國立政治大學 應用數學系

碩士學位論文

Diffy 六邊形之探討

A Study about Diffy Hexagons

碩士班學生：王偉名　撰

指導教授：李陽明　博士

中華民國 103 年 6 月 25 日

致謝

水井的外面，是怎麼樣的世界?
那是為了明白，值得費盡心思去相見的東西嗎？
水井的外面，是怎麼樣的世界？
那是數度墜落，依然充滿魅力值得挑戰的嗎？
水井的外面，是怎麼樣的世界？
我們一起為了明白而努力，一起品嘗掉下時的痛苦吧。
在最後來臨的世界，那裡一定是很棒的世界。
即使那裡只是水井的底端。
踏出水井之外的決心，是通往新世界的鑰匙。
不論踏得出去或踏不出去，
新的世界一定會來臨…

Frederica Bernkastel

首先，我要感謝生我育我的父母。如果沒有他們的支持與鼓勵，就沒有今天的我。

接下來，我要感謝的是政大應數系對我的栽培，把我從一個完全不懂得如何寫好一個證明的毛頭小子，栽培到足以寫出一份碩士論文的程度。在這其中，我要特別感謝我的指導老師李陽明老師：在我剛進入碩士班時，老師給了我人生中第一個擔任 TA 的機會，讓我成為老師在大學部所開設的離散數學課程的 TA，並從此開啟了我碩士班的 TA 生涯。在擔任 TA 的過程中，我學習到了不少東西，也更加堅定了我將來想繼續從事教學與研究工作的決心。此外，當我陷入低潮時，老師總是對我不離不棄，並且適時的給予我鼓勵與幫助，甚至不吝惜撥出暑假休息的時間陪我釐清問題的所在並將問題一一解決，這也是我在日後的種種考試中能夠平安順利通過的主要原因，真的非常謝謝老師。

謹以此論文獻給愛我的父母與我愛的母校

王偉名　謹誌于
國立政治大學應用數學系
中華民國一百零三年六月

中文摘要

在這篇論文裡，我們研究 Diffy 六邊形。本文一開始將 Diffy 六邊形視為 Ducci 序列，然後我們討論關於 Ducci 序列的一些性質。然而，Diffy 六邊形事實上是可以旋轉與翻轉的，但是，我們所考慮的 Ducci 序列並不具備這樣的性質。所以，在本文的最後，我們討論在考慮旋轉與翻轉情況下的 Ducci 序列。

關鍵字：循環、Diffy 六邊形、Ducci 過程、Ducci 序列、週期、相似循環

Abstract

In this thesis, we study the Diffy Hexagons: Initially, we regard a Ducci sequence as a Diffy Hexagon game and discuss some properties about Ducci sequences. However, a Ducci sequence isn't actually a Diffy Hexagon game due to the fact that regular hexagons has some symmetries under rotations and reflections, but the Ducci sequences don't. So, we apply an identification in the end.

Keywords: Cycles, Diffy Hexagons, Ducci processes, Ducci sequences, Periods, Similar cycles

Contents

Chapter 1

Introduction

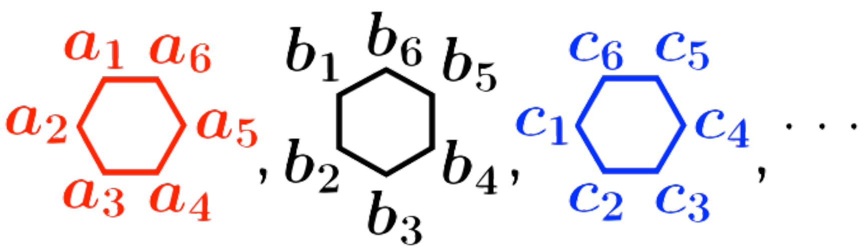
The Diffy Hexagons which are generalized Diffy Boxes (see [3]) are games with the following procedures:

Step 1. Arrange six nonnegative integers around a regular hexagon.

Step 2. Produce another regular hexagon of six nonnegative integers from the one obtained in **Step 1**: For each adjacent pair of numbers, compute the absolute value of their difference and place it between them. Then, remove the original numbers and the original regular hexagon. Finally, form the new regular hexagon with the remaining numbers.

Step 3. To obtain a sequence of regular hexagons of six nonnegative integers by performing **Step 2.** over and over.

Figure 1.1: Diffy Hexagon



Without loss of generality, we denote a regular hexagon of six nonnegative integers as Figure 1.1.

From now on, let N be a positive integer with $N \geq 2$. We denote the set of all N-tuples of nonnegative integers by A_N. Define $D : A_N \to A_N$ by

$$D(a_1, a_2, \cdots, a_N) = (\,|a_1 - a_2|, \cdots, |a_{N-1} - a_N|, |a_N - a_1|\,)$$

for all $(a_1, a_2, \cdots, a_N) \in A_N$. Then, D is a well-defined function.

Definition 1.1. The function $D : A_N \to A_N$ defined by

$$D(a_1, a_2, \cdots, a_N) = (\,|a_1 - a_2|, \cdots, |a_{N-1} - a_N|, |a_N - a_1|\,)$$

for all $(a_1, a_2, \cdots, a_N) \in A_N$ is called a *Ducci process*.

Definition 1.2. Let $\vec{a} = (a_1, a_2, \cdots, a_N) \in A_N$. A sequence of the form that $\vec{a}, D(\vec{a}), D^2(\vec{a}), \cdots$ is called the *Ducci sequence of* $\vec{a}$. On the other hand, we denote $\vec{a}$ by $D^0(\vec{a})$.

Remark 1.3. Note that a 6-tuple of nonnegative integers is regarded as written in a regular hexagon, and hence a Ducci sequence of 6-tuples in A_6 is regarded as a sequence of regular hexagons, that is, a Diffy Hexagon game.

Chapter 2

Ducci Sequences

Lemma 2.1. *Let $\vec{a} \in A_N$. Then, there are nonnegative integers n, k with $n > k$ such that $D^n(\vec{a}) = D^k(\vec{a})$.*

Proof.

Write $\vec{a} = (a_1, a_2, \cdots, a_N)$

Let $M = \max\{a_1, a_2, \cdots, a_N\}$

$\Longrightarrow$ There are at most $(M+1)^N$ different N-tuples which are obtained by performing Ducci processes on $\vec{a}$, and hence there are nonnegative integers n, k with $n > k$ such that $D^n(\vec{a}) = D^k(\vec{a})$ □

Definition 2.2. Let $\vec{a} \in A_N$. Suppose that n is the positive integer such that $\vec{a}, D(\vec{a}), D^2(\vec{a}), \cdots,$ $D^{n-1}(\vec{a})$ are all distinct and $D^n(\vec{a}) = D^k(\vec{a})$, where $0 \le k \le n-1$. We define the *period of $\vec{a}$* to be $n-k$ and the $(n-k)$-*cycle of $\vec{a}$* (or simply the *cycle of $\vec{a}$*) to be $D^k(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^{n-1}(\vec{a})$.

Definition 2.3. Let $\vec{a} \in A_N$. The largest component of $\vec{a}$ is denoted by $\max \vec{a}$.

Remark 2.4. If $0 \le x, y \le M$, then $|x-y| \le M$.

Proof. Note that $-M \le x-y \le M$, then we obtain $|x-y| \le M$ □

Lemma 2.5. *Let $\vec{a} \in A_N$. For all nonnegative integers r, s with $r \ge s$, then we have*

$$\max D^r(\vec{a}) \le \max D^s(\vec{a}).$$

Proof.

Given nonnegative integers r, s with $r \geq s$

If $r = s$, there is nothing to prove

Now, we may assume that $r > s$

It suffices to show that $\max D^{s+1}(\vec{a}) \leq \max D^s(\vec{a})$:

Write $D^s(\vec{a}) = (x_1, x_2, \cdots, x_N)$ and $D^{s+1}(\vec{a}) = (y_1, y_2, \cdots, y_N)$, where

$$y_1 = |x_1 - x_2|, y_2 = |x_2 - x_3|, \cdots, y_{N-1} = |x_{N-1} - x_N|, y_N = |x_N - x_1|$$

$\because 0 \leq x_1, x_2, \cdots, x_N \leq \max D^s(\vec{a})$

$\therefore$ By Remark 2.4, $y_i \leq \max D^s(\vec{a})$ for all $i = 1, 2, \cdots, N$

$\implies \max D^{s+1}(\vec{a}) \leq \max D^s(\vec{a})$ □

Lemma 2.6. *Let $\vec{a} \in A_N$. Suppose $D^k(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^{n-1}(\vec{a})$ is the $(n-k)$-cycle of $\vec{a}$. Then, $\max D^r(\vec{a}) = \max D^s(\vec{a})$ for $k \leq r, s \leq n-1$.*

Proof.

Given $k \leq r, s \leq n-1$

We may assume that $r \leq s$

If $r = s$, then it is trivial

Suppose $r < s$, then $\max D^s(\vec{a}) \leq \max D^r(\vec{a})$ by Lemma 2.5

Now, look at the Ducci sequence of $D^s(\vec{a})$:

$$D^s(\vec{a}), D^{s+1}(\vec{a}), \cdots, D^{n-1}(\vec{a}), D^n(\vec{a}) = D^k(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^r(\vec{a})$$

By Lemma 2.5, we know that

$$\max D^r(\vec{a}) \leq \max D^k(\vec{a}) = \max D^n(\vec{a}) \leq \max D^{n-1}(\vec{a}) \leq \max D^s(\vec{a})$$

Therefore, $\max D^r(\vec{a}) \leq \max D^s(\vec{a})$

So, we conclude that $\max D^r(\vec{a}) = \max D^s(\vec{a})$ □

Remark 2.7. If $0 \leq x, y \leq M$ with $|x - y| = M$, then $x, y \in \{0, M\}$ and at least one of them is M.

Proof.

Since $|x - y| = M$, we obtain $x - y = \pm M$

Case 1: $x - y = M$

$\implies M + y = x \leq M$

$\implies y \leq 0$

By assumption, $y \geq 0$

$\therefore y = 0$

$\implies x = M$

Therefore, $x, y \in \{0, M\}$ and at least one of them is M

Case 2: $x - y = -M$

$\implies x + M = y \leq M$

$\implies x \leq 0$

Note that $x \geq 0$

$\therefore x = 0$

$\implies y = M$

Hence, $x, y \in \{0, M\}$ and at least one of them is M □

Lemma 2.8. *Let* $\vec{a} = (a_1, a_2, \cdots, a_N)$, $\vec{b} = (b_1, b_2, \cdots, b_N) \in A_N$ *such that* $D(\vec{b}) = \vec{a}$ *and* $\max \vec{a} = \max \vec{b} = M$. *If* $a_i \in \{0, M\}$, $\forall\, i = 1, 2, \cdots, t$ *and at least one of them is M, then* $b_i \in \{0, M\}$, $\forall\, i = 1, 2, \cdots, t, t+1$ *and at least one of them is M.*

Proof.

