Diffy 六邊形之探討
A Study about Diffy Hexagons

王偉名
Wei-Ming Wang

Department of Mathematical Sciences,
National Chengchi University

August 2, 2014

Outline

Outline

Outline

Outline

Outline

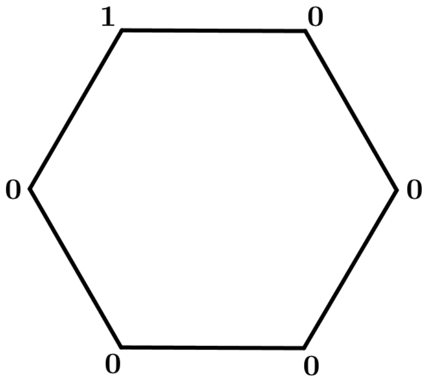
Introduction

Diffy Hexagons

The Diffy Hexagons which are generalized Diffy Boxes are games with the following procedures:

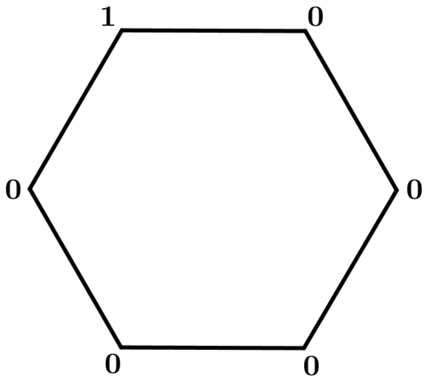
Step 1

Arrange six nonnegative integers around a regular hexagon.



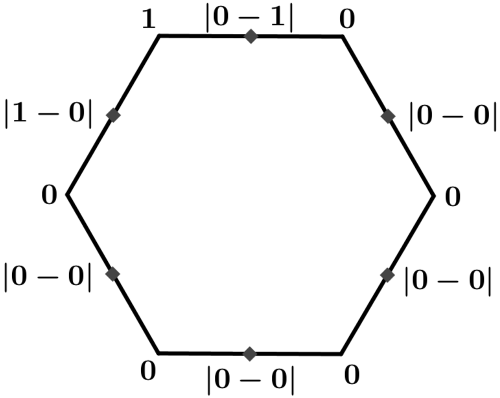
Step 2

Produce another regular hexagon of six nonnegative integers from the one obtained in Step 1:

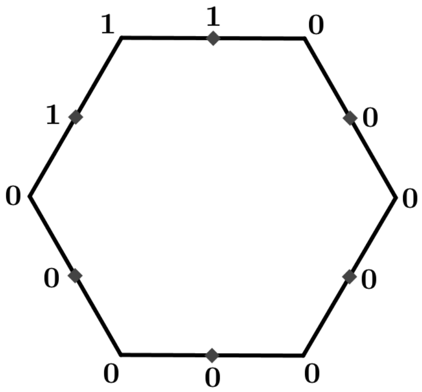


Step 2-1

For each adjacent pair of numbers, compute the absolute value of their difference and place it between them.

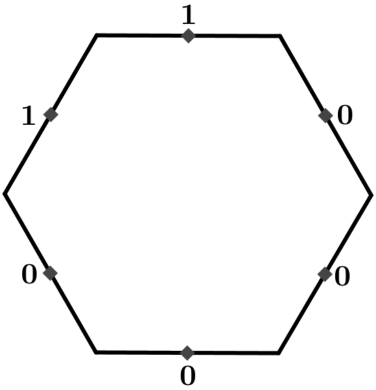


Step 2-1



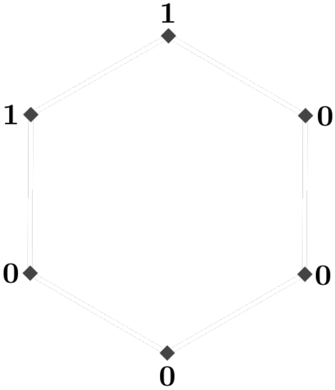
Step 2-2

Remove the original numbers.



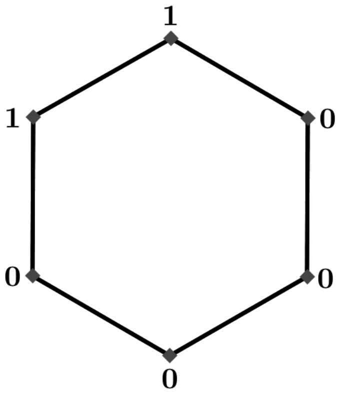
Step 2-3

Remove the original regular hexagon.



