in $(\mathbb{Z}/p^2\mathbb{Z})^*$. If 2 doesn't have order dp, then 2 has order d.
As

$$\begin{aligned} &2^d = 1 + kp, \quad k \text{ is constant.} \\ &2^{dp} = (1+kp)^p = 1 + p(kp) + \sum_{1<r\geq p} \binom{p}{r} p(kp)^r, \\ &2^{dp} \equiv 1 \text{ mod } p^2. \end{aligned}$$

Suppose dp is not the order of 2 mod (p^2), This means there exist smaller positive integer than dp which divides it and also the order of 2.
Let p be that integer.
$\implies 2^p \equiv 1$ mod p^2 as $p|p^2$, So $2^p \equiv 1$ mod p. This is a contradiction by *Fermat little theorem*. We will obtain the same contradiction for all proper divisors of d. So d is the order of 2 mod(p^2).

By induction we will show $\forall n \geq 3$ in $(\mathbb{Z}/p^n\mathbb{Z})^*$,

$$2 \text{ has order } t = \begin{cases} dp^{n-1} & \text{if order of } (2) = dp \text{ in } (\mathbb{Z}/p^2\mathbb{Z})^* \\ dp^{n-2} & \text{if order of } (2) = d \text{ in } (\mathbb{Z}/p^2\mathbb{Z})^* \end{cases}$$

If order of 2 is dp in $(\mathbb{Z}/p^2\mathbb{Z})^*$.
For $n = 2$ as the base case, the statement is true.
Suppose true for $n = k \implies 2^{dp^{k-1}} \equiv 1$ mod (p^k). So,

$$\begin{aligned} 2^{dp^{k-1}} &= (1 + kp^k) \quad \text{where } k \text{ is constant,} \\ \implies 2^{dp^k} &= (1+kp^k)^p \equiv 1 \text{ mod } (p^{k+1}). \end{aligned}$$

Thus 2 has order dp^k in $(\mathbb{Z}/p^{k+1}\mathbb{Z})^*$.
Similarly, when order of 2 is d in $(\mathbb{Z}/p^2\mathbb{Z})^*$.
For $n = 2$ as the base case, the statement is true.
Suppose true for $n = k \implies 2^{dp^{k-2}} \equiv 1$ mod (p^k) . So,

$$\begin{aligned} 2^{dp^{k-2}} &= (1+kp^k) \quad \text{where } k \text{ is constant,} \\ \implies 2^{dp^{k-1}} &= (1+kp^k)^p \equiv 1 \bmod (p^{k+1}). \end{aligned}$$

Thus 2 has order dp^{k-1} in $(\mathbb{Z}/p^{k+1}\mathbb{Z})^*$. ■

In both cases $c(p) = \frac{d}{p^2}$ which depends only on p.

Now if for $n = p^k$, $t \geq c(p)n$ then, $\frac{t}{\sqrt{n}} \geq c(p)\sqrt{n}$. Substituting this in the result obtained in corollary 6.4, we get,

$$\begin{aligned} P(n) &\geq \exp\left(\left(\frac{\log(4)}{\sqrt{2}} + o(1)\right)\frac{t}{\sqrt{n}}\right) \\ &\geq \exp\left(\left(\frac{\log(4)}{\sqrt{2}} + o(1)\right)\sqrt{n}\right). \end{aligned}$$

Hence corollary 6.4 gives a version of corollary 6.3 in the form

$$p(n) \geq \exp(c(p)\sqrt{n}).$$

□

In the case when 2 is primitive root modulo n, and $t \approx n$ from corollary 6.4, we get a similar result to corollary 6.2 and corollary 6.3 but with smaller constant in the exponent.

Chapter 7

Unbounded Ducci Sequences

7.1 Generalization of the Ducci Map

In this section, we will generalize the *Ducci Map* and study the specific versions of it. This will be done as follows, the map that we are dealing with gives the first iterate of a string $X = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ as $(|x_1 - x_2, |x_2 - x_3|, \ldots, |x_n - x_1|)$.
Now we can see that the first coefficient of the element of first iterate is 1 for x_i and -1 for x_{i+1}, $1 \leq i \leq n$ indices in $mod(n)$, we will denote such map by calling map with *weighting* $W = (\underline{1}, -1)$.
For example if $W = (-1, \underline{2}, -1)$, then the first iterate of such map is $(|2x_1 - x_3 - x_n|, |2x_2 - x_3 - x_1|), \ldots, |2x_n - x_1 - x_{n-1}|$.
Till now, we have studied the dynamics of the map with *weighting* $(\underline{1}, -1)$. In this chapter, we will study the dynamics of the map with *weighting* $(-1, \underline{2}, -1)$.

Definition 7.1. *The weighting* $W = (\underline{w_1}, w_2, w_3, \ldots, w_k)$ *is said to be bounded if the maximum of any string does not increase under iteration.*

$W = (\underline{1}, -1)$ is an example of bounded weighting.

Definition 7.2. *The weighting is said to be unbounded if the maximum of any string is non-decreasing under iteration.*

$W = (-1, \underline{2}, -1)$ is an example of bounded weighting.

Sum of weighting is the absolute sum of the element in the weighting.

7.2 Results on Weighting

Theorem 7.3. *Let W be the weighting having sum s. For any given string of arbitrary length, there exists a non-zero string that iterates under W to zero-string if and only if $s = 0$.*

Proof. Let $W = (w_1, w_2, \dots, w_k)$ be the weighting; with respect to this weighting we construct a $n \times n$ circulant matrix:

$$A = \begin{bmatrix} x_1 & x_2 & x_3 & x_k & ..0 \\ 0 & x_1 & x_2 & x_{k-1} & ..0 \\ . & . & . & & \dots \\ . & . & . & & \dots \\ x_2 & x_3 & . & \dots & x_1 \end{bmatrix}.$$

We first claim that for any given string, it iterates to zero-string if and only if the determinant of A is zero.

$\Longrightarrow$ Assume that $X = (x_1, x_2, ..., x_n)$ be any string, for any given weighting, we can construct matrix A, Also consider map $H : R^n \to R^n$, where $H(x_1, x_2, \dots, x_n) = (|x_1|, |x_2|, \dots, |x_n|)$.

Consider operation $H \circ A$ with X as a column matrix where $A(X)$ is usual matrix multiplication, here generalised *ducci* map is $D = H \circ A$.

If iterate of X goes to zero that means $\exists$ smallest integer k such that $D^k(X) = 0$.

$$\Longrightarrow D(D^{k-1}(X)) = 0,$$

as k is the smallest integer for iterate goes to zero, so $Y = D^{k-1}(X)$ is non-zero, that means $D(Y) = 0$ or $H \circ A(Y) = 0$. As kernal of H map is zero-string, so $A(Y) = 0$ as Y is non zero string that makes A a singular matrix.

$\Longleftarrow$ Now, Assume that the determinant of A is Zero, i.e., there exists a non-zero vector X Such that $A(X) = 0$. So string X goes to zero after 1 iteration.

Call this condition as "determinant condition". For $n \times n$ circulant matrix eign-value is:

$$\lambda_j = x_1 + x_2\omega + \cdots + x_n\omega^{n-1}. \tag{7.1}$$

If determinant condition holds for a circulant matrix, so $\lambda_j = 0$ for some j. If $s = 0$, string $X = [1, 1, \ldots, 1]$ or $\omega = 1$ will satisfy (7.1) for any $n \geq k$. If $s \neq 0$, let $n > k$, be any prime. Since n is prime, $\omega^n - 1$ is the lowest degree equation the algebraic number ω can satisfy unless $\omega = 1$. However, $\omega = 1$ does not satisfy (7.1) if $s \neq 0$.