We prove it by induction on t:

t=1:

Note that $M = a_1 = |b_1 - b_2|$ and $0 \leq b_1, b_2 \leq M$

By Remark 2.7, $b_1, b_2 \in \{0, M\}$ and at least one of them is M, holds

Suppose $t = 1, 2, \cdots, K$ holds

Then, $t = K + 1$:

By assumption, we have the following four cases:

Case 1: $a_1 = M$ and $a_2 = a_3 = \cdots = a_K = a_{K+1} = 0$

$\implies b_2 = b_3 = \cdots = b_K = b_{K+1} = b_{K+2}$, since $D(\vec{b}) = \vec{a}$

$\because M = a_1 = |b_1 - b_2|$ and $0 \leq b_1, b_2 \leq M$

$\therefore$ By Remark 2.7, $b_1, b_2 \in \{0, M\}$ and at least one of them is M

Therefore, we obtain

$$b_1, b_2, \cdots, b_K, b_{K+1}, b_{K+2} \in \{0, M\}$$

and at least one of them is M, holds

Case 2: $a_{K+1} = M$ and $a_1 = a_2 = a_3 = \cdots = a_K = 0$

$\implies b_1 = b_2 = \cdots = b_K = b_{K+1}$, since $D(\vec{b}) = \vec{a}$

$\because M = a_{K+1} = |b_{K+1} - b_{K+2}|$ and $0 \leq b_{K+1}, b_{K+2} \leq M$

$\therefore$ By Remark 2.7, $b_{K+1}, b_{K+2} \in \{0, M\}$ and at least one of them is M

$\implies b_1, b_2, \cdots, b_K, b_{K+1}, b_{K+2} \in \{0, M\}$ and at least one of them is M, holds

Case 3: $a_1 = a_{K+1} = M$ and $a_2 = a_3 = \cdots = a_K = 0$

$\implies b_2 = b_3 = \cdots = b_K = b_{K+1}$, since $D(\vec{b}) = \vec{a}$

$\because M = a_1 = |b_1 - b_2|$ and $0 \leq b_1, b_2 \leq M$

$\therefore$ By Remark 2.7, $b_1, b_2 \in \{0, M\}$ and at least one of them is M

Note that $M = a_{K+1} = |b_{K+1} - b_{K+2}|$ and $0 \leq b_{K+1}, b_{K+2} \leq M$

By Remark 2.7, we have $b_{K+1}, b_{K+2} \in \{0, M\}$ and at least one of them is M

So, we conclude that

$$b_1, b_2, \cdots, b_K, b_{K+1}, b_{K+2} \in \{0, M\}$$

and at least one of them is M, holds

Case 4: $\exists\, 2 \leq i \leq K$ such that $a_i = M$

$\because a_1, a_2, \cdots, a_i \in \{0, M\}$ and $a_i = M$ with $2 \leq i \leq K$

$\therefore$ By induction hypothesis,

$$b_1, b_2, \cdots, b_i, b_{i+1} \in \{0, M\}$$

and at least one of them is M

Note that $a_i = M, a_{i+1}, \cdots, a_{K+1} \in \{0, M\}$ and

$$\begin{aligned} 2 &= (K+1) - (K-1) \\ &\leq (K+1) - (i-1) \\ &\leq (K+1) - (2-1) \\ &= K \end{aligned}$$

Since Ducci processes are cyclic, we obtain

$$b_i, b_{i+1}, \cdots, b_K, b_{K+1}, b_{K+2} \in \{0, M\}$$

and at least one of them is M, by induction hypothesis

Hence, we conclude that

$$b_1, b_2, \cdots, b_i, b_{i+1}, \cdots, b_K, b_{K+1}, b_{K+2} \in \{0, M\}$$

and at least one of them is M, holds $\square$

Remark 2.9. In Lemma 2.8, we know that $1 \leq t \leq N-1$, since A_N is a collection of N-tuples of nonnegative integers.

Lemma 2.10. *Let $\vec{a} \in A_N$. Suppose $D^k(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^{n-1}(\vec{a})$ is the $(n-k)$-cycle of $\vec{a}$. Then, there are at least $i+1$ cyclic consecutive components of $D^{(n-1)-i}(\vec{a})$ taken from 0 or M such that at least one of them is M, where $M = \max D^k(\vec{a})$.*

Proof.

We prove it by induction on i:

$i = 0$:

By Lemma 2.6, $\max D^{n-1}(\vec{a}) = \max D^k(\vec{a}) = M$

$\Longrightarrow$ there is a component of $D^{n-1}(\vec{a})$ is M

$\Longrightarrow$there is one cyclic consecutive component of $D^{n-1}(\vec{a})$ which is taken from 0 or M such that at least one of them is M, holds

Suppose $i = K$ holds

Then $i = K + 1$:

We must prove that there are at least $(K+1)+1$ cyclic consecutive components of $D^{(n-1)-(K+1)}(\vec{a})$ taken from 0 or M such that at least one of them is M:

Write $D^{(n-1)-(K+1)}(\vec{a}) = (x_1, \cdots, x_N)$ and $D^{(n-1)-K}(\vec{a}) = (y_1, \cdots, y_N)$

$\Longrightarrow$ $D(x_1, x_2, \cdots, x_N) = (y_1, y_2, \cdots, y_N)$

By induction hypothesis, we know that there are at least the $K + 1$ cyclic consecutive components of $D^{(n-1)-K}(\vec{a})$ are taken from 0 or M such that at least one of them is M

Since Ducci processes are cyclic, we may assume $y_1, y_2, \cdots, y_K, y_{K+1}$ are $K + 1$ cyclic consecutive components of $D^{(n-1)-K}(\vec{a})$ which are taken from 0 or M such that at least one of them is M without loss of generality

By Lemma 2.8, we know that $x_1, x_2, \cdots, x_K, x_{K+1}, x_{K+2} \in \{0, M\}$ and at least one of them is M

Hence, we conclude that $x_1, x_2, \cdots, x_K, x_{K+1}, x_{K+2}$ are $(K + 1) + 1$ cyclic consecutive components of $D^{(n-1)-(K+1)}(\vec{a})$ which are taken from 0 or M such that at least one of them is M, holds □

Remark 2.11. In Lemma 2.10, we observe that:

(a) $0 \le i \le N - 1$.

(b) If $i \le \min\{n - k - 1, N - 1\}$, then $D^{(n-1)-i}(\vec{a})$ is in the $(n - k)$-cycle of $\vec{a}$.

Proof.

The first statement follows from the fact that A_N is a collection of N-tuples of nonnegative integers

Now, we prove the last statement:

$\because i \leq \min\{n-k-1, N-1\}$

$\therefore i \leq n-k-1$

By **(a)**, we have $0 \leq i \leq n-k-1$

$\Longrightarrow$

$$\begin{aligned} k &= (n-1)-(n-k-1) \\ &\leq (n-1)-i \\ &\leq (n-1)-0 \\ &= n-1 \end{aligned}$$

Therefore, $D^{(n-1)-i}(\vec{a})$ is in the $(n-k)$-cycle $\square$

Theorem 2.12. *Let $\vec{a} \in A_N$. Suppose $D^k(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^{n-1}(\vec{a})$ is the $(n-k)$-cycle of $\vec{a}$. Then, the components of $D^i(\vec{a})$ are all equal to either 0 or M for each $i = k, k+1, \cdots, n-1$, where $M = \max D^k(\vec{a})$.*

Proof.

By Lemma 2.6, we obtain

$$\max D^j(\vec{a}) = \max D^k(\vec{a}) = M$$

for all $j = k, k+1, \cdots, n-1$

In particular, $D^{n-1}(\vec{a}) = M$

By Lemma 2.10, we know that there are at least N cyclic consecutive components of $D^{(n-1)-(N-1)}(\vec{a})$ taken from 0 or M

$\Longrightarrow$ the components of $D^{n-N}(\vec{a})$ are all equal to either 0 or M which follows from $D^{n-N}(\vec{a}) \in A_N$

Now, look at the Ducci sequence of $D^{n-N}(\vec{a})$:

$$D^{n-N}(\vec{a}), D^{n-N+1}(\vec{a}), \cdots, D^{n-1}(\vec{a}), D^{n}(\vec{a}) = D^{k}(\vec{a}),$$
$$D^{k+1}(\vec{a}), D^{k+2}(\vec{a}), \cdots, D^{n-N-1}(\vec{a}), \cdots$$

$\Longrightarrow$ the components of $D^{k}(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^{n-1}(\vec{a})$ are all equal to either 0 or M, since the components of $D^{n-N}(\vec{a})$ are all equal to 0 or M

Hence, we complete this proof □

Remark 2.13. If $N \neq 2$, then there are $\vec{a}, \vec{b} \in A_N$ with $D(\vec{a}) = \vec{b}$ such that

$$\max \vec{a} = \max \vec{b} = M$$

and the components of $\vec{a}, \vec{b}$ aren't all equal to either 0 or M.

Proof.

Let $M > 1$ be an integer and $\vec{a} = (M, 0, 1, \cdots, 1, 1) \in A_N$

Choose $\vec{b} = D(\vec{a}) \in A_N$

$\Longrightarrow \vec{b} = (M, 1, 0, \cdots, 0, M-1)$

Note that $\max \vec{a} = \max \vec{b} = M$

Therefore, the components of $\vec{a}$, $\vec{b}$ aren't all equal to either 0 or M □

Definition 2.14. Let $\vec{a} \in A_N$ with $\vec{a} \neq \vec{\mathbf{0}}$. If $\vec{a} = (a_1, a_2, \cdots, a_N)$, then $\gcd \vec{a}$ is the number $\gcd(a_1, a_2, \cdots, a_N)$.

Lemma 2.15. *Let $\vec{a} \in A_N$ with $\vec{a} \neq \vec{\mathbf{0}}$ and n be a nonnegative integer. Then, we obtain that* $\gcd \vec{a} \mid \max D^{n}(\vec{a})$.

Proof.

Let $\gcd \vec{a} = d$

Write $\vec{a} = d\vec{b}$ with $\gcd \vec{b} = 1$

Note that $d > 0$ and $D(\vec{a}) = D(d\vec{b}) = dD(\vec{b})$

$\implies D^n(\vec{a}) = D^n(d\vec{b}) = dD^n(\vec{b})$ by induction on n

$\implies d \mid D^n(\vec{a})$

Therefore, we know that $\gcd \vec{a} \mid D^n(\vec{a})$ □

Corollary 2.16. *Let $\vec{a} \in A_N$ with $\vec{a} \neq \vec{\mathbf{0}}$. Suppose that $D^k(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^{n-1}(\vec{a})$ is the $(n-k)$-cycle of $\vec{a}$. Then, the components of $D^i(\vec{a})$ are all equal to either 0 or M for each $i = k, k+1, \cdots, n-1$, where M is a multiple of* $\gcd \vec{a}$.

Proof. It follows from Theorem 2.12 and Lemma 2.15 □

Example 2.17.

Let $d, K \geq 1$ be integers and $\vec{a} = (d, d, d, d, d, Kd) \in A_6$.

Then, we have $\gcd \vec{a} = d$.