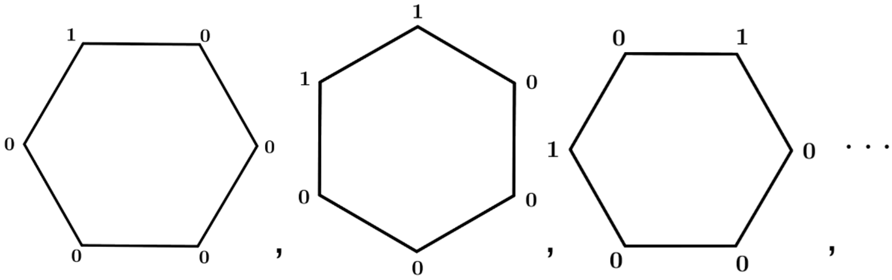
Step 2-4

Form the new regular hexagon with the remaining numbers.



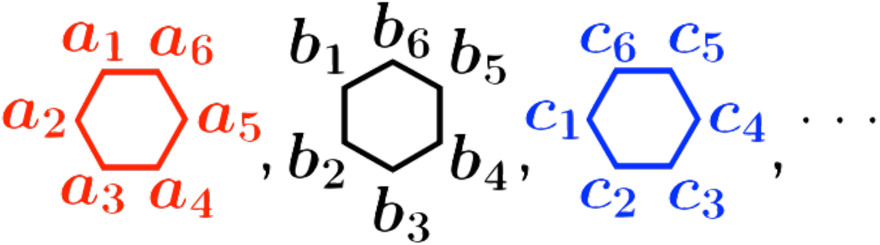
Step 3

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



Notations

Without loss of generality, we denote a regular hexagon of six nonnegative integers as follows:



where $b_i = |a_i - a_{i+1}|$, $c_i = |b_i - b_{i+1}|$, $b_6 = |a_6 - a_1|$, and $c_6 = |b_6 - b_1|$, $i = 1, 2, \cdots, 5$.

Notations

From now on, let N be a positive integer with $N \geq 2$

Notations

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

Notations

From now on, let N be a positive integer with $N \geq 2$ and 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 $(a_1, a_2, \cdots, a_N) \in A_N$.

Notations

From now on, let N be a positive integer with $N \geq 2$ and 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.

Ducci processes

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*.

Ducci sequences of N-tuples in A_N

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* $\vec{a}$.

Ducci sequences of N-tuples in A_N

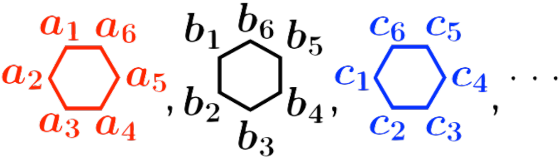
Definition (1.2)

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 $D^0(\vec{a})$.

Diffy Hexagon games

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.



$$D(a_1, a_2, \cdots, a_6) = (b_1, b_2, \cdots, b_6)$$
$$D(b_1, b_2, \cdots, b_6) = (c_1, c_2, \cdots, c_6)$$

Ducci Sequences

Existence of the period of 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

Existence of the period of 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

Example

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

$$\begin{aligned}
D^6(\vec{a}) &= (1,0,0,0,1,0) \\
D^7(\vec{a}) &= (1,0,0,1,1,1) \\
D^8(\vec{a}) &= (1,0,1,0,0,0) \\
D^9(\vec{a}) &= (1,1,1,0,0,1) \\
&= D^3(\vec{a})
\end{aligned}$$

The period and cycle of Ducci sequences

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 $0 \leq k \leq n-1$.

The period and cycle of Ducci sequences

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 $0 \leq k \leq n-1$.
We define the *period of* $\vec{a}$ to be $n-k$

The period and cycle of Ducci sequences

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 $0 \leq k \leq n-1$.
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 $D^k(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^{n-1}(\vec{a})$.

The largest component of N-tuples in A_N

Definition (2.3)

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

A property about the largest component of N-tuples in A_N

Lemma (2.5)

Let $\vec{a} \in A_N$. For all nonnegative integers r, s with $r \geq s$, then we have $\max D^r(\vec{a}) \leq \max D^s(\vec{a})$.

Proof

A property about the largest component of N-tuples in A_N

Lemma (2.5)

Let $\vec{a} \in A_N$. For all nonnegative integers r, s with $r \geq s$, then we have $\max D^r(\vec{a}) \leq \max D^s(\vec{a})$.