□

7.3 Results on S

Observe that:

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_k & ..0 \\ 0 & x_1 & x_2 & x_{k-1} & ..0 \\ . & . & . & & \ldots \\ . & . & . & & \ldots \\ x_2 & x_3 & . & \ldots & x_1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = \sum_{i=1}^{k} x_i \begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}.$$

Remark 7.4. *If $S = 0$, one-string goes to zero after 1 iteration.*

Remark 7.5. *If $S = 1$, then one-string is the fixed string.*

Remark 7.6. *If $S > 1$, then one-string diverges.*

7.4 Study of W = (-1,$\underline{2}$,-1)

In this section, we will study a map having $W = (-1,\underline{2},-1)$. This map has the property that it is unbounded. We are interested in the string that iterates to zero-string. The following theorem is in this regard.

Theorem 7.7. *For any integer $n \neq 2^m (m \in Z_{\geq 1})$, there are n-string that do not iterate to zero-string.*

Proof. Consider the entry of the string in mod 2, i.e., primitive string.

Claim: The only non-zero predecessor of zero-string in mod 2 is one-string

Proof: As $x \equiv -x$ mod 2 and $2x_i - x_{i+1} - x_{i-1} \equiv x_{i+1} + x_{i-1}$ mod 2. Index in mod n. Let A be a string having at least one non-zero element.

$$A = (x_1, x_2, x_3, \ldots, x_n),$$

$$D(A) = (0, 0, 0, \ldots, 0).$$

For i index entry to be zero after one iteration makes $x_{i+1} = x_{i-1}(1 \leq i \leq n)$, i.e

$$x_2 = x_n, x_1 = x_3, x_2 = x_4...$$

following the pattern, each even index term needs to be equal, and each odd index term also needs to be equal, but $x_2 = x_n$. As the length of string is odd, this makes string A to be one-string. ■

Case 1 : When n is odd.

The below table shows the iterate of the middle term(entry at second index) of the substring of $3-$element.

3-string $mod(2)$	iterate of middle term $mod(2)$
$(0, 0, 0)$	0
$(1, 0, 0)$	1
$(0, 1, 0)$	0
$(0, 0, 1)$	1
$(1, 0, 1)$	0
$(0, 1, 1)$	1
$(1, 1, 0)$	1
$(1, 1, 1)$	0

From the table, observe that $(1, 1, 0, 0)$ is the only possible string (upto shift) to make one-string after 1 iteration, but concatenating such string always results in an even length string, which is a contradiction.

Case 2 : When n is even $n \neq 2^m$.
Writing $n = p_1 p_2 ... p_k$ as a product of primes, choose any odd prime and divide n-string into n/p strings each of length p. As each substring has an odd length from the previous theorem, each substring cannot iterate to zero-string; thus original string cannot iterate to zero-string.

□

In Weighting $(1, -1)$ we proved that every n-string $n = 2^m (m \in \mathbb{N})$ iterate to zero string. But weighting $(-1,\underline{2},-1)$ such result doesn't hold as this weighting is unbounded
Example:

$$A = (1, 2, 3, 0, 1, 0, 1, 2),$$

$$D^{24}(A) = 2^8(1, 2, 3, 0, 1, 0, 1, 2).$$

This string diverges.

7.5 Every 4-string iterate to zero-string

Lemma 7.8. *Let a, b, c, d be any integers .Any string of the form $(0, b, d, d)$, $(0, 0, c, d)$, $(a, 0, c, 2a)$, (a, a, c, c), (a, b, a, b) iterate to zero-string.*

Theorem 7.9. *All integer 4-string iterate to zero-string.*

Proof. The idea is the same that we have used to prove that the ducci sequence in weighting $(1, -1)$ is eventually periodic. We first claim that after two iterations, the maximum is no more than double the original string. At last we will dispose of the cases where such behavior is not followed.
Important observation:
Let $L : \mathbb{Z}^n \to Z^n$ be a left-shift map. For $A = (x_1, x_2, \ldots, x_n)$ and $L(A) = (x_2, x_3, \ldots, x_1)$, $D(L(A)) = L(D(A))$. It is easy to check every 4-string mod2 iterate to zero-string.
To prove the claim, we have two cases to consider. After one iteration, every element of the string become positive; we will start with such string.

Case 1: $A = (a, b, c, d)$, where a is the minimum of string and d is the maximum.

$$D(A) = (|2a - b - d|, |2b - c - a|, |2c - d - b|, |2d - a - c|).$$

$2a - b - d \leq 0,\ 2d - a - c \geq 0,$

$$\implies D(A) = (b + d - 2a, |2b - c - a|, |2c - d - b|, 2d - a - c).$$

Cases	$D^2(A)$	Borderline case
$2b - a - c \geq 0$ $2c - d - b \geq 0$	$(2c - 2a, \|4b - 4c\|, \|6c - 4d - 4b + 2a\|, 4d - 4c)$	$(0, b, d, d)$ $(0, 0, 0, d)$
$2b - a - c \geq 0$ $2c - d - b \leq 0$	$(2c - 2a, 2d - 2b, 2c - 2a, 2d - 2b)$	(x, y, x, y)
$2b - a - c \leq 0$ $2c - d - b \geq 0$	$(4b - 4a, 4b - 4a, 4d - 4c, 4d - 4c)$	(x, x, y, y)
$2b - a - c \leq 0$ $2c - d - b \leq 0$	$(4b - 4a, \|4c + 4a - 6b - 2d\|, \|4b - 4c\|, 2d - 2b)$	$(0, 0, c, d)$

Case 2: $A = (a, b, c, d)$, where b minimum of string and d is maximum.

$$D(A) = (|2a - b - d|, |2b - c - a|, |2c - d - b|, |2d - a - c|).$$

$2b - c - a \leq 0,\ 2d - a - c \geq 0,$

$$\implies D(A) = (|2a - b - d|, c + a - 2b, |2c - d - b|, 2d - a - c).$$

Cases	$D^2(A)$	Borderline case
$2a-b-d \geq 0$ $2c-d-b \geq 0$	$(4d-4a, 2d-2b, 4d-4c, \lvert 6d-4a-4c+2b \rvert)$	$(a,0,c,2a)$ $(a,0,c,2c)$ $(a,0,a,a)$ b=0, maximum in term 2
$2a-b-d \geq 0$ $2c-d-b \leq 0$	$(4d-4a, 4c-4b, 4c-4b, 4d-4a)$	(x,y,y,x)
$2a-b-d \leq 0$ $2c-d-b \geq 0$	$(4a-4b, 4a-4b, 4d-4c, 4d-4c)$	(x,x,y,y)
$2a-b-d \leq 0$ $2c-d-b \leq 0$	$(4a-4b, \lvert 4c+4a-6b-2d \rvert, 4c-4b, 2d-2b)$	$(a,0,c,2a)$ $(a,0,c,2c)$ $(a,0,a,a)$ b=0, maximum in term 4

Let us suppose b is minimum and d is maximum. We can assume that $b=0$ due to the nature of the Ducci map. We discuss borderline situations for case 4 when $2a \leq d$ and $2c \leq d$.

- $2a-d=0$: This gives the tuple $(a,0,c,2a)$.
- $2c-d=0$: This gives the tuple $(a,0,c,2c)$.
- When either $2a-d<0$ or $2c-d<0$. We know that $D^2(a,0,c,d)=(4a, |4a+4c-2d|, 4c, 2d)$. Clearly the fourth term is maximum among the first, third and fourth terms. Now $2a \leq d$ and $2c \leq d$ implies $2a+2c \geq 2d$. Hence $4a+4c-2d \geq 0$. Thus $D^2(a,0,c,d)=(4a, 4a+4c-2d, 4c, 2d)$. Observe that $4a+4c-2d \leq 4a$ and also $4a+4c-2d \leq 4c$, hence the second term is the minimum of the second iterate of $(a,0,c,d)$.
  Again using the translation argument, we can make the minimum to be 0, which implies $4a+4c-2d=0 \iff 2a+2c=d$.
  Thus the second iterate is $(4a,0,4c,2d)=(4a,0,4c,4a+4c)$. Taking a factor

of 4 out, we get $(a, 0, c, a+c)$. Hence the maximum is $a+c$, which is strictly less than d (maximum of the initial tuple).