Now, apply Ducci processes on $\vec{a}$:

$$\begin{aligned}
D(\vec{a}) &= (0,0,0,0,(K-1)d,(K-1)d) \\
D^2(\vec{a}) &= (0,0,0,(K-1)d,0,(K-1)d) \\
D^3(\vec{a}) &= (0,0,(K-1)d,(K-1)d,(K-1)d,(K-1)d) \\
D^4(\vec{a}) &= (0,(K-1)d,0,0,0,(K-1)d) \\
D^5(\vec{a}) &= ((K-1)d,(K-1)d,0,0,(K-1)d,(K-1)d) \\
D^6(\vec{a}) &= (0,(K-1)d,0,(K-1)d,0,0) \\
D^7(\vec{a}) &= ((K-1)d,(K-1)d,(K-1)d,(K-1)d,0,0) \\
D^8(\vec{a}) &= (0,0,0,(K-1)d,0,(K-1)d) \\
&= D^2(\vec{a})
\end{aligned}$$

So, the period of $\vec{a}$ is 6 and the 6-cycle of $\vec{a}$ is $D^2(\vec{a}), D^3(\vec{a}), \cdots, D^7(\vec{a})$.

Note that the components of $D^i(\vec{a})$ are taken from 0 or $(K-1)d, \forall\, i = 2, 3, \cdots, 7$ and $(K-1)d$ is a multiple of $d = \gcd \vec{a}$, where the multiple is $(K-1)$.

Lemma 2.18. *Let $\vec{a} \in A_N$ with $\vec{a} \neq \vec{\mathbf{0}}$. For all nonnegative integers r, s with $r \leq s$, then* $\gcd D^r(\vec{a}) \mid \gcd D^s(\vec{a})$. *In particular, we have* $\gcd D^r(\vec{a}) \leq \gcd D^s(\vec{a})$.

Proof.

It suffices to show that $\gcd D^r(\vec{a}) \mid \gcd D^s(\vec{a})$

Given nonnegative integers r, s with $r \leq s$

If $r = s$, there is nothing to prove

Now, we may assume that $r < s$

It is reduced to prove that $\gcd D^r(\vec{a}) \mid \gcd D^{r+1}(\vec{a})$:

Write $D^r(\vec{a}) = (x_1 d, x_2 d, \cdots, x_N d)$ such that $\gcd(x_1, x_2, \cdots, x_N) = 1$, where $\gcd D^r(\vec{a}) = d$

$\implies d > 0$, since $D^r(\vec{a}) \in A_N$

$\implies D^{r+1}(\vec{a}) = (\, |x_1 - x_2|d, \cdots, |x_{N-1} - x_N|d, |x_N - x_1|d\,)$

Let $\gcd(\, |x_1 - x_2|, \cdots, |x_{N-1} - x_N|, |x_N - x_1|\,) = d^*$

$\implies \gcd D^{r+1}(\vec{a}) = d^* \cdot d = d^* \cdot \gcd D^r(\vec{a})$

$\therefore \gcd D^r(\vec{a}) \mid \gcd D^{r+1}(\vec{a})$ □

Lemma 2.19. *Let $\vec{a} \in A_N$ with $\vec{a} \neq \vec{\mathbf{0}}$. Suppose that $D^k(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^{n-1}(\vec{a})$ is the $(n-k)$-cycle of $\vec{a}$. Then, we have $\gcd D^r(\vec{a}) = \gcd D^s(\vec{a})$ for all $k \leq r, s \leq n-1$.*

Proof.

Given $k \leq r, s \leq n-1$

We may assume that $r \leq s$

If $r = s$, then it is trivial

Suppose $r < s$, then $\gcd D^r(\vec{a}) \leq \gcd D^s(\vec{a})$ by Lemma 2.18

Now, look at the Ducci sequence of $D^s(\vec{a})$:

$$D^s(\vec{a}), D^{s+1}(\vec{a}), \cdots, D^{n-1}(\vec{a}), D^n(\vec{a}) = D^k(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^r(\vec{a})$$

By Lemma 2.18, we know that

$$\gcd D^s(\vec{a}) \leq \gcd D^k(\vec{a}) = \gcd D^n(\vec{a}) \leq \gcd D^{k+1}(\vec{a}) \leq \gcd D^r(\vec{a})$$

Therefore, $\gcd D^s(\vec{a}) \leq \gcd D^r(\vec{a})$

So, we conclude that $\gcd D^r(\vec{a}) = \gcd D^s(\vec{a})$ $\square$

Example 2.20.

Let $\vec{e}_1 = (1,0,0,0,0,0) \in A_6$

$\Longrightarrow$

$$\begin{aligned} D(\vec{e}_1) &= (1,0,0,0,0,1) \\ D^2(\vec{e}_1) &= (1,0,0,0,1,0) \\ D^3(\vec{e}_1) &= (1,0,0,1,1,1) \\ D^4(\vec{e}_1) &= (1,0,1,0,0,0) \\ D^5(\vec{e}_1) &= (1,1,1,0,0,1) \\ D^6(\vec{e}_1) &= (0,0,1,0,1,0) \\ D^7(\vec{e}_1) &= (0,1,1,1,1,0) \\ D^8(\vec{e}_1) &= (1,0,0,0,1,0) \\ &= D^2(\vec{e}_1) \end{aligned}$$

$\Longrightarrow$ the period of $\vec{e}_1$ is $(8-2) = 6$, and the 6-cycle of $\vec{e}_1$ is $D^2(\vec{e}_1), D^3(\vec{e}_1), D^4(\vec{e}_1), D^5(\vec{e}_1),$ $D^6(\vec{e}_1), D^7(\vec{e}_1)$

Note that $\gcd D^i(\vec{e}_1) = 1 = \max D^i(\vec{e}_1)$ for all $i = 0, 1, \cdots, 7$

However, $D^0(\vec{e}_1) = \vec{e}_1, D(\vec{e}_1)$ are not in the cycle of $\vec{e}_1$

Chapter 3

Similar Cycles

Definition 3.1. Let $\vec{a} \in A_N$ and $\vec{b} \in (\mathbb{Z}_2)^N$. Suppose $D^k(\vec{b}), D^{k+1}(\vec{b}), \cdots, D^{n-1}(\vec{b})$ is the $(n-k)$-cycle of $\vec{b}$. The cycle of $\vec{a}$ is said to be *similar to the cycle of* $\vec{b}$, if $\exists\, m \in \mathbb{N}$ such that $D^r(\vec{a}) = mD^s(\vec{b})$, where r, s are nonnegative integers with $k \leq s \leq n-1$.

Theorem 3.2. *Let $\vec{a} \in A_N$. Then, the cycle of $\vec{a}$ is similar to the cycle of $\vec{b}$, where $\vec{b} \in (\mathbb{Z}_2)^N$ and the period of $\vec{b}$ is equal to the period of $\vec{a}$.*

Proof.

By Lemma 2.1, we may assume that the period of $\vec{a}$ is $n-k$ and

$$D^k(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^{n-1}(\vec{a})$$

is the $(n-k)$-cycle of $\vec{a}$

Let $D^k(\vec{a}) = (x_1, x_2, \cdots, x_N)$

By Theorem 2.12, $x_1, x_2, \cdots, x_N \in \{0, M\}$, where $M = \max D^k(\vec{a})$

Since $D^k(\vec{a}) \in A_N$, we know that M is a nonnegative integer

Case 1: $M = 0$

$\implies D^k(\vec{a}) = (0, 0, \cdots, 0) \in (\mathbb{Z}_2)^N$

$\implies D^{k+1}(\vec{a}) = D(D^k(\vec{a})) = D(0, 0, \cdots, 0) = (0, 0, \cdots, 0) = D^k(\vec{a})$

$\implies n-1 \leq k$, since $\vec{a}, D(\vec{a}), \cdots, D^k(\vec{a}), \cdots, D^{n-1}(\vec{a})$ are all distinct

$\because$ the period of $\vec{a}$ is $n-k$

$\therefore k \leq n-1$

Therefore, we have $n-1=k$

So, the period of $\vec{a}$ is $n-k=1$

Choose $\vec{b}=\vec{\mathbf{0}} \in (\mathbb{Z}_2)^N$

$\implies D(\vec{b})=D(0,0,\cdots,0)=(0,0,\cdots,0)=\vec{b}=D^0(\vec{b})$

$\implies$ the period of $\vec{b}$ is $(1-0)=1$ and the 1-cycle of $\vec{b}$ is $D^0(\vec{b})=\vec{\mathbf{0}}$

Therefore, the period of $\vec{a}$ is equal to the period of $\vec{b}$

Note that $D^{k+1}(\vec{a})=\vec{\mathbf{0}}=D^0(\vec{b})$

$\implies$ the cycle of $\vec{a}$ is similar to the cycle of $\vec{b}$

Hence, we are done

Case 2: $M>0$

$\implies M \in \mathbb{N}$

Write $D^k(\vec{a})=(x_1,x_2,\cdots,x_N)=M(y_1,y_2,\cdots,y_N)$, where $y_1,y_2,\cdots,y_N$ are taken from 0 or 1

Choose $\vec{b}=(y_1,y_2,\cdots,y_N) \in (\mathbb{Z}_2)^N$

$\implies D^k(\vec{a})=M\vec{b}$

$\implies D^{k+1}(\vec{a})=D(D^k(\vec{a}))=D(M\vec{b})=MD(\vec{b})$

$\implies D^{k+i}(\vec{a})=MD^i(\vec{b}), \forall\, i=1,2,\cdots,n-k$

In particular, $M\vec{b}=D^k(\vec{a})=D^n(\vec{a})=MD^{n-k}(\vec{b})$

$\implies D^0(\vec{b})=\vec{b}=D^{n-k}(\vec{b})$

By assumption, $D^k(\vec{a})=M\vec{b}, D^{k+1}(\vec{a})=MD(\vec{b}),\cdots,D^{n-1}(\vec{a})=D^{n-k-1}(\vec{b})$ are all distinct

$\implies D^0(\vec{b})=\vec{b}, D(\vec{b}),\cdots,D^{n-k-1}(\vec{b})$ are all distinct

Therefore, the period of $\vec{b}$ is $(n-k)-0=n-k$ and the $(n-k)$-cycle of $\vec{b}$ is

$$D^0(\vec{b})=\vec{b}, D(\vec{b}),\cdots,D^{n-k-1}(\vec{b})$$

So, the period of $\vec{a}$ is equal to the period of $\vec{b}$

$\because D^k(\vec{a})=M\vec{b}=MD^0(\vec{b})$

$\therefore$ the cycle of $\vec{a}$ is similar to the cycle of $\vec{b}$

Hence, we complete this proof $\square$

Remark 3.3. When we discuss cycles of N-tuples in A_N, it is enough to cope with N-tuples in $(\mathbb{Z}_2)^N$ according to Theorem 3.2.

Lemma 3.4. *Let $\vec{a} = (a_1, a_2, \cdots, a_N) \in A_N$ and $\max \vec{a} = M$. Suppose that the cycle of $\vec{a}$ is similar to the cycle of $\vec{b}$, where $\vec{b} \in (\mathbb{Z}_2)^N$ and the period of $\vec{b}$ is equal to the period of $\vec{a}$. If $\vec{a^c} = (M - a_1, M - a_2, \cdots, M - a_N)$, then the cycle of $\vec{a^c}$ is similar to the cycle of $\vec{b}$.*

Proof.