Proof

Example

$$\begin{aligned}
\vec{a} &= (1,0,0,2,1,0) & \max \vec{a} &= 2 \\
D(\vec{a}) &= (1,0,2,1,1,1) & \max D(\vec{a}) &= 2 \\
D^2(\vec{a}) &= (1,2,1,0,0,0) & \max D^2(\vec{a}) &= 2 \\
D^3(\vec{a}) &= (1,1,1,0,0,1) & \max D^3(\vec{a}) &= 1 \\
D^4(\vec{a}) &= (0,0,1,0,1,0) & \max D^4(\vec{a}) &= 1 \\
&\vdots & &\vdots
\end{aligned}$$

The largest component of N-tuples in the cycle

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,

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

Proof

The largest component of N-tuples in the cycle

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,

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

Proof

Example

$$\vec{a} = (0,1,2,2,1,0)$$
$$D(\vec{a}) = (1,1,0,1,1,0)$$
$$D^2(\vec{a}) = (0,1,1,0,1,1)$$
$$D^3(\vec{a}) = (1,0,1,1,0,1)$$
$$D^4(\vec{a}) = (1,1,0,1,1,0) = D(\vec{a})$$

Components of N-tuples in the cycle

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 $\vec{a}$.

Components of N-tuples in the cycle

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

Components of N-tuples in the cycle

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

Example

$$\vec{a} = (0,2,4,4,2,0) \qquad D^3(\vec{a}) = (2,0,2,2,0,2)$$

$$D(\vec{a}) = (2,2,0,2,2,0) \qquad D^4(\vec{a}) = (2,2,0,2,2,0)$$

$$D^2(\vec{a}) = (0,2,2,0,2,2) \qquad = D(\vec{a})$$

The converse of Theorem 2.12 fails in general

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

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

The converse of Theorem 2.12 fails in general

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

The converse of Theorem 2.12 fails in general

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

Example

Let $N = 6$, $\vec{a} = (2014, 0, 1, 1, 1, 1)$ and $D(\vec{a}) = \vec{b}$

The converse of Theorem 2.12 fails in general

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

Example

Let $N = 6$, $\vec{a} = (2014, 0, 1, 1, 1, 1)$ and $D(\vec{a}) = \vec{b}$
Then, $\vec{b} = (2014, 1, 0, 0, 0, 2013)$

The greatest common divisor of components of N-tuples in A_N

Definition (2.14)

Let $\vec{a} \in A_N$ with $\vec{a} \neq \vec{\mathbf{0}}$.

The greatest common divisor of components of N-tuples in A_N

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 $\gcd(a_1, a_2, \cdots, a_N)$.

The relation between $\max \vec{a}$ and $\gcd \vec{a}$

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

The relation between $\max \vec{a}$ and $\gcd \vec{a}$

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

Example

Let $\vec{a} = (0, 2, 4, 4, 2, 0)$

The relation between $\max \vec{a}$ and $\gcd \vec{a}$

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

Example

Let $\vec{a} = (0, 2, 4, 4, 2, 0)$

$\implies \gcd(\vec{a}) = 2$

The relation between $\max \vec{a}$ and $\gcd \vec{a}$

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

Example

Let $\vec{a} = (0, 2, 4, 4, 2, 0)$

$\implies \gcd(\vec{a}) = 2$

$$D(\vec{a}) = (2, 2, 0, 2, 2, 0)$$

$$D^2(\vec{a}) = (0, 2, 2, 0, 2, 2)$$

$$D^3(\vec{a}) = (2, 0, 2, 2, 0, 2)$$

$$D^4(\vec{a}) = (2, 2, 0, 2, 2, 0) = D(\vec{a})$$

Components of N-tuples in the cycle

Corollary (2.16)

Let $\vec{a} \in A_N$ with $\vec{a} \neq \vec{\mathbf{0}}$. Suppose $D^k(\vec{a}), D^{k+1}(\vec{a}), \cdots, D^{n-1}(\vec{a})$ is the $(n-k)$-cycle of $\vec{a}$.

Components of N-tuples in the cycle

Corollary (2.16)

Let $\vec{a} \in A_N$ with $\vec{a} \neq \vec{\mathbf{0}}$. 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 is a multiple of $\gcd \vec{a}$.

Proof

In Corollary 2.16, M may be any nonnegative integer

Example (2.17)

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

In Corollary 2.16, M may be any nonnegative integer

Example (2.17)

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

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

Similar Cycles

Similar cycles

Definition (3.1)

Let $\vec{a} \in A_N$ and $\vec{b} \in (\mathbb{Z}_2)^N$. Suppose that $D^k(\vec{b}), D^{k+1}(\vec{b}), \cdots, D^{n-1}(\vec{b})$ is the $(n-k)$-cycle of $\vec{b}$.