The other case when $2a - b \geq 0$ and $2c - d \geq 0$ can be handled similarly. □

7.6 String of length 3

Theorem 7.10. *Any integer* $3-$*string maps to* $(a, b, a+b)$ *after one iteration.*

Proof.

$$A = (x, y, z).$$

$$D(A) = (|2x - y - z|, |2y - z - x|, |2z - x - y|).$$

$$a = 2x - y - z,\ b = 2y - z - x \implies a + b = |2z - x - y|.$$

□

Theorem 7.11. *The iterate of any string* $(a, b, a{+}b)$*, where* $a, b \in \mathbb{Z}^+$ *and* $gcd(a, b) = 1$ *may only have* 3 *as a common factor.*

Proof.

$$Let\ A = (a, b, a+b),$$

$$D(A) = (|2b - a|, |2a - b|, |a + b|).$$

WLOG, let $b \geq a$

$$\implies D(A) = (2b - a, |2a - b|, a + b).$$

If string has factor k then,
$2b - a \equiv 0 \bmod k$ and $2a - b \equiv 0 \bmod k$, subtracting them gives:
$3b \equiv 0 \bmod k$ and $3a \equiv 0 \bmod k$, $k|3$ or $k|a$ and $k|b$.
$\implies k|gcd(a, b)$ gives $k = 1$. So 3 is the only nontrivial common factor.

□

Theorem 7.12. *Any integer* $3-$*string either diverges or iterate to fixed point* $(x, x, 2x)$ *(or shifted version)*

Proof. For any given $3-$string, we claim that its middle term(in size, not in position) is non-decreasing. WLOG let $b \geq a$.
For $A = (a, b, a+b)$, $D(A) = (2b-a, |2a-b|, a+b)$.
Now, $b+b-a \geq b$ and $a+b \geq b$.

<u>Claim:</u> $|2a-b|$ is less than b.
<u>Proof:</u> On contrary assume $|2a-b| \geq b \implies 2a-b \geq b$ gives $2a \geq 2b$, which is false as $b \geq a$ or $|2a-b| \leq -b$ gives $2a \leq 0$ false and equality holds when $a=0$ which makes A fixed string, so $|2a-b| \leq b$ ■
$2b-a$ or $a+b$ is the middle element of $D(A)$ which increases from the previous string. The middle term remains the same if $a=b$ leads $D(A) = (b, b, 2b)$, which is a fixed string. □

The previous three theorems gave the description of $3-$string iterates. Now, the question remains whether a given string will diverge or not. The following theorem provides a basis for that answer.

Theorem 7.13. *Let $a, b \in \mathbb{Z}^+$ with $gcd(a,b) = 1$ amd $a \leq b$.Then if $a \not\equiv 1 \bmod 3$ or $b \not\equiv 2 \bmod 3$ then sting $(a, b, a+b)$ diverges.*

Proof. Scale the string $(a, b, a+b)$ by dividing each entry by b to $(m, 1, 1+m)$, where $m \in [0,1]$ and consider ratio: $R_A = \frac{\textit{smallest term}}{\textit{midlle term}}$ (middle in terms of size, not in position).
For string $A = (m, 1, 1+m)$ $R_A = m$. After one iteration $D(A) = (2-m, 1-2m, m+1)$ if $m \in [0, \frac{1}{2}]$, so the ratio $R_{D(A)} = \frac{1-2m}{m+1}$. Similarly, $D(A) = (2-m, 2m-1, m+1)$ if $m \in [\frac{1}{2}, 1]$ and ratio is $R_{D(A)} = \frac{2m-1}{2-m}$.
In summary, the ratio of smallest to middle term iterates via map $\bar{f} : [0,1] \to [0,1]$ defined by:

$$\bar{f} = \begin{cases} \dfrac{1-2x}{1+x}, & x \in [0, \dfrac{1}{2}] \\ \dfrac{2x-1}{2-x}, & x \in (\dfrac{1}{2}, 1]. \end{cases}$$

By theorem 7.12 string $A = (a, b, a+b)$ diverges if and only if $m = a/b$ does not iterate to one under $\bar{f}$ in finitely many steps, else it will converge to fixed string

$(1,1,2)$.
Under $\bar{f}$ there exist two predecessor of $x \in [0,1]$

$$\frac{1-x}{x+2}, \quad \frac{1+2x}{x+2}.$$

If

$$x = \frac{a}{b}, a, b \in \mathbb{Z}^{+}, a \equiv 1 \bmod 3, \; b \equiv 2 \bmod 3,$$

the $\bar{f}$ predecessors are also of the same form

$$\frac{1-x}{x+2} = \frac{1 - \frac{1+3k_1}{2+3k_2}}{\frac{1+3k_1}{2+3k_2} + 2} = \frac{1 \bmod 3}{2 \bmod 3}.$$

$$\frac{1+2x}{x+2} = \frac{1 + \frac{2+3k_1}{2+3k_2}}{\frac{1+3k_1}{2+3k2} + 2} = \frac{1 \bmod 3}{2 \bmod 3}.$$

As $\bar{f}^{-}(1) = 0$ or 1 and $\bar{f}^{-}(0) = 1/2$. So, we concluded that $\bar{f}^{k} = 1$, $(k \in \mathbb{Z}^{+})$ if and only if $x = 0$, $x = 1$ or

$$x = \frac{a}{b}, a, b \in \mathbb{Z}^{+}, a \equiv 1 \bmod 3, b \equiv 2 \bmod 3.$$

So, in contrast $\bar{f}^{k} \neq 1$ if $a \not\equiv 1 \bmod 3$ or $b \not\equiv 2 \bmod 3$. □

Chapter 8

Ducci Matrices

In this section, we will study the *Ducci Map* in matrix form with some other versions of it. We will use results from Linear Algebra. The goal of this section is to show that *Ducci Map* is just one of the representations of a large class of maps showing similar iterative behavior.

Definition 8.1. *The Ducci Map with respect to $n \times n$ matrix A on $\mathbb{R}^n$ is defined as*

$$\delta_A(x) = |Ax|.$$

Where, $x = (|x_1|, |x_2|, \ldots, |x_n|)$. For $x \in \mathbb{R}^n$, the sequence $x, \delta_A(x), \delta_A^2(x), \ldots,$ is called Ducci Sequence.

Definition 8.2. *The $n \times n$ matrix A is said to be Ducci Matrix if the Ducci Sequence corresponding to it contains zero-vector for almost all $x \in \mathbb{R}^n$.*

Example 8.3. For $x \in \mathbb{R}^4$, corresponding original *Ducci Matrix* is

$$A_0 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \\ -1 & 0 & 0 & 1 \end{pmatrix}.$$

Example 8.4. Let $x \in \mathbb{R}^4$. For $s = x_1 + x_2 + \cdots + x_n$. The map $(x_1, x_2, \ldots, x_n) \mapsto (x_1, x_2, \ldots, x_n)$ having matrix form

$$A_1 = \begin{pmatrix} 3 & -1 & -1 & -1 \\ -1 & 3 & -1 & -1 \\ -1 & -1 & 3 & -1 \\ -1 & -1 & -1 & 3 \end{pmatrix}.$$

The *Ducci Sequence* for all $x \in \mathbb{R}^4$ corresponding to A_1 terminates, except for the vectors having three, not all components are equal.

Definition 8.5. *Let $A \neq 0$ be a real $n \times n$ matrix. The Ducci Length(length) of $x \in \mathbb{R}^n$ is smallest k such that $\delta_A^k(x) = 0$, denoted by $\lambda_A(X)$. If not such k exists then $\lambda_A(x) = \infty$.*

Definition 8.6. *The $n \times n$ matrix A is said to be Ducci Matrix, if the set $\{x \in \mathbb{R}^n : \lambda_A(x) = \infty\}$ has 0 Lebesgue measure.*

Definition 8.7. *For a Ducci Matrix A, $x \in \mathbb{R}^n$ such that $\lambda_A(x) = \infty$ called an exception vector.*

Definition 8.8. *The $n \times n$ matrix A is called the difference matrix if every row consists of 1 and -1 exactly once and zero otherwise.*

Definition 8.9. *The $n \times n$ matrix A having entries in $\mathbb{Z}$ is called $\mathbb{Z}-$Ducci Matrix if the length is finite for all $x \in \mathbb{Z}^n$.*

Example 8.10.

$$A_{0,n} = \begin{pmatrix} 1 & -1 & 0 & \ldots & 0 \\ 0 & 1 & -1 & \ldots & 0 \\ . & . & . & \ldots & . \\ . & . & . & \ldots & . \\ -1 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Matrix $A_{0,n}$ is an example of *difference matrix*, we proved that it is $\mathbb{Z}-$*Ducci Matrix* if and only if n is a power of 2.