Note that $D(\vec{a^c}) = (|a_1 - a_2|, |a_2 - a_3|, \cdots, |a_N - a_1|) = D(\vec{a})$

Since the cycle of $\vec{a}$ is similar to the cycle of $\vec{b}$, $\exists\, m \in \mathbb{N}$ such that

$$D^r(\vec{a}) = mD^s(\vec{b}),$$

where r, s are nonnegative integers with $k \leq s \leq n-1$

Then, we have:

$$\begin{aligned} D^{r+1}(\vec{a^c}) = D^r(D(\vec{a^c})) = D^r(D(\vec{a})) = D^{r+1}(\vec{a}) \\ = D(D^r(\vec{a})) = D(mD^s(\vec{b})) = mD(D^s(\vec{b})) = mD^{s+1}(\vec{b}) \end{aligned}$$

which completes this proof $\square$

Remark 3.5. In the proof of Lemma 3.4, $D^{s+1}(\vec{b})$ is in the cycle of $\vec{b}$.

Proof.

If $k \leq s < n-1$, then it is trivial

Now, we may assume that $s = n-1$:

$\Longrightarrow\ s + 1 = n$

$\Longrightarrow\ D^{s+1}(\vec{b}) = D^n(\vec{b}) = D^k(\vec{b})$ is in the cycle of $\vec{b}$ $\square$

Lemma 3.6. *Let $\vec{a} = (a_1, a_2, \cdots, a_N) \in A_N$ and $\max \vec{a}$=M. Suppose that*

$$D^k(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^{n-1}(\vec{a})$$

is the $(n-k)$-cycle of $\vec{a}$. Then, $\vec{a^c} = (M - a_1, M - a_2, \cdots, M - a_N)$ is in the $(n-k)$-cycle of $\vec{a}$ if and only if $\vec{a} = \vec{\mathbf{0}}$.

Proof.

Note that $D(\vec{a^c}) = (|a_1 - a_2|, |a_2 - a_3|, \cdots, |a_N - a_1|) = D(\vec{a})$

"⇒" Suppose the condition holds

$\implies \exists\, k \leq r \leq n-1$ such that $\vec{a^c} = D^r(\vec{a})$

$\implies D(\vec{a}) = D(\vec{a^c}) = D(D^r(\vec{a})) = D^{r+1}(\vec{a})$

$\implies n-1 \leq r$, since $D^0(\vec{a}) = \vec{a}, D(\vec{a}), \cdots, D^k(\vec{a}), \cdots, D^r(\vec{a}), \cdots, D^{n-1}(\vec{a})$ are all distinct

Therefore, $r = n-1$

$\implies n = r+1$

$\implies D^k(\vec{a}) = D^n(\vec{a}) = D^{r+1}(\vec{a}) = D(\vec{a^c}) = D(\vec{a}) \qquad (*)$

Claim: $k = 0$

Proof.

If not, suppose $k \geq 1$

By assumption, $D^0(\vec{a}) = \vec{a}, D(\vec{a}), \cdots, D^{k-1}(\vec{a}), D^k(\vec{a}), \cdots, D^{n-1}(\vec{a})$ are all distinct

$\implies n-1 \leq k-1$, by $(*)$

$\implies n \leq k$ which is a contradiction to $n > k$ □

By **Claim** and $(*)$, we obtain $\vec{a} = D^0(\vec{a}) = D(\vec{a^c})$

$\implies \forall\, 1 \leq i \leq N, a_i = M - a_i$

$\implies \forall 1 \leq i \leq N, a_i = \frac{M}{2}$

$\implies M = \max \vec{a} = \frac{M}{2}$

$\implies M = 0$

$\because 0 \leq a_1, a_2, \cdots, a_N \leq M = 0$

$\therefore a_1 = a_2 = \cdots = a_N = 0$

$\implies \vec{a} = \vec{\mathbf{0}}$

"$\Leftarrow$" Suppose $\vec{a} = \vec{\mathbf{0}}$

$\implies a_1 = a_2 = \cdots = a_N = 0$

$\implies M = 0$

$\implies \vec{a^c} = (0, 0, \cdots, 0)$

Note that $D(\vec{a}) = D(0, 0, \cdots, 0) = (0, 0, \cdots, 0) = \vec{a} = D^0(\vec{a})$

$\implies$ the period of $\vec{a}$ is $(1 - 0) = 1$ and the 1-cycle of $\vec{a}$ is

$$D^0(\vec{a}) = (0, 0, \cdots, 0) = \vec{a^c}$$

Hence, we complete this proof

$\square$

Now, we define $T : A_N \to A_N$ by

$$T(x_1, x_2, \cdots, x_{N-1}, x_N) = (x_2, x_3, \cdots, x_N, x_1)$$

for all $(x_1, x_2, \cdots, x_{N-1}, x_N) \in A_N$. Clearly, T is well-defined. On the other hand, we fix the following notations: $\mathscr{D} = D \mid_{(\mathbb{Z}_2)^N}$, $\mathscr{T} = T \mid_{(\mathbb{Z}_2)^N}$, and $\mathscr{D}^0 = \mathscr{T}^0 = \mathscr{I}$, where $\mathscr{I}$ is the identity on $(\mathbb{Z}_2)^N$.

Lemma 3.7. *Let $\vec{x}, \vec{y} \in A_N$ and c be a nonnegative integer, then*

(a) $T(c\vec{x}+\vec{y}) = cT(\vec{x}) + T(\vec{y})$.

(b) $D \circ T = T \circ D$.

Proof.

Write $\vec{x} = (x_1, x_2, \cdots, x_N), \vec{y} = (y_1, y_2, \cdots, y_N) \in A_N$

(a)

$$\begin{aligned} T(c\vec{x}+\vec{y}) &= T(cx_1+y_1, cx_2+y_2, \cdots, cx_N+y_N) \\ &= (cx_2+y_2, \cdots, cx_N+y_N, cx_1+y_1) \\ &= c(x_2, \cdots, x_N, x_1) + (y_2, \cdots, y_N, y_1) \\ &= cT(\vec{x}) + T(\vec{y}) \end{aligned}$$

(b)

Given $(a_1, a_2, \cdots, a_N) \in A_N$

$$\begin{aligned} D \circ T(a_1, a_2, \cdots, a_N) &= D(T(a_1, a_2, \cdots, a_N)) \\ &= D(a_2, \cdots, a_N, a_1) \\ &= (|a_2 - a_3|, \cdots, |a_N - a_1|, |a_1 - a_2|) \end{aligned}$$

$$\begin{aligned} T \circ D(a_1, a_2, \cdots, a_N) &= T(D(a_1, a_2, \cdots, a_N)) \\ &= T(|a_1 - a_2|, \cdots, |a_{N-1} - a_N|, |a_N - a_1|) \\ &= (|a_2 - a_3|, \cdots, |a_N - a_1|, |a_1 - a_2|) \end{aligned}$$

$\implies D \circ T(a_1, a_2, \cdots, a_N) = T \circ D(a_1, a_2, \cdots, a_N)$

$\therefore D \circ T = T \circ D$

□

Remark 3.8. Let $x, y \in \mathbb{Z}_2$. Then, $|x-y| = x+y$.

Proof.

Given $x, y \in \mathbb{Z}_2$

$\implies 2y = 0$

$\implies x - y = x - y + 2y = x + y$

$\implies |x-y| = |x+y|$

$\implies |x-y| = x+y$, since $x, y \in \mathbb{Z}_2$ □

Remark 3.9. Let $\mathscr{L} : (\mathbb{Z}_2)^N \to (\mathbb{Z}_2)^N$ be a function. Then, we know that $\mathscr{L}$ is a linear transformation if and only if $\mathscr{L}(\vec{x}+\vec{y}) = \mathscr{L}(\vec{x}) + \mathscr{L}(\vec{y})$ for all $\vec{x}, \vec{y} \in (\mathbb{Z}_2)^N$.

Proof.

"⇒" It is trivial

"⇐" Suppose the condition holds

Given $\vec{x}, \vec{y} \in (\mathbb{Z}_2)^N$, and $c \in \mathbb{Z}_2$

We must show that $\mathscr{L}(c\vec{x}+\vec{y}) = c\mathscr{L}(\vec{x}) + \mathscr{L}(\vec{y})$:

If $c = 1$, then there is nothing to prove

Now, we may assume that $c = 0$:

$\implies$

$$\mathscr{L}(c\vec{x}+\vec{y}) = \mathscr{L}(\vec{\mathbf{0}}+\vec{y}) = \mathscr{L}(\vec{y})$$

and

$$c\mathscr{L}(\vec{x}) + \mathscr{L}(\vec{y}) = \vec{\mathbf{0}} + \mathscr{L}(\vec{y}) = \mathscr{L}(\vec{y})$$

$\therefore \mathscr{L}(c\vec{x}+\vec{y}) = c\mathscr{L}(\vec{x}) + \mathscr{L}(\vec{y})$

□

Lemma 3.10. *$\mathscr{T}^i$ is a linear transformation for each $i = 0, 1, 2, \cdots$.*

Proof.

We prove it by induction on i:

$i = 0$:

$\mathscr{T}^0 = \mathscr{I}$ is a linear transformation, holds

Suppose $i = K$ holds

Then, $i = K + 1$:

By Remark 3.9, it suffices to show that

$$\mathscr{T}^{K+1}(\vec{x}+\vec{y}) = \mathscr{T}^{K+1}(\vec{x}) + \mathscr{T}^{K+1}(\vec{y}), \forall\, \vec{x},\vec{y} \in (\mathbb{Z}_2)^N$$

Given $\vec{x} = (x_1, x_2, \cdots, x_N), \vec{y} = (y_1, y_2, \cdots, y_N) \in (\mathbb{Z}_2)^N$

$$\begin{aligned}
\mathscr{T}^{K+1}(\vec{x}+\vec{y}) &= \mathscr{T}^K(T(\vec{x}+\vec{y})) \\
&= \mathscr{T}^K(\mathscr{T}(x_1+y_1, x_2+y_2, \cdots, x_N+y_N)) \\
&= \mathscr{T}^K(x_2+y_2, \cdots, x_N+y_N, x_1+y_1) \\
&= \mathscr{T}^K(x_2, \cdots, x_N, x_1) + \mathscr{T}^K(y_2, \cdots, y_N), \text{ by} \\
&\quad \text{induction hypothesis} \\
&= \mathscr{T}^K(\mathscr{T}(x_1, x_2, \cdots, x_N)) + \mathscr{T}^K(\mathscr{T}(y_1, y_2, \cdots, y_N)) \\
&= \mathscr{T}^{K+1}(x_1, x_2, \cdots, x_N) + \mathscr{T}^{K+1}(y_1, y_2, \cdots, y_N) \\
&= \mathscr{T}^{K+1}(\vec{x}) + \mathscr{T}^{K+1}(\vec{y})
\end{aligned}$$

By induction, we complete this proof □

Lemma 3.11. *$\mathscr{D}^i$ is a linear transformation for each $i = 0, 1, 2, \cdots$.*

Proof.