Similar cycles

Definition (3.1)

Let $\vec{a} \in A_N$ and $\vec{b} \in (\mathbb{Z}_2)^N$. Suppose that $D^k(\vec{b}), D^{k+1}(\vec{b}), \cdots, D^{n-1}(\vec{b})$ is the $(n-k)$-cycle of $\vec{b}$. The cycle of $\vec{a}$ is said to be *similar to the cycle of* $\vec{b}$,

Similar cycles

Definition (3.1)

Let $\vec{a} \in A_N$ and $\vec{b} \in (\mathbb{Z}_2)^N$. Suppose that $D^k(\vec{b}), D^{k+1}(\vec{b}), \cdots, D^{n-1}(\vec{b})$ 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 $k \leq s \leq n-1$.

The period of similar cycles

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

The period of similar cycles

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

Example

$$\begin{aligned} \vec{a} &= (0,2,4,4,2,0) \\ D(\vec{a}) &= (2,2,0,2,2,0) \\ D^2(\vec{a}) &= (0,2,2,0,2,2) \\ D^3(\vec{a}) &= (2,0,2,2,0,2) \\ D^4(\vec{a}) &= (2,2,0,2,2,0) \\ &= D(\vec{a}) \end{aligned}$$

$$\begin{aligned} \vec{b} &= (0,1,0,0,1,0) \\ D(\vec{b}) &= (1,1,0,1,1,0) \\ D^2(\vec{b}) &= (0,1,1,0,1,1) \\ D^3(\vec{b}) &= (1,0,1,1,0,1) \\ D^4(\vec{b}) &= (1,1,0,1,1,0) \\ &= D(\vec{b}) \end{aligned}$$

Cycles of N-tuples in A_N

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.

Periods of N-tuples in A_N

Theorem (3.13)

Let $\vec{e}_i = (\delta_{i1}, \delta_{i2}, \cdots, \delta_{iN}) \in A_N$*, where* δ_{ij} *is the Kronecker delta for all* $i, j \in \{1, 2, \cdots, N\}$.

Periods of N-tuples in A_N

Theorem (3.13)

Let $\vec{e}_i = (\delta_{i1}, \delta_{i2}, \cdots, \delta_{iN}) \in A_N$*, where* δ_{ij} *is the Kronecker delta 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

Periods of N-tuples in A_N

Theorem (3.13)

Let $\vec{e}_i = (\delta_{i1}, \delta_{i2}, \cdots, \delta_{iN}) \in A_N$, *where* δ_{ij} *is the Kronecker delta 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:* $D^r(\vec{b}) = D^s(\vec{b}), \forall \vec{b} \in (\mathbb{Z}_2)^N$.

Periods of N-tuples in A_N

Theorem (3.13)

Let $\vec{e}_i = (\delta_{i1}, \delta_{i2}, \cdots, \delta_{iN}) \in A_N$*, where* δ_{ij} *is the Kronecker delta 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.*

Periods of N-tuples in A_N

Theorem (3.13)

Let $\vec{e}_i = (\delta_{i1}, \delta_{i2}, \cdots, \delta_{iN}) \in A_N$, where δ_{ij} is the Kronecker delta 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 $\vec{e}_1$.*

Periods of N-tuples in A_N

Theorem (3.13)

Let $\vec{e}_i = (\delta_{i1}, \delta_{i2}, \cdots, \delta_{iN}) \in A_N$, where δ_{ij} is the Kronecker delta 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

Cycles of 2^r-tuples in A_{2^r}

Theorem (3.15)

Let r be a positive integer. Suppose that $N = 2^r$.

Cycles of 2^r-tuples in A_{2^r}

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

Cycles of 2^r-tuples in A_{2^r}

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

Example

$$\begin{aligned} \vec{a} &= (0,1,2,0) \\ D(\vec{a}) &= (1,1,2,0) \\ D^2(\vec{a}) &= (0,1,2,1) \\ D^3(\vec{a}) &= (1,1,1,1) \end{aligned}$$

$$\begin{aligned} D^4(\vec{a}) &= (0,0,0,0) \\ D^5(\vec{a}) &= (0,0,0,0) \\ &= D^4(\vec{a}) \end{aligned}$$

Diffy Hexagons

Introduction

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

The period of 6-tuples in A_6

Theorem (4.1)

The period of 6-tuples in A_6 divides 6.