In the following lemma, we will see the connection between *difference matrix* and $\mathbb{Z}-$*Ducci Matrix.*

Lemma 8.11. *let A be a difference matrix, if there exist an integer k such that A^k have only even entries, then A is $\mathbb{Z}-$Ducci Matrix.*

Proof. Let A b a difference matrix, as given, suppose for $x \in \mathbb{Z}^n$ and $m = \max(|x_i|)$ $1 \leq I \leq n$, we have $\delta_A^k(x) = 2y$ for some $y \in \mathbb{N}^n$. Since A is a difference matrix, so maximum element of the vectors is non-increasing.
Therefore, $y_i \in y$ satisfy $0 \leq 2y_i \leq m$, thus $\max(y_i) \leq m/2$ for all i. Suppose after kl steps vector obtained having element 1 at each position thus maximum of the vector becomes 1.

$$\frac{m}{2^l} = 1 \implies l = \log_2 m.$$

After one more application vector becomes *zero vector.* Thus total number of steps are $\lceil k \log_2 m \rceil$. □

8.1 Maps with Traps

After exhibiting random behavior for a long time, we observed that the *Ducci* sequence suddenly settles down to periodic or terminating behavior. This phenomenon is similar to one of the features of *dynamical system* known as *transient chaos.* There are self-maps whose iteration shows chaotic behavior for a while and suddenly turns into *regular*(periodic or constant). In this part, we will explore this phenomenon in *Ducci sequences.* In the following example, we will install the trap for *tent map.*

Example 8.12. Let $f : [0, 1] \to [0, 1]$ defined as

$$f(n) = \begin{cases} 2x & \text{if } 0 \leq x \leq \frac{1}{2}, \\ 2 - 2x & \text{if } \frac{1}{2} \leq x \leq 1. \end{cases}$$

Definition 8.13. *For a self-map f, a point x_0 in the domain is said to be a fixed point if $f(x_0) = x_0$. A fixed point is repelling if $|f'(x_0)| \geq 1$.*

For *tent map* $x_0 = 2/3$, it is a repelling fixed point. We choose $0 < \delta < 1/6$ and let $I_\delta = (x_0 - \delta, x_0 + \delta)$, we modify the *tent map* by installing a trap.
Let $f_\delta : [0,1] \to [0,1]$

$$f_\delta(x) = \begin{cases} f_x & \text{if } \ x \in [0,1] \backslash I_\delta, \\ x_0 & \text{if } \ x \in I_\delta. \end{cases}$$

As *tent map* is chaotic, it implies that for every $x \in (0,1)$, its orbit eventually reaches I_δ resulting in constant orbit after that. The region I_δ is a trap for *tent map.*

8.2 Trap Matrices

In this section, we will install a trap for *Ducci Matrices.*

Definition 8.14. *Let A be $n \times n$ non zero matrix, for $x \in \mathbb{R}^n$, a signed Ducci map is a map $\sigma_A : x \mapsto A|x|$. The sequence $x, \sigma_A(x), \sigma_A^2(x), \ldots$ is called signed Ducci sequence.*

$$\begin{aligned} \text{Ducci sequence of x} \quad & x, |Ax|, |A|Ax||, |A|A|Ax|||, \ldots \\ \text{Signed Ducci sequence of x} \quad & x, A|x|, A|Ax|, A|A|Ax||, \ldots \end{aligned}$$

Definition 8.15. *For a signed tuple $s = (s_1, s_2, \ldots, s_n) \in \{0,1\}^n$. Let $R_s \subset \mathbb{R}^n$ is the closure of $\{(x_1, x_2, \ldots, x_n)^T : s_1x_1 > 0, s_2x_2 >, \ldots, s_nx_n > 0\}$.*

Such $R_s \subset \mathbb{R}^n$ partition the $\mathbb{R}^n$, where σ_A is linear. So we get for $x \in R_s$, $\sigma_A(x) = A|x| = ASx$, where S is diagonal matrix having entries from s.
We observe that for $x \in \mathbb{R}^n$ after the first iteration, the *signed Ducci sequence* completely lie in *Im(A)*, so we can consider σ_A on *Im(A)*. For a non-zero *Ducci matrix A*, the kernel is non-trivial, then by *rank-nullity theorem* the *Im(A)* is a proper subspace of $\mathbb{R}^n$.

Definition 8.16. *Let A be a $n \times n$ matrix. A trap of A is a region R_s such that for its corresponding sign matrix S, the map $x \mapsto ASx$ is non-invertible on Im A. If A has at least one trap, it is known as a trap matrix.*

From the above definition, we demand the non-invertibility on proper subspace *Im A*. Since on R^n, the map $x \mapsto ASx$, where A is *Ducci matrix* and S is sign matrix is always non-invertible because *Ducci matrix* is a type of *circulant matrix* which are singular.

Theorem 8.17. *Every Ducci matrix is a trap matrix.*

Proof. To prove that every *Ducci matrix* is a *trap matrix*, we need the existence of at least one trap. Consider the *signed Ducci sequence*, the second last element $u \neq 0$(this element exist since the given matrix is *Ducci matrix*), such that $v = \sigma_A(u) \neq 0$ but $\sigma_A(v) = 0$. Let S be the sign matrix corresponding to the sign of v. Since $v \in$*Im A*, the map $v \mapsto ASv = 0$ is non-invertible on *Im A*. □

In order to explain the above concept, let us look at an example.

Example 8.18. For

$$A_0 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \\ -1 & 0 & 0 & 1 \end{pmatrix}.$$

A_0 has six traps corresponding to the sign tuple $s = \pm(1, -1, 1, -1), \pm(1, 1, -1, -1)$ and $\pm(1, -1, -1, 1)$. Suppose $s = (1, -1, 1, -1)$ then,

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad A_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$$

The first three columns of matrix B form basis of *Im A*, forth column is *(Im A)*$^\perp =$

$Ker(A^T)$. Consider matrix $M = B^{-1}A_0SB$, matrix M is similar to matrix A_0S.

$$M = B^{-1}A_0SB = \begin{pmatrix} 1 & 1 & 0 & 2 \\ 0 & -1 & -1 & -2 \\ -1 & -1 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The last row is zero indicating that matrix M is singular matrix, for any $x = (x_1, x_2, x_3, x_4) \in \mathbb{R}^4$ the forth component of x become zero after one application of M, thus vectors in $Im\ A$ can be considered in $\mathbb{R}^3$. If $C = R_s \cap Im\ A$, $\sigma_A(C)$ has lower dimension than C. This dimensionaltiy reduction by matrix M is analogus to the trap that is studied for *trap matrix*.

Thus we can repersent map $(x \mapsto A_0Sx)|Im\ A$ by matrix $\overline{M} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & -1 \\ -1 & -1 & 0 \end{pmatrix}$, since the determinant of $\overline{M} = 0$, the corresponding region R_s is a trap.

Lemma 8.19. *Let A be $n \times n$ matrix over $\mathbb{R}$. Then the following conditions on A are equivalent.*

1. *The map $x \mapsto Ax$ is invertible on ImA.*

2. *$ImA \bigoplus KerA = \mathbb{R}^n$.*

3. *rankA^2 =rank$A$.*
   The following condition is also equivalent if matrix A is singular.