We prove it by induction on i:

$i = 0$:

$\mathscr{D}^0 = \mathscr{I}$ is a linear transformation, holds

Suppose $i = K$ holds

Then, $i = K + 1$:

By Remark 3.9, it suffices to show that:

$$\mathscr{D}^{K+1}(\vec{x}+\vec{y}) = \mathscr{D}^{K+1}(\vec{x}) + \mathscr{D}^{K+1}(\vec{y}), \forall\, \vec{x}, \vec{y} \in (\mathbb{Z}_2)^N$$

Given $\vec{x} = (x_1, x_2, \cdots, x_N), \vec{y} = (y_1, y_2, \cdots, y_N) \in (\mathbb{Z}_2)^N$

$$\begin{aligned}
\mathscr{D}^{K+1}(\vec{x}+\vec{y}) &= \mathscr{D}^{K}(\mathscr{D}(\vec{x}+\vec{y})) \\
&= \mathscr{D}^{K}(\mathscr{D}(x_1+y_1, x_2+y_2, \cdots, x_N+y_N)) \\
&= \mathscr{D}^{K}(\,|(x_1+y_1)-(x_2+y_2)|, \cdots, |(x_{N-1}+y_{N-1})-(x_N+y_N)|, \\
&\quad |(x_N+y_N)-(x_1+y_1)|\,) \\
&= \mathscr{D}^{K}(\,(x_1+y_1)+(x_2+y_2), \cdots, (x_{N-1}+y_{N-1})+(x_N+y_N), \\
&\quad (x_N+y_N)+(x_1+y_1)\,), \text{by Remark 3.8} \\
&= \mathscr{D}^{K}((x_1+x_2)+(y_1+y_2), \cdots, (x_{N-1}+x_N)+(y_{N-1}+y_N), \\
&\quad (x_N+x_1)+(y_N+y_1)) \\
&= \mathscr{D}^{K}(x_1+x_2, \cdots, x_{N-1}+x_N, x_N+x_1) + \mathscr{D}^{K}(y_1+y_2, \cdots, \\
&\quad y_{N-1}+y_N, y_N+y_1), \text{by induction hypothesis} \\
&= \mathscr{D}^{K}(\,|x_1-x_2|, \cdots, |x_{N-1}-x_N|, |x_N-x_1|\,) + \\
&\quad \mathscr{D}^{K}(\,|y_1-y_2|, \cdots, |y_{N-1}-y_N|, |y_N-y_1|), \text{by Remark 3.8} \\
&= \mathscr{D}^{K}(\mathscr{D}(x_1, x_2, \cdots, x_N)) + \mathscr{D}^{K}(\mathscr{D}(y_1, y_2, \cdots, y_N)) \\
&= \mathscr{D}^{K+1}(x_1, x_2, \cdots, x_N) + \mathscr{D}^{K+1}\mathscr{D}(y_1, y_2, \cdots, y_N) \\
&= \mathscr{D}^{K+1}(\vec{x}) + \mathscr{D}^{K+1}(\vec{y})
\end{aligned}$$

By induction, we complete this proof $\square$

Lemma 3.12. *Let $\vec{a} \in A_N$. Suppose that r, s, t are nonnegative integers such that $s \leq r$ and*

$s \leq t$. If $D^r(\vec{a}) = D^s(\vec{a})$, then

$$D^{(r-s)i}(D^t(\vec{a})) = D^t(\vec{a})$$

for each $i = 0, 1, 2, \cdots$.

Proof.

We prove it by induction on i:

$i = 0$: It is trivial

Suppose $i = K$ holds

Then, $i = K + 1$:

$$\begin{aligned}
D^{(r-s)(K+1)}(D^t(\vec{a})) &= D^{r-s}(D^{(r-s)K}(D^t(\vec{a}))) \\
&= D^{r-s}(D^t(\vec{a})), \text{ by induction hypothesis} \\
&= D^{r-s+t}(\vec{a}) \\
&= D^{t-s}(D^r(\vec{a})), \text{ since } s \leq t \\
&= D^{t-s}(D^s(\vec{a})) \\
&= D^t(\vec{a}), \text{ holds}
\end{aligned}$$

By induction, we complete this proof □

Theorem 3.13. *Let $\vec{e}_i = (\delta_{i1}, \delta_{i2}, \cdots, \delta_{iN}) \in A_N$, where*

$$\delta_{ij} = \begin{cases} 1, & \text{if } j = i \\ 0, & \text{if } j \neq i \end{cases}$$

for all $i, j \in \{1, 2, \cdots, N\}$. Then, we have:

(a) *If $D^r(\vec{e}_1) = D^s(\vec{e}_1)$ for some nonnegative integers r, s, then we have:*

$$D^r(\vec{b}) = D^s(\vec{b}), \forall \vec{b} \in (\mathbb{Z}_2)^N.$$

(b) *The period of $\vec{e}_1, \vec{e}_2, \cdots, \vec{e}_N$ are all identical.*

(c) *If $\vec{a} \in A_N$, then the period of $\vec{a}$ divides the period of $\vec{e}_1$. In particular, the maximal period of N-tuples in A_N is equal to the period of $\vec{e}_1$.*

Proof.

Note that $\{\vec{e}_1, \vec{e}_2, \cdots, \vec{e}_N\}$ is a basis of $(\mathbb{Z}_2)^N$ over $\mathbb{Z}_2$

(a)

Claim: $D^r(\vec{e}_i) = D^s(\vec{e}_i)$ for each $i = 1, 2, \cdots, N$

Proof.

Given $i \in \mathbb{N}$ with $1 \leq i \leq N$

If $i = 1$, then there is nothing to prove

Now, we may assume that $2 \leq i \leq N$

Note that $\vec{e}_i = T^{N-i+1}(\vec{e}_1)$

$\Longrightarrow$

$$\begin{aligned} D^r(\vec{e}_i) &= D^r(T^{N-i+1}(\vec{e}_1)) \\ &= T^{N-i+1}(D^r(\vec{e}_1)), \text{by Lemma 3.7}\textbf{(b)} \\ &= T^{N-i+1}(D^s(\vec{e}_1)) \\ &= D^s(T^{N-i+1}(\vec{e}_1)), \text{by Lemma 3.7}\textbf{(b)} \\ &= D^s(\vec{e}_i) \end{aligned}$$

$\therefore D^r(\vec{e}_i) = D^s(\vec{e}_i)$ for each $i = 1, 2, \cdots, N$ □

Given $\vec{b} \in (\mathbb{Z}_2)^N$

Finally, we must show that $D^r(\vec{b}) = D^s(\vec{b})$:

$\because \{\vec{e}_1, \vec{e}_2, \cdots, \vec{e}_N\}$ is a basis of $(\mathbb{Z}_2)^N$ over $\mathbb{Z}_2$

$\therefore \exists\, c_1, c_2, \cdots, c_N \in \mathbb{Z}_2$ such that $\vec{b} = c_1\vec{e}_1 + c_2\vec{e}_2 + \cdots + c_N\vec{e}_N$

$\Longrightarrow$

$$
\begin{aligned}
D^r(\vec{b}) &= \mathscr{D}^r(\vec{b}) \\
&= \mathscr{D}^r(c_1\vec{e}_1 + c_2\vec{e}_2 + \cdots + c_N\vec{e}_N) \\
&= c_1\mathscr{D}^r(\vec{e}_1) + c_2\mathscr{D}^r(\vec{e}_2) + \cdots + c_N\mathscr{D}^r(\vec{e}_N), \text{ by Lemma 3.11} \\
&= c_1 D^r(\vec{e}_1) + c_2 D^r(\vec{e}_2) + \cdots + c_N D^r(\vec{e}_N) \\
&= c_1 D^s(\vec{e}_1) + c_2 D^s(\vec{e}_2) + \cdots + c_N D^s(\vec{e}_N), \text{ by } \textbf{Claim} \\
&= c_1\mathscr{D}^s(\vec{e}_1) + c_2\mathscr{D}^s(\vec{e}_2) + \cdots + c_N\mathscr{D}^s(\vec{e}_N) \\
&= \mathscr{D}^s(c_1\vec{e}_1 + c_2\vec{e}_2 + \cdots + c_N\vec{e}_N), \text{ by Lemma 3.11} \\
&= \mathscr{D}^s(\vec{b}) \\
&= D^s(\vec{b})
\end{aligned}
$$

(b)

Given $i \in \mathbb{N}$ with $2 \le i \le N$

It suffices to show that the period of $\vec{e}_i$ is equal to the period of $\vec{e}_1$:

By Lemma 2.1, we may assume that the period of $\vec{e}_1 = n - k$

$\Longrightarrow$ $D^0(\vec{e}_1) = \vec{e}_1, D(\vec{e}_1), D^2(\vec{e}_1), \cdots, D^{n-1}(\vec{e}_1)$ are all distinct and

$$D^n(\vec{e}_1) = D^k(\vec{e}_1)$$

By **(a)**, we know that $D^n(\vec{e}_i) = D^k(\vec{e}_i)$ $\quad (*)$

Claim: $D^0(\vec{e}_i) = \vec{e}_i, D(\vec{e}_i), D^2(\vec{e}_i), \cdots, D^{N-1}(\vec{e}_i)$ are all distinct

Proof.

If not, suppose $\exists\, a, b \in \mathbb{Z}$ with $0 \le a < b \le n-1$ such that $D^a(\vec{e}_i) = D^b(\vec{e}_i)$

$\Longrightarrow$ $T^{i-1}(D^a(\vec{e}_i)) = T^{i-1}(D^b(\vec{e}_i))$

$\Longrightarrow\ D^a(T^{i-1}(\vec{e}_i)) = D^b(T^{i-1}(\vec{e}_i))$, by Lemma 3.7**(b)**

$\Longrightarrow\ D^a(\vec{e}_1) = D^b(\vec{e}_1)$ which is a contradiction to

$$D^0(\vec{e}_1) = \vec{e}_1, D(\vec{e}_1), D^2(\vec{e}_1), \cdots, D^{n-1}(\vec{e}_1)$$

are all distinct □

By **Claim** and (∗), the period of $\vec{e}_i$ is equal to $n-k$

$\Longrightarrow$ the period of $\vec{e}_i$ is equal to the period of $\vec{e}_1$

(c)

It is enough to prove that the period of $\vec{a}$ divides the period of $\vec{e}_1$

By Lemma 2.1, we may assume that the periods of $\vec{a}$ and $\vec{e}_1$ are $n-k$ and $n'-k'$, respectively

Write $n'-k' = (n-k)q + r$, where q, r are nonnegative integers with

$$0 \le r < n-k$$

So, it suffices to show that $r = 0$:

By Theorem 3.2, $\exists\, \vec{b} \in (\mathbb{Z}_2)^N$ with the period of $\vec{b}$ which is equal to the period of $\vec{a}$ such that the cycle of $\vec{a}$ is similar to the cycle of $\vec{b}$

$\Longrightarrow\ D^n(\vec{b}) = D^k(\vec{b})$

Moreover, the period of $\vec{e}_1$ is $n'-k'$

$\Longrightarrow\ D^{n'}(\vec{e}_1) = D^{k'}(\vec{e}_1)$

By **(a)**, we obtain $D^{n'}(\vec{b}) = D^{k'}(\vec{b})$

Take $\vec{\boldsymbol{b}} = D^{k+k'}(\vec{b})$

By Lemma 3.12, we obtain $D^{n'-k'}(\vec{\boldsymbol{b}}) = \vec{\boldsymbol{b}}$