The period of 6-tuples in A_6

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

The period of 6-tuples in A_6

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

Example

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

Cycles of 6-tuples in $(\mathbb{Z}_2)^6$

Lemma (4.2)

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

Cycles of 6-tuples in $(\mathbb{Z}_2)^6$

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) $(0, 0, 0, 0, 0, 0)$

$$\mathbf{(0, 0, 0, 0, 0, 0)} \circlearrowleft$$

$\rightarrow$: *a Ducci process*

Cycles of 6-tuples in $(\mathbb{Z}_2)^6$

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) $(0,0,0,0,0,0)$

$$\begin{tikzcd}[column sep=small]
(0,1,0,1,0,1) \arrow[dr] & & (1,0,1,0,1,0) \arrow[dl] \\
& (1,1,1,1,1,1) \arrow[d] & \\
& \mathbf{(0,0,0,0,0,0)} \arrow[loop below] &
\end{tikzcd}$$

$\rightarrow$: *a Ducci process*

Cycles of 6-tuples in $(\mathbb{Z}_2)^6$

Lemma (4.2)

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

$$\begin{tikzcd}
& \mathbf{(0,1,1,0,1,1)} \arrow[dr, bend left] & \\
\mathbf{(1,1,0,1,1,0)} \arrow[ur, bend left] & & \mathbf{(1,0,1,1,0,1)} \arrow[ll, bend left]
\end{tikzcd}$$

$\rightarrow$: *a Ducci process*

Cycles of 6-tuples in $(\mathbb{Z}_2)^6$

Lemma (4.2)

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

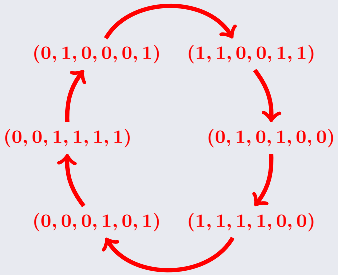
$$
\begin{tikzcd}[column sep=tiny]
 & & (0,0,0,1,1,1) \arrow[dr] & & (1,1,1,0,0,0) \arrow[dl] & & \\
 & & & (0,0,1,0,0,1) \arrow[d] & & & \\
 & & & \mathbf{(0,1,1,0,1,1)} \arrow[dr, bend left] & & & \\
 & & \mathbf{(1,1,0,1,1,0)} \arrow[ur, bend left] & & \mathbf{(1,0,1,1,0,1)} \arrow[ll, bend left] & & \\
 & (0,1,0,0,1,0) \arrow[ur] & & & & (1,0,1,1,0,0) \arrow[ul] & \\
(1,1,0,0,0,1) \arrow[ur] & & (0,0,1,1,1,0) \arrow[ul] & & (0,1,1,1,0,0) \arrow[ur] & & (1,0,0,0,1,1) \arrow[ul]
\end{tikzcd}
$$

$\rightarrow$: *a Ducci process*

Cycles of 6-tuples in $(\mathbb{Z}_2)^6$

Lemma (4.2)

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

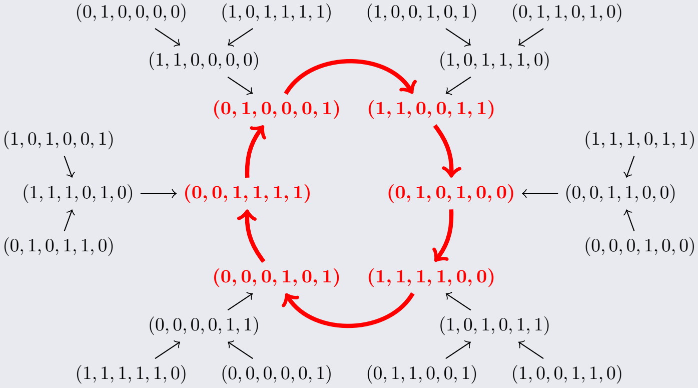


$\rightarrow$: *a Ducci process*

Cycles of 6-tuples in $(\mathbb{Z}_2)^6$

Lemma (4.2)

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

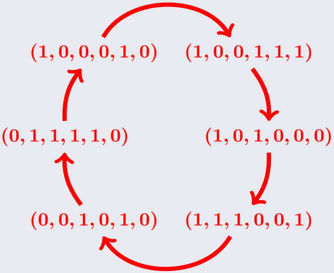


$\longrightarrow$: *a Ducci process*

Cycles of 6-tuples in $(\mathbb{Z}_2)^6$

Lemma (4.2)