4. *If K and C are matrices whose columns consist a basis of $KerA$ and of $KerA^T$, repectively, then det$(C^TK) \neq 0$.*

Proof. $1 \implies 2$
Consider the map $ImA \mapsto \mathbb{R}^n$, since this map is invertible implies for $x \in \mathbb{R}^n$, $A(A(x)) = 0$ if and only if $Ax = 0$. We will show that $KerA \cap ImA = (0, 0, \ldots, 0)$.

Suppose $y \neq 0$ such that $y \in KerA \cap ImA$.

$$\begin{aligned} Ax = y &\implies A^2x = 0, \text{ (since } y \in \ KerA) \\ &\implies A(Ax) = 0, \\ &\implies y = Ax = 0. \text{ (since } ImA \mapsto \mathbb{R}^n \text{ is invertible)} \end{aligned}$$

Thus $KerA \cap ImA = (0, 0, \ldots, 0)$, by *rank nullity theorem* $ImA \bigoplus KerA = \mathbb{R}^n$.
$2 \implies 3$
Given that $KerA \cap ImA = (0, 0, \ldots, 0)$. By *rank nullity theorem*

$$\text{Rank}A^2 + \text{Nullity}A^2 = \text{Rank}A + \text{Nullity}A = n.$$

We will show that Nullity$A$=NullityA^2.
let $u \in KerA$, so $Au = 0 \implies A^2u = 0$, thus $KerA \subset KerA^2$.
Now Let $v \in KerA^2 \implies A^2v = 0$ or $A(Av) = 0$, so $Av \in KerA$ and $Av \in ImA$. As $KerA \cap ImA = (0, 0, \ldots, 0)$, thus $Av = 0$. Hence $KerA^2 \subset KerA$.
$4 \implies 2$
We know from *linear algebra*, column space is the image space or the span of the column vectors.
Given that K is the column space consists a basis of $KerA$ implies $ImK = KerA$. Similarly $ImC = KerA^T$. Suppose $KerA \neq 0$. Then $\det(C^TK) \neq 0$ holds if and only if $C^TKx \neq 0$ for all $x \neq 0$ as $Kx \in ImK = KerA$ thus $C^Ty \neq 0$ for all $y \in KerA$, $y \neq 0$. So we conclude $KerA \cap KerC^T = \{0\}$. Fact $KerA^T = (ImA)^\perp$. Since ImC= $KerA^T \implies (KerC^T)^\perp = (ImA)^\perp$, since both are finite-dimensional, we get $KerC^T = ImA$ or $KerA \cap ImA = \{0\}$. □

Definition 8.20. *A square matrix satisfying the conditions of 8.19 is called range regular.*

Lemma 8.21. *Suppose A is a real $n \times n$ matrix of rank $n-1$ and x, y are the vectors generating the kernel and cokernel of A, respectively. Then A is the range regular if and only if $< x, y > \neq 0$. As a special case, A is Ducci matrix if and only if there exists a sign matrix S such that $< Sx, y >= 0$*

Proof. As A is singular, by condition 4 of 8.19, take K and C to be single column x and y respectively. Hence $C^T K = (< x, y >) \neq 0$ this proves first claim of lemma.
$\Rightarrow$ Suppose A is trap matrix, then there exist sign matrix S such that the map $x \mapsto A(Sx)$ is not invertible on ImA which is contrapositive statement to condition 1 of 8.19, thus $\det C^T K =< Sx, y >= 0$.
$\Leftarrow$ Suppose $< Sx, y >= 0$ then

$$\begin{aligned}
&Sx \in (KerA^T)^{\perp} = ImgA. \\
&Sx = Au, \quad \text{for some } u \in \mathbb{R}^n. \\
&x = S^{-1}Au, \quad (S^{-1} = S) \\
\Longrightarrow\ &x = SAu. \\
&Ax = 0, \quad (x \in KerA) \\
\Longrightarrow\ &AS(Au) = 0.
\end{aligned}$$

Since, $Au \in ImA$ is a non-trivial kernel, the map $x \mapsto ASx$ is non-invertible on ImA. □

For matrix $A = A_{0,n}$, the sum of all column is 0, thus $KerA$ and $(KerA)^T$ is generated by $v = (1, 1, \dots, 1)$, from previous lemma $A_{0,n}$ is trap matrix if there is a sign tuple $s = (s_1, s_2, \dots, s_n)$ such that $\sum_{i=1}^{n} s_i = 0$, which is possible if and only if n is even number. However, we know $A_{0,n}$ is $\mathbb{Z}-$Duuci for $n = 2^k$.

Lemma 8.22. *Let A and D be real $n \times n$ matrix, suppose that D is invertible and $D|x| = |Dx|$ for all $x \in \mathbb{R}^n$. Then if A is Ducci matrix so does $B = D^{-1}AD$.*

Proof. Let $f(x) = Dx$, f is invertible since D is invertible also $\sigma_B : u \mapsto B|u|$. Then

$$\sigma_B = f^{-1} \circ \sigma_A \circ f.$$

Because

$$\begin{aligned}
\sigma_B(u) &= D^{-1}AD|u|, \\
&= D^{-1}A|Du|, \quad sinceD|x| = |Dx| \\
&= f^{-1} \circ \sigma_A \circ f(u).
\end{aligned}$$

Then, $\sigma_B^k(u) = f^{-1} \circ (\sigma_A)^k \circ f(u)$. Hence *signed Ducci sequence* corresponding to A and B matrix will terminate after same number of steps. Thus B is also a *Ducci matrix.* $\square$

With the help of 8.22 we will emphasize two special cases.

Case 1: Consider diagonal matrix $D = \begin{pmatrix} d_1 & . & . & \mathbf{0} \\ . & d_2 & . & . \\ . & . & . & . \\ \mathbf{0} & . & . & d_n \end{pmatrix}$, where $d_i > 0$ satisfy $D|x| = |Dx| \quad \forall \quad x \in \mathbb{R}^n$. Suppose A is *Ducci matrix* and $kerA$ is generated by $x = (x_1, x_2, \ldots, x_n)$, then as $B = D^{-1}AD$, $KerB$ is generated by $y = (\frac{x_1}{d_1}, \ldots, \frac{x_n}{d_n})$, taking $d_i = x_i$, we can create *Ducci matrxi* B such that $KerB = (1, 1, \ldots, 1)$ thus making row sums zero of matrix B.

Example 8.23.

$$A = \begin{pmatrix} 2 & 1 & -3 \\ 1 & 3 & -4 \\ 0 & 5 & -5 \end{pmatrix}.$$

$$B = D^{-1}AD = \begin{pmatrix} 1/d_1 & 0 & 0 \\ 0 & 1/d_2 & 0 \\ 0 & 0 & 1/d_3 \end{pmatrix} \begin{pmatrix} 2 & 1 & -3 \\ 1 & 3 & -4 \\ 0 & 5 & -5 \end{pmatrix} \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}.$$

$$B = \begin{pmatrix} 2 & d_2/d_1 & -3d_3/d_1 \\ d_1/d_2 & 3 & -4d_3/d_2 \\ 0 & 5d_2/d_3 & 5 \end{pmatrix}.$$

Case 2 *Permutation Matrix* is matrix obtained by permuting rows of *Identity matrix.* Take D a *Permutation Matrix*, it also satisfy $D|x| = |Dx|$.

8.3 The Reduced Ducci Map

We observe that $\delta_A(cx) = |c|\delta_A(x)$ and $\sigma_A(cx) = |c|\sigma_A(x)$, so the *Ducci sequence* of x and cx is same upto a constant factor. Therefore we define an equivalence relation on R^n as follows; $x \sim y$ iff $y = cx$ for some non-zero x and $[x]$ denotes the equivalence class of x. Thus, we conclude that the iterative behavior of σ_A on equivalent vectors will be identical.