$\Longrightarrow$

$$\begin{aligned}\vec{\boldsymbol{b}} = D^{n'-k'}(\vec{\boldsymbol{b}}) &= D^{(n-k)q+r}(\vec{\boldsymbol{b}}) \\ &= D^{r}(D^{(n-k)q}(\vec{\boldsymbol{b}})) \\ &= D^{r}(\vec{\boldsymbol{b}}), \text{ by Lemma 3.12}\end{aligned}$$

$\Longrightarrow \; D^{k+k'}(\vec{b}) = D^{k+k'+r}(\vec{b})$

Write $k' = (n-k)q_0 + r_0$, where q_0, r_0 are nonnegative integers with

$$0 \leq r_0 < n-k$$

$\Longrightarrow$

$$\begin{aligned}D^{k+k'}(\vec{b}) &= D^{(k+(n-k)q_0+r_0)}(\vec{b}) \\ &= D^{(n-k)q_0}(D^{k+r_0}(\vec{b})) \\ &= D^{k+r_0}(\vec{b}), \text{ by Lemma 3.12}\end{aligned}$$

and

$$\begin{aligned}D^{k+k'+r}(\vec{b}) &= D^{k+((n-k)q_0+r_0)+r}(\vec{b}) \\ &= D^{(n-k)q_0}(D^{k+r_0+r}(\vec{b})) \\ &= D^{k+r_0+r}(\vec{b}), \text{ by Lemma 3.12}\end{aligned}$$

$\Longrightarrow \; D^{k+r_0+r}(\vec{b}) = D^{k+k'+r}(\vec{b}) = D^{k+k'}(\vec{b}) = D^{k+r_0}(\vec{b}) \qquad (*')$

Note that $k + r_0 \leq k + r_0 + r < k + r_0 + (n-k) = n + r_0$

$\Longrightarrow \; k + r_0 \leq k + r_0 + r \leq (n-1) + r_0$, since $k + r_0 + r, n + r_0$ are integers

On the other hand, $\vec{b}, D(\vec{b}), \cdots, D^{k}(\vec{b}), D^{k+1}(\vec{b}), \cdots, D^{n-1}(\vec{b})$ are all distinct and $D^{n}(\vec{b}) = D^{k}(\vec{b})$, since the period of $\vec{b}$ is $n-k$

$\Longrightarrow\ D^{k+r_0}(\vec{b}), D^{k+r_0+1}(\vec{b}), \cdots, D^{k+r_0+r}(\vec{b}), \cdots, D^{(n-1)+r_0}(\vec{b})$ are all distinct

By $(*')$, we conclude that $k + r_0 = k + r_0 + r$

$\Longrightarrow\ r = 0$

Hence, we complete this proof

$\square$

Lemma 3.14. *Let r, s be nonnegative integers. Then, we have:*

(a) $\mathscr{D} = \mathscr{I} + \mathscr{T}$.

(b) *If* $2^r \equiv s \pmod{N}$, *then* $\mathscr{D}^{2^r} = \mathscr{I} + \mathscr{T}^s$.

Proof.

(a)

Given $\vec{x} = (x_1, x_2, \cdots, x_N) \in (\mathbb{Z}_2)^N$

$$\begin{aligned}
\mathscr{I} + \mathscr{T}(\vec{x}) &= \mathscr{I}(\vec{x}) + \mathscr{T}(\vec{x}) \\
&= \mathscr{I}(x_1, x_2, \cdots, x_N) + \mathscr{T}(x_1, x_2, \cdots, x_N) \\
&= (x_1, x_2, \cdots, x_N) + (x_2, \cdots, x_N, x_1) \\
&= (x_1 + x_2, \cdots, x_{N-1} + x_N, x_N + x_1) \\
&= (\,|x_1 - x_2|, \cdots, |x_{N-1} - x_N|, |x_N - x_1|\,), \text{by Remark 3.8} \\
&= \mathscr{D}(x_1, x_2, \cdots, x_N) \\
&= \mathscr{D}(\vec{x})
\end{aligned}$$

$\therefore \mathscr{D} = \mathscr{I} + \mathscr{T}$

(b)

By **(a)**, $\mathscr{D}^{2^r} = (\mathscr{I} + \mathscr{T})^{2^r}$

Claim: $(\mathscr{I} + \mathscr{T})^{2^r} = \mathscr{I} + \mathscr{I}^{2^r}$

Proof.

We prove it by induction on r:

$r = 0$: It is trivial

Suppose $r = K$ holds

Then, $r = K + 1$:

$$\begin{aligned}(\mathscr{I} + \mathscr{T})^{2^{K+1}} &= ((\mathscr{I} + \mathscr{T})^{2^K})^2 \\ &= (\mathscr{I} + \mathscr{T}^{2^K})^2, \text{ by induction hypothesis} \\ &= \mathscr{I}^2 + \mathscr{I}\mathscr{T}^{2^K} + \mathscr{T}^{2^K}\mathscr{I} + (\mathscr{T}^{2^K})^2 \\ &= \mathscr{I} + \mathscr{T}^{2^K} + \mathscr{T}^{2^K} + \mathscr{T}^{2^{K+1}} \\ &= \mathscr{I} + \mathscr{T}^{2^{K+1}}, \text{ since } \mathscr{T}(\mathbb{Z}_2) \subseteq \mathbb{Z}_2\end{aligned}$$

So, $r = K + 1$ holds □

Note that $\mathscr{T}^N = \mathscr{T}$

By assumption, we know that $\mathscr{T}^{2^r} = \mathscr{T}^s$

$\therefore \mathscr{D}^{2^r} = (\mathscr{I} + \mathscr{T})^{2^r} = \mathscr{I} + \mathscr{T}^{2^r} = \mathscr{I} + \mathscr{T}^s$

Hence, we complete this proof

□

Theorem 3.15. *Let r be a positive integer. Suppose that $N = 2^r$. If $\vec{a} \in A_N$, then the cycle of $\vec{a}$ is similar to the 1-cycle of $\vec{\mathbf{0}}$.*

Proof.

By Lemma 2.1, we may assume that the period of $\vec{a}$ is $n - k$

Note that $2^r \equiv 0 \pmod{N}$

By Theorem 3.2, $\exists \vec{b} \in (\mathbb{Z}_2)^N$ with the period of $\vec{b}$ which is equal to the period of $\vec{a}$ such that the cycle of $\vec{a}$ is similar to the cycle of $\vec{b}$

$\implies \exists m \in \mathbb{N}$ such that $D^r(\vec{a}) = mD^s(\vec{b})$, where r, s are nonnegative integers with $k \leq s \leq n-1$

$\because$

$$
\begin{aligned}
D^N(\vec{b}) &= \mathscr{D}^N(\vec{b}), \text{ since } \vec{b} \in (\mathbb{Z}_2)^N \\
&= \mathscr{I} + \mathscr{T}^0(\vec{b}), \text{ by Lemma 3.14} \\
&= \mathscr{I} + \mathscr{I}(\vec{b}) \\
&= \mathscr{I}(\vec{b}) + \mathscr{I}(\vec{b}) \\
&= \vec{\mathbf{0}}, \text{ since } \mathscr{I}(\vec{b}) \in (\mathbb{Z}_2)^6
\end{aligned}
$$

$\therefore$

$$
\begin{aligned}
D^{r+N}(\vec{a}) &= D^N(D^r(\vec{a})) \\
&= D^N(mD^s(\vec{b})) \\
&= mD^{N+s}(\vec{b}) \\
&= mD^s(D^N(\vec{b})) \\
&= mD^s(\vec{\mathbf{0}}) \\
&= m\vec{\mathbf{0}} \\
&= \vec{\mathbf{0}}
\end{aligned}
$$

On the other hand, $D(\vec{\mathbf{0}}) = D(0, 0, \cdots, 0) = (0, 0, \cdots, 0) = \vec{\mathbf{0}} = D^0(\vec{\mathbf{0}})$

$\implies$ the period of $\vec{\mathbf{0}}$ is $1 - 0 = 1$ and the 1-cycle of $\vec{\mathbf{0}}$ is $\vec{\mathbf{0}}$

$\implies$ the cycle of $\vec{a}$ is similar to the 1-cycle of $\vec{\mathbf{0}}$ $\square$

For further informations, please see [1] and [2].

Chapter 4

Diffy Hexagons

According to Remark 1.3, we shall concentrate on the cycles of 6-tuples in A_6 in this chapter.

Theorem 4.1. *The period of* 6*-tuples in* A_6 *divides* 6*. In particular, the maximal period of* 6*-tuples in* A_6 *is equal to* 6*.*

Proof.

Given $\vec{a} \in A_6$

Let $\vec{e}_1 = (1,0,0,0,0,0)$

$\Longrightarrow$

$$\begin{aligned} D(\vec{e}_1) &= (1,0,0,0,0,1) \\ D^2(\vec{e}_1) &= (1,0,0,0,1,0) \\ D^3(\vec{e}_1) &= (1,0,0,1,1,1) \\ D^4(\vec{e}_1) &= (1,0,1,0,0,0) \\ D^5(\vec{e}_1) &= (1,1,1,0,0,1) \\ D^6(\vec{e}_1) &= (0,0,1,0,1,0) \\ D^7(\vec{e}_1) &= (0,1,1,1,1,0) \\ D^8(\vec{e}_1) &= (1,0,0,0,1,0) \\ &= D^2(\vec{e}_1) \end{aligned}$$

$\implies$ the period of $\vec{e}_1$ is $(8-2) = 6$

By Theorem 3.13**(c)**, the period of $\vec{a}$ divides 6 and the maximal period of 6-tuples in A_6 is equal to 6 □

Lemma 4.2. *If* $\vec{b} \in (\mathbb{Z}_2)^6$*, then the cycle of* $\vec{b}$ *is one of the followings:*

(i) (1-cycle) $(0,0,0,0,0,0)$.

(ii) (3-cycle) $(0,1,1,0,1,1), (1,0,1,1,0,1), (1,1,0,1,1,0)$.

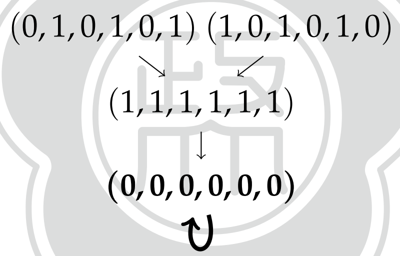
(iii) (6-cycle) $(0,1,0,0,0,1), (1,1,0,0,1,1), (0,1,0,1,0,0), (1,1,1,1,0,0), (0,0,0,1,0,1), (0,0,1,1,1,1)$.

(iv) (6-cycle) $(1,0,0,0,1,0), (1,0,0,1,1,1), (1,0,1,0,0,0), (1,1,1,0,0,1), (0,0,1,0,1,0), (0,1,1,1,1,0)$.

Proof.