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

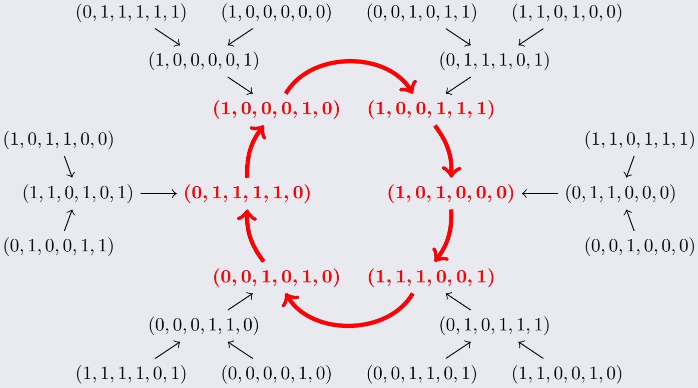


$\rightarrow$: *a Ducci process*

Cycles of 6-tuples in $(\mathbb{Z}_2)^6$

Lemma (4.2)

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



$\longrightarrow$: *a Ducci process*

Ducci sequences and Diffy Hexagons

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.

Ducci sequences and Diffy Hexagons

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,

Ducci sequences and Diffy Hexagons

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.

Prepare for an identification on Ducci sequences

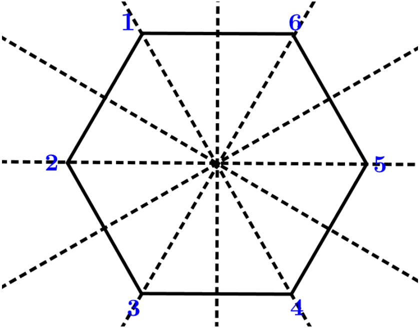
Write $\mathcal{D}_6 = \{(1)(2)(3)(4)(5)(6), (123456), (135)(246), (14)(25)(36), (153)(264), (165432), (16)(25)(34), (1)(4)(26)(35), (12)(36)(45), (2)(5)(13)(46), (14)(23)(56), (3)(6)(15)(24)\}$

Prepare for an identification on Ducci sequences

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.

Prepare for an identification on Ducci sequences

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.



Prepare for an identification on Ducci sequences

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 $(a_1, a_2, \cdots, a_6) \in A_6$.

Prepare for an identification on Ducci sequences

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.

Prepare for an identification on Ducci sequences

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

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

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

An identification on Ducci sequences

For all $\vec{x}, \vec{y} \in A_6$, define $\vec{x} \equiv \vec{y}$ by $\vec{x} = \pi * \vec{y}$ for some $\pi \in \mathcal{D}_6$.

An identification on Ducci sequences

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

An identification on Ducci sequences

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 $(a_1, a_2, \cdots, a_6) \in A_6$.

An identification on Ducci sequences

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 $\vec{x} \equiv \vec{y}$.

An identification on Ducci sequences

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 $[\,\vec{a}\,] = [\,\vec{b}\,]$.

An identification on Ducci sequences

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.

Diffy Hexagons whose components are consisting of $\{0, 1\}$

Lemma (4.9)

There are 13 *equivalence classes of* $(\mathbb{Z}_2)^6$.

Diffy Hexagons whose components are consisting of $\{0, 1\}$

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 $(1,1,1,1,1,1)$.

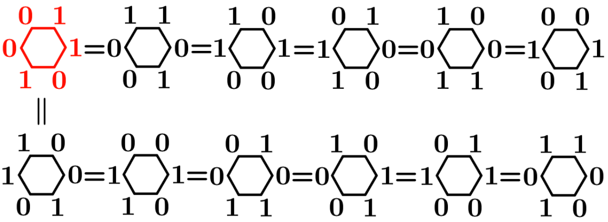
Proof

Diffy Hexagons whose components are consisting of $\{0,1\}$

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



Cycles of Diffy Hexagons whose components are consisting of $\{0, 1\}$

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) $(0, 0, 0, 0, 0, 0)$

$$\mathbf{(0, 0, 0, 0, 0, 0)}$$
$$\circlearrowleft$$

$\rightarrow$: *a Ducci process*

Cycles of Diffy Hexagons whose components are consisting of $\{0,1\}$

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) $(0,0,0,0,0,0)$

$$\begin{array}{c} (0,1,0,1,0,1) \\ \downarrow \\ (1,1,1,1,1,1) \\ \downarrow \\ \mathbf{(0,0,0,0,0,0)} \\ \circlearrowleft \end{array}$$

$\rightarrow$: *a Ducci process*

Cycles of Diffy Hexagons whose components are consisting of $\{0, 1\}$

Theorem (4.10)

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

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

$\circlearrowleft$

$\rightarrow$: *a Ducci process*

Cycles of Diffy Hexagons whose components are consisting of $\{0, 1\}$

Theorem (4.10)

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

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

$\longrightarrow$: *a Ducci process*

Cycles of Diffy Hexagons whose components are consisting of $\{0, 1\}$

Theorem (4.10)