Note that the quotient space $\mathbb{R}^n/\sim$ by this relation, with the *quotient topology* is a *real projective space* $\mathbb{R}P^{n-1}$ union $\mathbf{0}$. *real projective space* n space $\mathbb{R}P^n$ is homeomorphic to an n-sphere with antipodal points identified.

$$n\text{-sphere } \; S^n = \{x \in \mathbb{R}^{n+1} \; : \; ||x|| = 1\}.$$
$$\mathbb{R}P^n \cong S^n/x \sim -x \; .$$

Definition 8.24. *Let A be real valued $n \times n$ matrix, and $\mathbb{P}_A = ImA/\sim$. The map $\rho_A \; : \; \mathbb{P}_A \to \mathbb{P}_A$ defined by $\rho_A([x]) = [\sigma_A(x)]$ is called reduced Ducci map of A.*

The map ρ_A is well defined. If $x \sim y$ i.e. $x = \lambda y$, $\sigma_A(x) = |\lambda|A|y|$. Hence $\sigma_A(x) \sim \sigma_A(y)$. Since ImA is r-dimensional real vector space, where $r = \text{rank}(A)$. Then $\mathbb{P}_A = ImA/\sim \cong \mathbb{R}P^{r-1} \cup \{\mathbf{0}\}$. For any $x \in \mathbb{P}_{\mathbb{A}}$ *Ducci sequence* and *Ducci length* are well-defined notation. The sets $R_s = \{[x] \in \mathbb{P}_A \; : \; x \in R_s \cap ImA\}$ defines regions in $\mathbb{P}_A$ where ρ_A is quotient of a linear map.

Our next task is calculating ρ_A for specific matrix A. In this direction, first, we find the matrix representation of the maps $(x \mapsto ASx)|ImA$. Second, we will choose a representation for $\mathbb{R}P^{r-1}$, then calculate an explicit form of ρ_A.

Step 1 We will stick to the approach that we have used in example 8.18. We will choose matrix B whose column consists basis for ImA and for a sign matrix S calculate $B^{-1}ASB$.

Step 2 We will represent the line in ImA by their intersection with a hyperplane $H \subset ImA$.

The following example will summarize the theory.

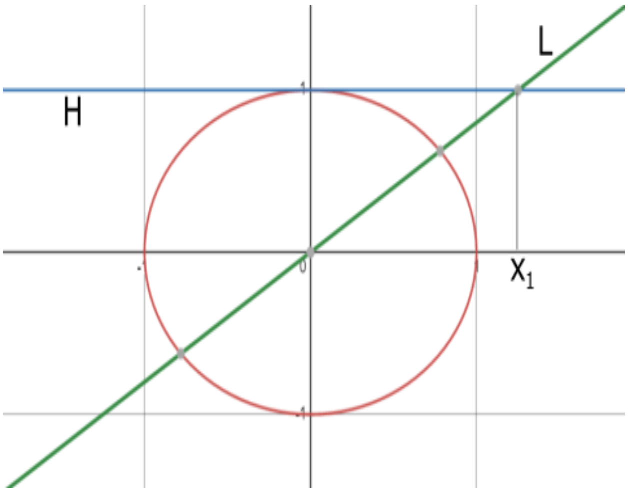


Figure 8.1: The real projective space $\mathbb{R}P^1 \cong S^1 \,/x \sim -x$.

Example 8.25. Choose $H = \{(x_1, x_2) \in ImA \ : \ x_2 = 1\}$. The idea is for any $x = (x_1, x_2)^T \in ImA, \ \ x_2 \neq 0$, $[x]$ can be identified by $[(t, 1)] \in H$, where $t = x_1/x_2$. For above diagram, $H = \{h_t, t \in \mathbb{R}\}$, $h_t = t(1, 0)^T + (0, 1)^T = (t, 1)^T$.

Example 8.26. We will calculate ρ_A for $A_2 = \begin{pmatrix} 2 & 1 & -3 \\ 1 & 3 & -4 \\ 0 & 5 & -5 \end{pmatrix}$. Basis for $ImA = \{(1, 0, -1)^T, (0, 1, 2)^T\}$ and basis for $(ImA)^{\perp} = KerA^T = \{(1, -2, 1)^T\}$. Since $ImA \bigoplus KerA^T = \mathbb{R}^3$, thus matrix $B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -2 \\ -1 & 2 & -1 \end{pmatrix}$.

For sign matrix $S = \begin{pmatrix} s_1 & 0 & 0 \\ 0 & s_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\quad B^{-1}ASB = \begin{pmatrix} 2s_1 + 3 & s_2 - 6 & 2s_1 - 2s_2 - 3 \\ s_1 + 4 & 3s_2 - 8 & s_1 - 6s_2 - 4 \\ 0 & 0 & 0 \end{pmatrix}$.

We choose $H = \{h_t : \ t \in \mathbb{R}\}$, where $h_t = t \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} t \\ 1 \\ 2 - t \end{pmatrix}$.

$t \in \mathbb{P}_A$ corsponds to $h_t \in ImA$. For $s = (1,1,1)$, we will construct region R_s as follows; from explicit form of h_t we get $t \geq 0 \cap 2 - t \geq 0 \implies 0 \leq t \leq 2$, and matrix $A^{[s]} = \begin{pmatrix} 5 & -5 \\ 5 & -5 \end{pmatrix}$. This matrix is not invertible, so R_s is a trap region. For $v = (t,1)^T \in h_t$, $A^{[s]}v = (1,1)^T \in h_t$ gives $t = 1 \in \mathbb{P}_A$. The same calculation with other sign matrices gives explicit behavior of ρ_A as shown in the table.

s	$(1,1,1)$	$(-1,1,1)$	$(-1,1,-1)$	$(1,1,-1)$
R_s	$0 \leq t \leq 2$	$t \leq 0$	no region	$2 \leq t$
$A^{[s]}$	$\begin{pmatrix} 5 & -5 \\ 5 & -5 \end{pmatrix}$	$\begin{pmatrix} 1 & -5 \\ 3 & -5 \end{pmatrix}$	$\begin{pmatrix} 5 & -7 \\ 5 & -11 \end{pmatrix}$	$\begin{pmatrix} 1 & -7 \\ 3 & -11 \end{pmatrix}$

The map $\rho_A \ : \mathbb{P}_A \to \mathbb{P}_A$ is

$$\rho_{A_2}(t) = \begin{cases} \frac{t-5}{3t-5} & \text{if } t \leq 0, \\ 1 & \text{if } 0 \leq t \leq 2, t \neq 1, \\ \frac{t-7}{3t-11} & \text{if } 2 \leq t \text{ and } t \neq \frac{11}{3}, \\ \infty & \text{if } t \neq \frac{11}{3}, \\ \frac{1}{3} & \text{if } t = \infty, \\ 0 & \text{if } t = 1 \text{ or } t = 0. \end{cases}$$

Lemma 8.27. *Matrix* $A_2 = \begin{pmatrix} 2 & 1 & -3 \\ 1 & 3 & -4 \\ 0 & 5 & -5 \end{pmatrix}$ *is a Ducci matrix.*

Proof. From explicit formula ρ_{A_2}, When $0 \leq t \leq 2$, $t \neq 0$, $\rho_{A_2} = 1$. So element in this region takes at most 1 steps to reach zero. When $t \leq 0$, $0 \leq \rho_{A_2} \leq 1$, after two step point from this region reach zero. For region $t \geq 2$, there is a unique repelling fixed point t_*, can be calculated by $\rho_{A_2}(t_*) = t_*$. Thus except for the fixed point, all points eventually reach one of the two regions. Hence A_2 is a *Ducci* matrix. □

Lemma 8.28. *Let* t_n *is a sequence define recursively,* $t_0 = 2$, $t_n = \frac{11t_{n-1}-7}{3t_{n-1}-1}$ *for* $n > 0$, *with* $t_\infty = \lim_{n\to\infty} t_n = 2 + \frac{\sqrt{15}}{3}$. *Then for* $x_n = (t_n, 1, t_n - 2)^T$, $\lambda_{A_2}(x_n) = n + 2$. *The Ducci sequence of* $x_\infty = \lim_{n\to\infty} x_n = (t_\infty, 1, -2)^T$ *does not terminate.*