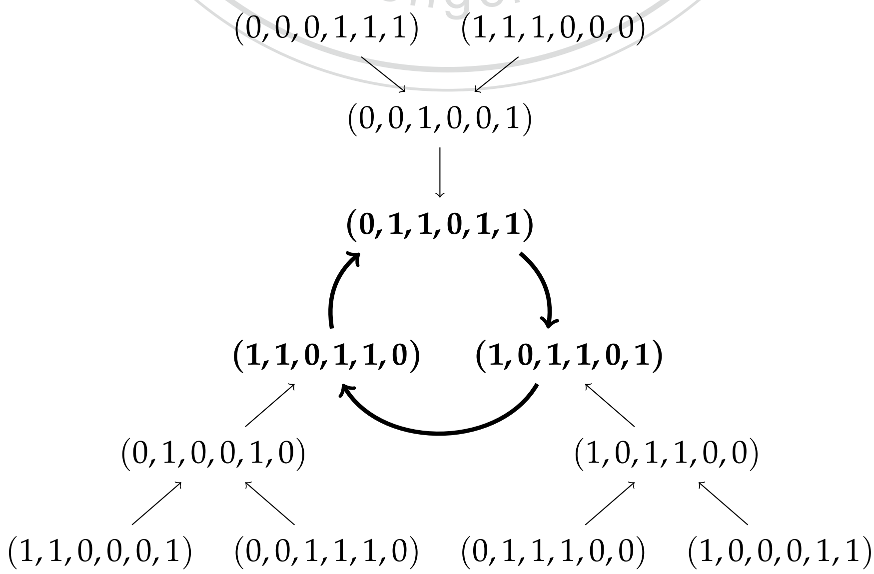
We prove it by enumerating as shown in the following diagrams:

(i) (1-cycle):



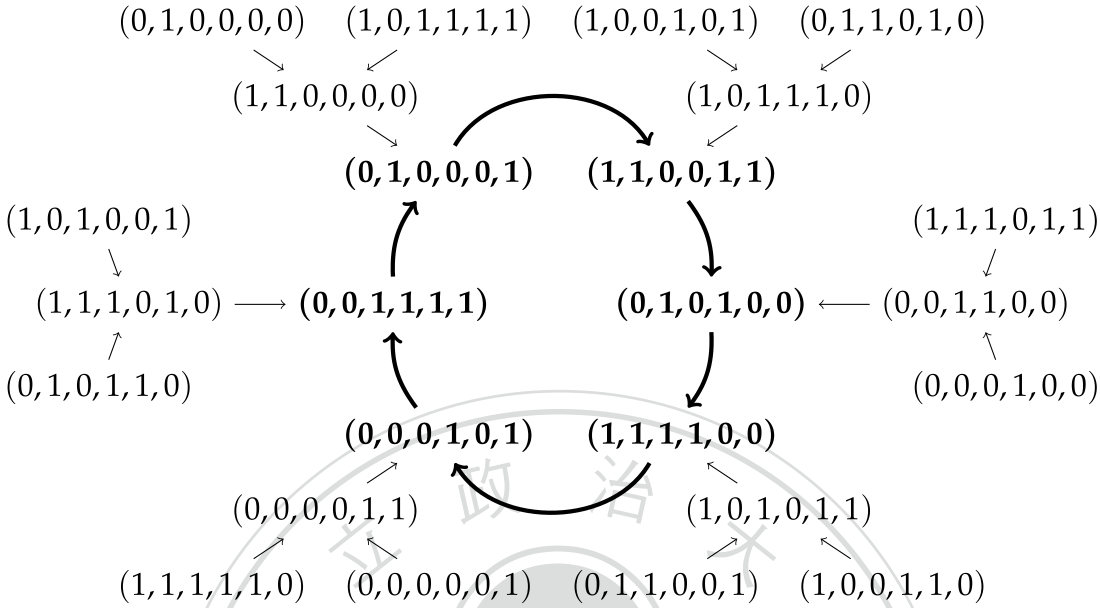
$\rightarrow$: a Ducci process

(ii) (3-cycle):



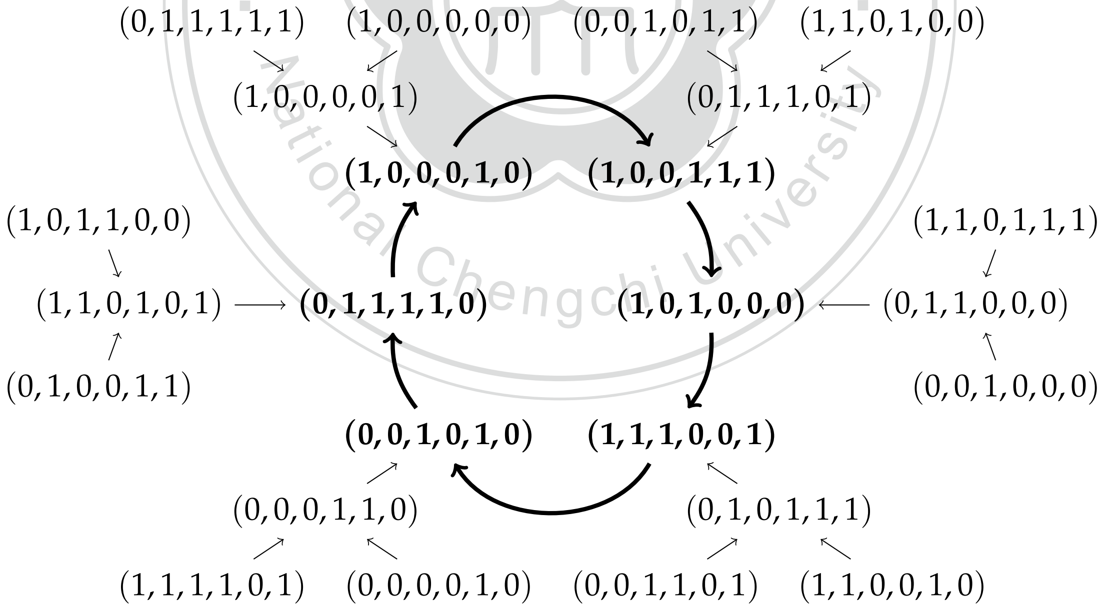
→: a Ducci process

(iii) (6-cycle):



→: a Ducci process

(iv) (6-cycle):



→: a Ducci process

□

Theorem 4.3. *Let $\vec{a} \in A_6$. Then, the cycle of $\vec{a}$ is similar to one of the following cycles:*

(i) (1-cycle) $(0,0,0,0,0,0)$.

(ii) (3-cycle) $(0,1,1,0,1,1),(1,0,1,1,0,1),(1,1,0,1,1,0)$.

(iii) (6-cycle) $(0,1,0,0,0,1),(1,1,0,0,1,1),(0,1,0,1,0,0),(1,1,1,1,0,0),(0,0,0,1,0,1),(0,0,1,1,1,1)$.

(iv) (6-cycle) $(1,0,0,0,1,0),(1,0,0,1,1,1),(1,0,1,0,0,0),(1,1,1,0,0,1),(0,0,1,0,1,0),(0,1,1,1,1,0)$.

Proof. It follows from Theorem 3.2 and Lemma 4.2. □

As in Remark 1.3, a 6-tuple $(a_1,a_2,a_3,a_4,a_5,a_6)$ in A_6 is regarded as written in a regular hexagon. However, regular hexagons have symmetries under rotations and reflections, but $(a_1,a_2,a_3,a_4,a_5,a_6)$ does not.

Write $\mathcal{D}_6 = \{(1)(2)(3)(4)(5)(6),(123456),(135)(246),(14)(25)(36),(153)(264),(165432),$ $(16)(25)(34),(1)(4)(26)(35),(12)(36)(45),(2)(5)(13)(46),(14)(23)(56),(3)(6)(15)(24)\}$ which is the permutation group corresponding to all possible rotations and reflections of the regular hexagon.

Define $* : \mathcal{D}_6 \times A_6 \to A_6$ by

$$\pi * (a_1,a_2,\cdots,a_6) = (a_{\pi(1)},a_{\pi(2)},\cdots,a_{\pi(6)})$$

for all $\pi \in \mathcal{D}_6$ and $(a_1,a_2,\cdots,a_6) \in A_6$. Clearly, $*$ is well-defined.

Lemma 4.4. *$*$ is a left group action of $\mathcal{D}_6$ on A_6.*

Proof.

Write $e = (1)(2)(3)(4)(5)(6)$ which is the identity element of $\mathcal{D}_6$

Claim 1: $e * \vec{a} = \vec{a}, \forall\, \vec{a} \in A_6$

Proof.

Given $\vec{a} = (a_1,a_2,\cdots,a_6) \in A_6$

$\Longrightarrow$

$$\begin{aligned} e * \vec{a} &= (a_{e(1)}, a_{e(2)}, \cdots, a_{e(6)}) \\ &= (a_1, a_2, \cdots, a_6) \\ &= \vec{a} \end{aligned}$$

□

Claim 2: $(\pi_1 \circ \pi_2) * \vec{a} = \pi_1 * (\pi_2 * \vec{a}), \forall\, \pi_1, \pi_2 \in \mathcal{D}_6$ and $\vec{a} \in A_6$

Proof.

Given $\pi_1, \pi_2 \in \mathcal{D}_6$ and $\vec{a} = (a_1, a_2, \cdots, a_6) \in A_6$

Note that

$$(\pi_1 \circ \pi_2) * \vec{a} = (a_{\pi_1 \circ \pi_2(1)}, a_{\pi_1 \circ \pi_2(2)}, \cdots, a_{\pi_1 \circ \pi_2(6)})$$

and

$$\begin{aligned} \pi_1 * (\pi_2 * \vec{a}) &= \pi_1 * (a_{\pi_2(1)}, a_{\pi_2(2)}, \cdots, a_{\pi_2(6)}) \\ &= (a_{\pi_1(\pi_2(1))}, a_{\pi_1(\pi_2(2))}, \cdots, a_{\pi_1(\pi_2(6))}) \\ &= (a_{\pi_1 \circ \pi_2(1)}, a_{\pi_1 \circ \pi_2(2)}, \cdots, a_{\pi_1 \circ \pi_2(6)}) \end{aligned}$$

$\therefore (\pi_1 \circ \pi_2) * \vec{a} = \pi_1 * (\pi_2 * \vec{a})$ □

By **Claim 1** and **Claim 2**, we complete this proof □

For all $\vec{x}, \vec{y} \in A_6$, define $\vec{x} \equiv \vec{y}$ by $\vec{x} = \pi * \vec{y}$ for some $\pi \in \mathcal{D}_6$. Then, $\equiv$ is the equivalence relation on A_6 induced by $\mathcal{D}_6$ and we denote an equivalence class of A_6 by $[(a_1, a_2, \cdots, a_6)]$, where $(a_1, a_2, \cdots, a_6) \in A_6$.

From now on, we identify two 6-tuples $\vec{x}, \vec{y}$ in A_6, written by $\vec{x} = \vec{y}$, if and only if $\vec{x} \equiv \vec{y}$.

Remark 4.5. In our identification, we observe that:

(a) If $\vec{a}, \vec{b} \in A_6$, then $\vec{a} = \vec{b}$ if and only if $[\,\vec{a}\,] = [\,\vec{b}\,]$.

(b) According to Remark 1.3, a sequence of regular hexagons, that is, a Diffy Hexagon game, is actually a Ducci sequence of 6-tuples in A_6.

Definition 4.6. Let $\vec{a} = (a_1, a_2, \cdots, a_6) \in (\mathbb{Z}_2)^6$. The *complement of* $\vec{a}$ is defined to be $(1-a_1, 1-a_2, \cdots, 1-a_6)$ and we denote it by $\vec{a^c}$.

Remark 4.7. If $\vec{a} = (a_1, a_2, \cdots, a_6) \in (\mathbb{Z}_2)^6$, then $\vec{a^c} \in (\mathbb{Z}_2)^6$.