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

$$\begin{tikzcd} \mathbf{(1,0,0,0,1,0)} \arrow[r, bend left] & \mathbf{(1,0,0,1,1,1)} \arrow[l, bend left] \end{tikzcd}$$

$\rightarrow$: *a Ducci process*

Cycles of Diffy Hexagons whose components are consisting of $\{0, 1\}$

Theorem (4.10)

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

$$
\begin{tikzcd}
(0,1,1,1,1,1) \arrow[dr] & & (1,0,0,0,0,0) \arrow[dl] & & & (0,1,1,1,0,1) \arrow[dl] \\
& (0,1,1,1,0,1) \arrow[dr] & & & (0,1,1,1,0,1) \arrow[dl] & \\
& & \mathbf{(1,0,0,0,1,0)} \arrow[r, bend left] & \mathbf{(1,0,0,1,1,1)} \arrow[l, bend left] & &
\end{tikzcd}
$$

$\rightarrow$: *a Ducci process*

The period of Diffy Hexagons

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

Thank You

Appendix

Proof for Lemma 2.1

Lemma 2.1

Proof.

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

Proof for Lemma 2.1

Lemma 2.1

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 $\vec{a}$

Proof for Lemma 2.1

Lemma 2.1

Proof.

Write $\vec{a} = (a_1, a_2, \cdots, a_N)$
Let $M = \max\{a_1, a_2, \cdots, a_N\}$
$\implies$ 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 $D^n(\vec{a}) = D^k(\vec{a})$ $\square$

Proof for Remark 2.4

Remark 2.4

Proof.

Note that $-M \leq x - y \leq M$

Proof for Remark 2.4

Remark 2.4

Proof.

Note that $-M \leq x - y \leq M$, then we obtain $|x - y| \leq M$ $\square$

Proof for Lemma 2.5

Lemma 2.5

Proof.

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

Proof for Lemma 2.5

Lemma 2.5

Proof.

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

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

Proof for Lemma 2.5

Lemma 2.5

Proof.

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

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

Now, we may assume that $r > s$

Proof for Lemma 2.5

Lemma 2.5

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

Proof for Lemma 2.5

Lemma 2.5

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

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

Proof for Lemma 2.5

Lemma 2.5

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

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

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

Proof for Lemma 2.5

Lemma 2.5

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

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

$\because 0 \leq x_1, x_2, \cdots, x_N \leq \max D^{s}(\vec{a})$
$\therefore$ By Remark 2.4, $y_i \leq \max D^{s}(\vec{a})$ for all $i = 1, 2, \cdots, N$

Proof for Lemma 2.5

Lemma 2.5

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

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

$\because 0 \leq x_1, x_2, \cdots, x_N \leq \max D^s(\vec{a})$
$\therefore$ By Remark 2.4, $y_i \leq \max D^s(\vec{a})$ for all $i = 1, 2, \cdots, N$
$\implies \max D^{s+1}(\vec{a}) \leq \max D^s(\vec{a})$ $\square$

Proof for Lemma 2.6

Lemma 2.6

Proof.

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

We may assume that $r \leq s$

Proof for Lemma 2.6

Lemma 2.6

Proof.

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

We may assume that $r \leq s$

If $r = s$, then it is trivial

Proof for Lemma 2.6

Lemma 2.6

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

Proof for Lemma 2.6

Lemma 2.6

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 $\square$

Proof for Lemma 2.6

(continued...)

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

Proof for Lemma 2.6

(continued...)

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

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

Proof for Lemma 2.6

(continued...)

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

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

Proof for Remark 2.7

Remark 2.7

Proof.

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

Proof for Remark 2.7

Remark 2.7

Proof.

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

Case 1: $x-y = M$

Proof for Remark 2.7

Remark 2.7

Proof.

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

Case 1: $x - y = M$

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

Proof for Remark 2.7

Remark 2.7

Proof.

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

Case 1: $x - y = M$

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

$\implies y \leq 0$

Proof for Remark 2.7

Remark 2.7

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, $y \geq 0$

Proof for Remark 2.7

Remark 2.7

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, $y \geq 0$

$\therefore y = 0$

Proof for Remark 2.7

Remark 2.7

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, $y \geq 0$

$\therefore y = 0$

$\implies x = M$

Proof for Remark 2.7

Remark 2.7

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

Proof for Remark 2.7

Remark 2.7

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: $x - y = -M$

Proof for Remark 2.7

Remark 2.7

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: $x - y = -M$

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

Proof for Remark 2.7

Remark 2.7

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: $x - y = -M$

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

$\implies x \leq 0$

Proof for Remark 2.7

Remark 2.7

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 $x \geq 0$ □

Proof for Remark 2.7

(continued...)