Proof. In the interval $2 \leq t \leq 11/3$, $\rho_{A_2}(t)$ is invertible, where $\rho_{A_2}^{-1}(t) = \frac{11t-7}{3t-1}$. Thus sequence defined as $t_0 = 2$, $t_n = \rho_{A_2}^{-1}(t_{n-1})$. Since t_n is an increasing sequence $t_n > 2$, then $x_n = |y_n|$, where $y_n = (t_n, 1, 2 - t_n) \in ImA$. Thus $[\sigma_A(y_n)] = [y_{n-1}] \Rightarrow [\sigma_A(y_{n-1})] = [y_{n-2}]$ and so on and $\lambda_{A_2}(x_0) = 2$. Thus $\lambda_{A_2}(x_n) = n + 2$.
Given $t_\infty = 2 + \frac{\sqrt{15}}{3}$, it is unique repelling fixed point t_* of $\rho_{A_2}(t)$. $t_* = 2 + \frac{\sqrt{15}}{3}$ correspond to vector $x_* = (6 + \sqrt{15}, 3, 3 - \sqrt{15})$, which is an eignvector of AS, where S is sign matrix correspond to sign tuple $(1, 1, -1)$ and $|x_*|$ is only exception vector of A_2. □

8.4 Families of Ducci Matrices

In the previous section, we observed that if $t = t_*$, the orbit of t is driven away until it reaches one of the traps. This section will show a similar phenomenon for 4 × 4 *Ducci* matrices.
For $p \in \mathbb{R}$, define

$$A_c(p) = \begin{pmatrix} p+1 & -1 & 1-p & -1 \\ -1 & p+1 & -1 & 1-p \\ 1-p & -1 & p+1 & -1 \\ -1 & 1-p & -1 & p+1 \end{pmatrix}.$$

Subscript c indicate $A = A_c(p)$ is a circulant matrix. First, we will determine the *reduced Ducci map* ρ_A.

Following the same procedure. As $\mathbb{R}^4 = ImA \bigoplus CokerA$. $B = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$.

$$ImA = \left\{ c_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}, c_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \end{pmatrix}, c_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix} \right\}, \; H = \{h_{(x,y)} : \; x, y \in \mathbb{R}\},$$

then $(x, y) \in \mathbb{P}_A$ corresponds to $h_{(x,y)} = xc_1 + yc_2 + c_3 \in ImA$.
ImA consist of vectors $v = (x, y, 1, -1 - x - y)^T$, corresponding region R_i can be calculated by inequalities $siv_i \geq 0$. We will construct region for $s = (1, 1, 1, 1)$, same

argument will work for constructing other region and getting *reduced Ducci map*. For $S_1 = (-1,1,1,1) \implies -x \geq 0 \cap y \geq 0 \cap -1-x-y \geq 0$ will give region R_1 and $A^{[1]} = (B^{-1}AS_1B)|ImA = \begin{pmatrix} -p & 0 & 2-p \\ p & 2p & p-2 \\ p & 0 & p+2 \end{pmatrix}$.

In region R_i, the *reduced Ducci map* ρ_A given by $[v] \mapsto [A^i v]$, if we consider $[(x,y,z)^T]$ by $[(\frac{x}{z},\frac{y}{z})] \in \mathbb{R}^2$, for region R_1, we get

$$\rho_A(x,y) = \left(\frac{-p-px+2}{p+px+2}, \frac{p+px+2py-2}{p+px+2}\right)$$

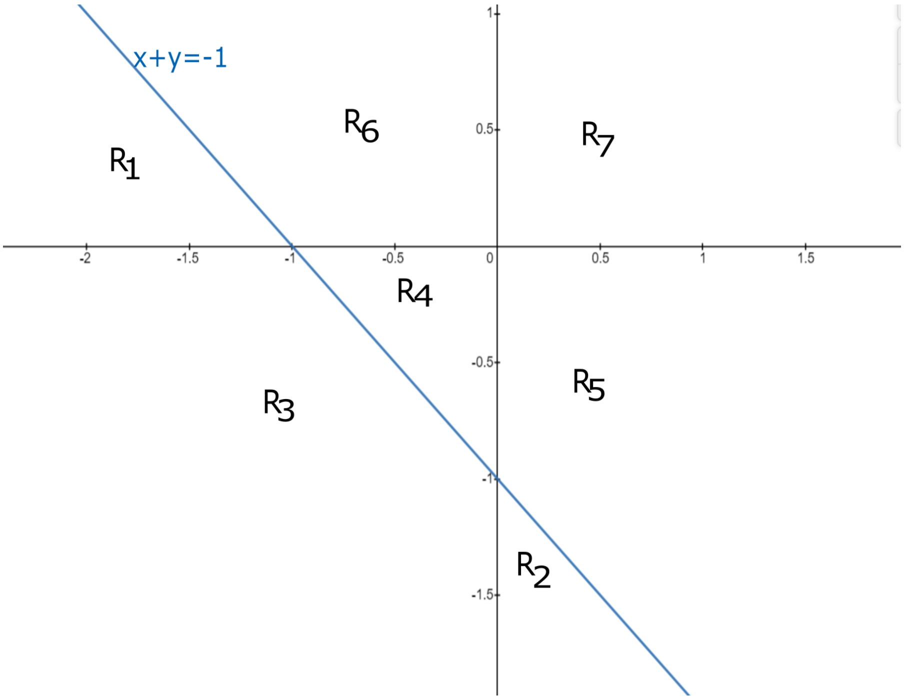


Figure 8.2: Seven Region of $\mathbb{P}_{A_c}$

The *reduced Ducci map* $\rho_A : \mathbb{P}_A \to \mathbb{P}_A$ for matrix $A = A_c(p)$ is,

$$\rho_A(t) = \begin{cases} (\frac{-p-px+2}{p+px+2}, \frac{p+px+2py-2}{p+px+2}) & (x+y) \leq -1 \cap 0 \leq y \ \ (R_1), \\ (\frac{2x-p+2y+px+2}{p+2x+2y-px+2}, \frac{-2x+p-2y+px-2}{p+2x+2y-px+2}) & (x+y) \leq -1 \cap 0 \leq x \ \ (R_2), \\ (\frac{p-2y+px-2}{p+2y+px+2})(-1,1) & (x+y) \leq -1 \cap x \leq 0 \cap y \leq 0, (x,y) \neq (-1,-1) \ \ (R_3), \\ (\frac{-p-2x-px}{p-2x+px}, \frac{-p+2x-px-2py}{p-2x+px}) & -1 \leq (x+y) \cap x \leq 0 \cap y \leq 0 \ \ (R_4), \\ (-1, \frac{x+2y+1}{x-1}) & -1 \leq (x+y) \cap 0 \leq x \cap y \leq 0, (x,y) \neq (-1,-1) \ \ (R_5), \\ (\frac{p+2x+2y+px}{p-2x-2y+px}, -1) & -1 \leq (x+y) \cap x \leq 0 \cap 0 \leq y, (x,y) \neq (-1,1) \ \ (R_6), \\ (\frac{p+2y-px}{2y-p+px}, \frac{p-2y+px}{2y-p+px}) & 0 \leq x \cap 0 \leq y. \end{cases}$$

The above map is calculated by $(\frac{x_1}{x_3}, \frac{x_2}{x_3})$ from $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = A^{[i]} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$.

Theorem 8.29. *For every $p \in \mathbb{R}_+$, the matrix $A = A_c(p)$ is a Ducci matrix. If $p \neq 0$, the reduced Ducci map ρ_A has four exception points in $\mathbb{P}_A$ and these are fixed points..*

Proof. Matrices $A^{[3]}, A^{[5]}, A^{[6]}$ used for explicit representation of ρ_A are non-Invertible , so region $3, 5, 6$ are traps. If $u \in \mathbb{P}_A$ is in one of these regions, then u has a length at most three. This can be shown as follows: For $u \in R_3$, $w = \rho_A(u)$ lie on the line $L:\ x + y = 0$, $\rho_A(x, -x) = (-1, -1)$, and $\rho_A(-1, -1) = (0.0)$. Region 5 is mapped to line $x = -1$ and region 6 mapped to $y = -1$, making the length of each element in the regions no more than 3.