Proof.

By assumption, we know that $a_1, a_2, \cdots, a_6 \in \{0, 1\}$

$\Longrightarrow\ 1-a_1, 1-a_2, \cdots, 1-a_6 \in \{0,1\}$

$\Longrightarrow\ \vec{a^c} = (1-a_1, 1-a_2, \cdots, 1-a_6) \in (\mathbb{Z}_2)^6$ □

Lemma 4.8. *If* $\vec{a} = (a_1, a_2, \cdots, a_6) \in (\mathbb{Z}_2)^6$, *then* $\pi * \vec{a^c} = (\pi * \vec{a})^c$ *for all* $\pi \in \mathcal{D}_6$.

Proof.

Write $\vec{a^c} = (b_1, b_2, \cdots, b_6)$

$\Longrightarrow\ b_i = 1 - a_i, \forall\, i = 1, 2, \cdots, 6$

Given $\pi \in \mathcal{D}_6$

Note that

$$\begin{aligned}\pi * \vec{a^c} &= (b_{\pi(1)}, b_{\pi(2)}, \cdots, b_{\pi(6)}) \\ &= (1-a_{\pi(1)}, 1-a_{\pi(2)}, \cdots, 1-a_{\pi(6)})\end{aligned}$$

and

$$\begin{aligned}(\pi * \vec{a})^c &= (a_{\pi(1)}, a_{\pi(2)}, \cdots, a_{\pi(6)})^c \\ &= (1-a_{\pi(1)}, 1-a_{\pi(2)}, \cdots, 1-a_{\pi(6)})\end{aligned}$$

$\therefore\ \pi * \vec{a^c} = (\pi * \vec{a})^c$ □

Lemma 4.9. *There are* 13 *equivalence classes of* $(\mathbb{Z}_2)^6$*. In fact, they are:* $(0,0,0,0,0,0)$, $(0,0,0,1,1,1)$, $(0,0,1,0,0,1)$, $(0,0,1,0,1,1)$, $(0,1,0,1,0,1)$, $(0,1,1,0,1,1)$, $(0,1,1,1,0,1)$, $(0,1,1,1,1,1)$, $(1,0,0,0,0,0)$, $(1,0,0,0,0,1)$, $(1,0,0,0,1,0)$, $(1,0,0,1,1,1)$, *and* $(1,1,1,1,1,1)$.

Proof.

For each $\pi \in \mathcal{D}_6$, let $Z_\pi = \{z \in (\mathbb{Z}_2)^6 \mid \pi * z = z\}$

By the Burnside's Lemma, we obtain:

$$
\begin{aligned}
|(\mathbb{Z}_2)^6/\equiv| &= \frac{1}{|\mathcal{D}_6|}\sum_{\pi\in\mathcal{D}_6}|Z_\pi| \\
&= \frac{1}{12}(2^6+2+2^2+2^3+2^2+2+2^3+2^4+2^3+2^4+2^3+2^4) \\
&= \frac{1}{12}(64+2+4+8+4+2+8+16+8+16+8+16) \\
&= \frac{1}{12}\cdot 156 \\
&= 13
\end{aligned}
$$

Finally, we enumerate 13 equivalence classes of $(\mathbb{Z}_2)^6$:

By Lemma 4.8, it is reduced to write out $[(0,0,0,0,0,0)]$, $[(1,0,0,0,0,0)]$, $[(0,0,1,0,0,1)]$, $[(1,0,0,0,0,1)]$, $[(1,0,0,0,1,0)]$, $[(0,0,0,1,1,1)]$, $[(0,0,1,0,1,1)]$, $[(0,1,0,1,0,1)]$:

$[(0,0,0,0,0,0)] = \{(0,0,0,0,0,0)\}$

$[(1,0,0,0,0,0)] = \{(1,0,0,0,0,0),(0,1,0,0,0,0),(0,0,1,0,0,0),(0,0,0,1,0,0),(0,0,0,0,1,0),(0,0,0,0,0,1)\}$

$[(0,0,1,0,0,1)] = \{(0,0,1,0,0,1),(1,0,0,1,0,0),(0,1,0,0,1,0)\}$

$[(1,0,0,0,0,1)] = \{(1,0,0,0,0,1),(1,1,0,0,0,0),(0,1,1,0,0,0),(0,0,1,1,0,0),(0,0,0,1,1,0),(0,0,0,0,1,1)\}$

$[(1,0,0,0,1,0)] = \{(1,0,0,0,1,0),(0,1,0,0,0,1),(1,0,1,0,0,0),(0,1,0,1,0,0),(0,0,1,0,1,0),(0,0,0,1,0,1)\}$

$$[(0,0,0,1,1,1)] = \{(0,0,0,1,1,1),(1,0,0,0,1,1),(1,1,0,0,0,1),(1,1,1,0,0,0),(0,1,1,1,0,0),$$
$$(0,0,1,1,1,0)\}$$
$$[(0,0,1,0,1,1)] = \{(0,0,1,0,1,1),(1,0,0,1,0,1),(1,1,0,0,1,0),(0,1,1,0,0,1),(1,0,1,1,0,0),$$
$$(0,1,0,1,1,0),(1,1,0,1,0,0),(0,1,1,0,1,0),(0,0,1,1,0,1),(1,0,0,1,1,0),$$
$$(0,1,0,0,1,1),(1,0,1,0,0,1)\}$$
$$[(0,1,0,1,0,1)] = \{(0,1,0,1,0,1),(1,0,1,0,1,0)\}$$

□

Theorem 4.10. *Let* $\vec{b} \in (\mathbb{Z}_2)^6$*. Then, the cycle of* $\vec{b}$ *is one of the followings:*

(i) (1-cycle) $(0,0,0,0,0,0)$.

(ii) (1-cycle) $(0,1,1,0,1,1)$.

(iii) (2-cycle) $(0,0,1,0,1,0),(0,1,1,1,1,0)$.

Proof.

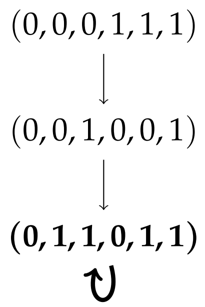
By Lemma 4.9 and Remark 4.5**(b)**, we prove it by enumerating as shown in the following diagrams:

(i) (1-cycle):

$$(0,1,0,1,0,1)$$
$$\downarrow$$
$$(1,1,1,1,1,1)$$
$$\downarrow$$
$$\mathbf{(0,0,0,0,0,0)}$$
$$\circlearrowright$$

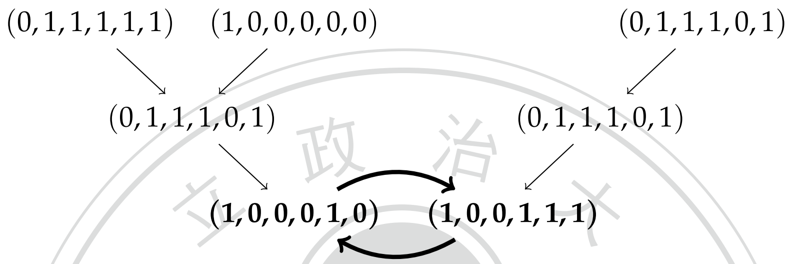
$\rightarrow$: a Ducci process

(ii) (1-cycle):



$\rightarrow$: a Ducci process

(iii) (2-cycle):



$\rightarrow$: a Ducci process

□

Corollary 4.11. *Let $\vec{a} \in A_6$. Then, the cycle of $\vec{a}$ is similar to one of the following cycles:*

(i) (1-cycle) $(0, 0, 0, 0, 0, 0)$.

(ii) (1-cycle) $(0, 1, 1, 0, 1, 1)$.

(iii) (2-cycle) $(0, 0, 1, 0, 1, 0), (0, 1, 1, 1, 1, 0)$.

Proof. It follows from Theorem 3.2 and Theorem 4.10 □

Theorem 4.12. *Let $\vec{e}_1 = (1, 0, 0, 0, 0, 0) \in A_6$. If r is a positive integer, then r is the period of $\vec{a}$ for some $\vec{a} \in A_6$ if and only if r divides the period of $\vec{e}_1$.*

Proof.

"$\Rightarrow$"

Suppose that r is the period of $\vec{a}$ for some $\vec{a} \in A_6$

By Theorem 3.13**(c)**, the period of $\vec{a}$ divides the period of $\vec{e}_1$

Therefore, r divides the period of $\vec{e}_1$

"$\Leftarrow$"

Suppose the condition holds

Note that

$$
\begin{aligned}
D(\vec{e}_1) &= (1,0,0,0,0,1) \\
D^2(\vec{e}_1) &= (1,0,0,0,1,0) \\
D^3(\vec{e}_1) &= (1,0,0,1,1,1) \\
D^4(\vec{e}_1) &= (1,0,1,0,0,0) \\
&= (1,0,0,0,1,0), \text{ by the proof in Lemma 4.9} \\
&= D^2(\vec{e}_1)
\end{aligned}
$$

By Remark 4.5**(a)** and Lemma 4.9, $\vec{e}_1, D(\vec{e}_1), D^2(\vec{e}_1), D^3(\vec{e}_1)$ are all distinct

$\therefore$ the period of $\vec{e}_1$ is $(4-2) = 2$

By assumption, we know that $r \mid 2$

So, we have the following two cases:

Case 1: $r = 1$

Choose $\vec{a} = (0,0,0,0,0,0) \in (\mathbb{Z}_2)^6 \subset A_6$

By Theorem 4.10, the cycle of $\vec{a}$ is $(0,0,0,0,0,0)$ and the period of $\vec{a}$ is 1

$\Longrightarrow$ the period of $\vec{a}$ is r

Case 2: $r = 2$

Choose $\vec{a} = (0,0,1,0,1,0) \in (\mathbb{Z}_2)^6 \subset A_6$

By Theorem 4.10, the cycle of $\vec{a}$ is $(0,0,1,0,1,0), (0,1,1,1,1,0)$ and the period of $\vec{a}$ is 2

$\Longrightarrow$ the period of $\vec{a}$ is r

By **Case 1 and 2**, we complete this proof

□

Let r, s be positive integers. Suppose that $N = 2^s$ and $\vec{e}_1 = (1, 0, \cdots, 0) \in A_N$. By Theorem 3.15, all similar cycles of N-tuples in A_N are 1-cycle of $\vec{\mathbf{0}}$ which implies the period of every N-tuples in A_N is 1, and hence the conclusion in Theorem 4.12, that is r is the period of $\vec{a}$ for some $\vec{a} \in A_N$ if and only if r divides the period of $\vec{e}_1$, is true without identification we use in this chapter. However, above conclusion does not hold in A_6 due to Lemma 4.2.

If we had enough time, we would like to have further discussions about that at what positive integer N above conclusion holds (even if the identification we use in this chapter is necessary).

Bibliography

[1] M. Burmester, R. Forcade, and E. Jacobs. Circles of numbers. *Glasgow Mathematical Journal*, 19:115–119, July 1978.

[2] Amos Ehrlich. Periods in ducci's n-number game of differences. *Fibonacci Quarterly*, 28(4):302–305, November 1990.

[3] 蔡秀芬. Diffy box. 2008.