Region R_4 is a traingle, having corners $w_1 = (0, 0), w_2 = (0, -1), w_3 = (-1, 0)$ as shown in the figure below.

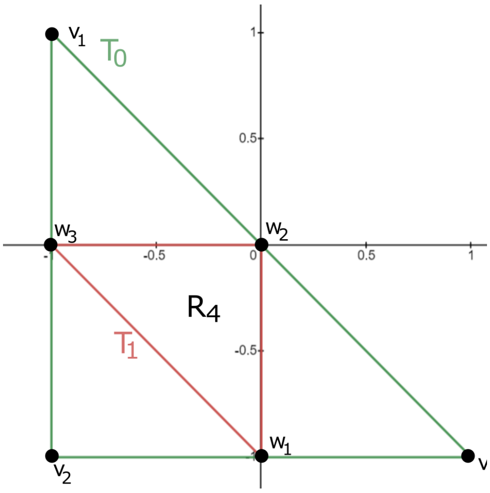


Figure 8.4: Region R_4

Denote $\rho_A|R_4$ by f, that is, $f(x,y) = (\frac{-p-2x-px}{p-2x+px}, \frac{-p+2x-px-2py}{p-2x+px})$. The image $f(R_4)$ is a triangle call it T_0 having vertices $f(w_1) = v_1 = (-1,1)$, $f(w_2) = v_2 = (-1,-1)$ and $f(w_3) = v_3 = (1,-1)$. As A^4 is invertible, region R_4 is not a trap, therefore f is a bijective map from R_4 to $T_0 = f(R_4)$ and it's inverse is $g(x,y) = f^{-1}(x,y) = (\frac{-(p+px)}{p-2x+px+2}, \frac{-(2y+2)}{p-2x+px+2})$.
Consider the sequence of triangles $T_n = g^n(T_0)$. We can deduce from the figure 8.4 that vertices of T_1 lie on the side of T_0, thus for the sequence of triangles lie on the sides of T_{n-1} for $n > 0$. Now, for each n, Tn consist of four smaller triangles $T_n^i \ \{i = 0,1,2,3\}$, $T_n^0 = T_{n+1}$ contains the corner of $g^n(v_i)$, where $i = 0,1,2,3$. In figure 8.4, $T_0^0 = T_1$. As g is inverse of f, triangle T_n^i is mapped f bijectively to T_{n-1}^i, where $(n > 0, i = 0,1,2,3)$.
Since T_n is a sequence of shrinking triangles, there is a fixed point $t_*(p) = (x_*, y_*)$, which can be calculated by $g(x,y) = (x,y)$. We get $t_*(p) = (\frac{r-p-1}{p-2}, \frac{3-r}{2p-4})$, where $r = \sqrt{4p+1}$ and $t_*(2) = (-\frac{1}{3}, -\frac{1}{3})$. Now, $\lim_{p\to 0} t_*(p) = (0, -\frac{1}{2})$ and $\lim_{p\to\infty} t_*(p) = (0,-1)$. Thus set all all fixed points lie on the line connecting these two points.
Now for any $v \in T_1 \backslash \{t_*(p)\}$, there exist some n such that $v \in T_n \backslash T_n^0$, this is because v is not a fixed point and T_n is sequence of shrinking triangles. Then $v \in T_n^i$ for some $i \in \{1,2,3\}$, or $f^l(x) \in T_{n-l}^i$ for $l = 0,1,2,3\ldots,l$, for $l = n$, all the points lie in T_0 which itself lie in trap regions $3,5,6$ and from there it takes at most three steps to

terminate.

We know regions $1, 2, 4, 7$ are not traps since matrices $A^{[1]}, A^{[2]}, A^{[4]}, A^{[7]}$ are invertible. We verified that the fixed point in R_4 is the only exception point. Similarly, we can verify that corresponding to each non-trap region fixed point is the only exception point. Hence, there are four exception points. □

Appendix

Theorem 8.30. *The Ducci map $D : \mathbb{R}^n \to \mathbb{R}^n$ defined as*

$$D(b_1, b_2, \ldots, b_n) = (|b_1 - b_2|, |b_2 - b_3|, \ldots, |b_n - b_1|).$$

is continuous.

Proof. Let $x = (x_n) \in \mathbb{R}^n$ and $y = (y_n) \in \mathbb{R}^n$ and $\epsilon > 0$ is given,

$$\begin{aligned} D(x) &= (|x_1 - x_2|, |x_2 - x_3|, \ldots, |x_n - x_1|), \\ D(y) &= (|y_1 - y_2|, |y_2 - y_3|, \ldots, |y_n - y_1|), \\ D(x) - D(y) &= (|x_1 - x_2| - |y_1 - y_2|, \ldots, |x_n - x_1| - |y_n - y_1|). \end{aligned}$$

Now observing that

$$\begin{aligned} ||x_i - x_{i+1}| - |y_i - y_{i+1}|| &\leq |x_i - x_{i+1} - y_i + y_{i+1}| \quad \text{by } \ ||a| - |b|| \leq |a - b| \\ &\leq |x_i - y_i| + |x_{i+1} - y_{i+1}| \\ &\leq ||x - y||_2 + ||x - y||_2 \\ &= 2||x - y||_2 \\ &\leq 2\delta, \ \text{ where } \ ||x - y||_2 \leq \delta. \end{aligned}$$

So,

$$\begin{aligned} ||D(x)-D(y)||_2 &= \sqrt{\sum_{i=1}^{n}(|x_i - x_{i+1}| - |y_i - y_{i+1}|)^2} \\ &\leq \sqrt{\sum_{i=1}^{n}(2\delta)^2} \\ &= 2\sqrt{n}\delta = \epsilon. \end{aligned}$$

Choose $\delta = \frac{\epsilon}{2\sqrt{n}}$. □

Lemma 8.31. ${}^{2^m}C_r = \binom{2^m}{r} \equiv 0 \bmod 2$, *where* $0 < r < 2^m$.

Proof.

$$\begin{aligned} \binom{2^m}{r} &= \frac{2^m!}{r!\,(2^m - r)!} \\ &= \frac{2^m}{r}\left[\frac{(2^m-1)\ldots..(2^m-(r-1))}{(r-1)!}\right]. \end{aligned}$$

Fact 1: The product of n consecutive integers is divisible by $n!$.
Fact 2: $\binom{2^m}{r}$ is a positive integer for each r.
Thus, letting $K = \left[\frac{(2^m-1).....(2^m-(r-1))}{(r-1)!}\right]$

$$\binom{2^m}{r} = \frac{2^m}{r}K.$$

- If r is odd then $r|K$.
- If r is even and $r < 2^m$, to make $\binom{2^m}{r}$ an integer r can have at most $m-1$ factors of 2. Thus in this case $\binom{2^m}{r} = 2.\gamma \equiv 0 \bmod 2$, where γ is a constant.

□

Bibliography

[1] Burmester, M., Forcade, R., & Jacobs, E. (1978) *Circles of numbers*, Glasgow Mathematical Journal, 19(2), 115–119.

[2] Ludington A.L. (1981) *Cycles of differences of integers*, Journal of Number Theory, 13, 255–261.

[3] Ehrlich, A. (1990) *Periods in Ducci's n-number game of differences*, Fibonacci Quart, 28(4), 302–305.

[4] Schinzel, A., Misiurewicz, M. (1988). *On n numbers on a circle.* In Hardy-Ramanujan Journal: Vol. Volume 11-1988

[5] Marc Chamberland (2003) *Unbounded Ducci Sequences*, Journal of Difference Equations and Applications, 9:10, 887-895, DOI: 10.1080/1023619021000041424

[6] Breuer, F., Shparlinski, I. (2020). *Lower bounds for periods of Ducci sequences.* Bulletin of the Australian Mathematical Society, 102(1), 31-38.

[7] Clausing, A. (2018). *Ducci matrices.* The American Mathematical Monthly, 125(10), 901-921.

[8] Breuer, F., Lötter, E., Van Der Merwe, B. (2007). *Ducci-sequences and cyclotomic polynomials.* Finite Fields and Their Applications, 13(2), 293-304.