$\therefore x = 0$

Proof for Remark 2.7

(continued...)

$\therefore x = 0$

$\implies y = M$

Proof for Remark 2.7

(continued...)

$\therefore\ x = 0$

$\implies y = M$

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

Proof for Lemma 2.8

Lemma 2.8

Proof.

We prove it by induction on t:

Proof for Lemma 2.8

Lemma 2.8

Proof.

We prove it by induction on t:

t=1:

Proof for Lemma 2.8

Lemma 2.8

Proof.

We prove it by induction on t:

t=1:

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

Proof for Lemma 2.8

Lemma 2.8

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

Proof for Lemma 2.8

Lemma 2.8

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, $t = K + 1$:

Proof for Lemma 2.8

Lemma 2.8

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 $a_2 = a_3 = \cdots = a_K = a_{K+1} = 0$

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

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

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

Proof for Lemma 2.8

(continued...)

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

Proof for Lemma 2.8

(continued...)

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

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

Proof for Lemma 2.8

(continued...)

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 $0 \leq b_1, b_2 \leq M$

Proof for Lemma 2.8

(continued...)

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

Proof for Lemma 2.8

(continued...)

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 $\square$

Proof for Lemma 2.8

(continued...)

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

Proof for Lemma 2.8

(continued...)

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 $D(\vec{b}) = \vec{a}$

Proof for Lemma 2.8

(continued...)

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 $0 \leq b_{K+1}, b_{K+2} \leq M$

Proof for Lemma 2.8

(continued...)

Case 2: $a_{K+1} = M$ and $a_1 = a_2 = a_3 = \cdots = a_K = 0$
$\Longrightarrow\ b_1 = b_2 = \cdots = b_K = b_{K+1}$, 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, we obtain $b_{K+1}, b_{K+2} \in \{0, M\}$ and at least one of them is M

Proof for Lemma 2.8

(continued...)

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, we obtain $b_{K+1}, b_{K+2} \in \{0, M\}$ 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

$\square$

Proof for Lemma 2.8

(continued...)

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

Proof for Lemma 2.8

(continued...)

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 $D(\vec{b}) = \vec{a}$

Proof for Lemma 2.8

(continued...)

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 $0 \leq b_1, b_2 \leq M$

Proof for Lemma 2.8

(continued...)

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

Proof for Lemma 2.8

(continued...)

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 $0 \leq b_{K+1}, b_{K+2} \leq M$

Proof for Lemma 2.8

(continued...)

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 $0 \le b_1, b_2 \le M$
$\therefore$ 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 $0 \le b_{K+1}, b_{K+2} \le M$
By Remark 2.7, we have $b_{K+1}, b_{K+2} \in \{0, M\}$ and at least one of them is M

Proof for Lemma 2.8

(continued...)

Case 3: $a_1 = a_{K+1} = M$ and $a_2 = a_3 = \cdots = a_K = 0$
$\Longrightarrow \; b_2 = b_3 = \cdots = b_K = b_{K+1}$, since $D(\vec{b}) = \vec{a}$
$\because M = a_1 = |b_1 - b_2|$ and $0 \le b_1, b_2 \le M$
$\therefore$ 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 $0 \le b_{K+1}, b_{K+2} \le M$
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 $\square$

Proof for Lemma 2.8

(continued...)

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

Proof for Lemma 2.8

(continued...)

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 $2 \leq i \leq K$

Proof for Lemma 2.8

(continued...)

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

Proof for Lemma 2.8

(continued...)

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

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

$\square$

Proof for Lemma 2.8

(continued...)

Since Ducci processes are cyclic,

Proof for Lemma 2.8

(continued...)

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

Proof for Lemma 2.8

(continued...)

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 □

Proof for Lemma 2.10

Lemma 2.10

Proof.

We prove it by induction on i:

Proof for Lemma 2.10

Lemma 2.10

Proof.

We prove it by induction on i:

$i = 0$:

Proof for Lemma 2.10

Lemma 2.10

Proof.

We prove it by induction on i:

$i = 0$:

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

Proof for Lemma 2.10

Lemma 2.10

Proof.

We prove it by induction on i:

$i = 0$:

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

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

Proof for Lemma 2.10

Lemma 2.10

Proof.

We prove it by induction on i:

$i = 0$:

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

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

$\implies$ 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

Proof for Lemma 2.10

Lemma 2.10

Proof.

We prove it by induction on i:

$i = 0$:

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

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

$\implies$ 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 $i = K + 1$:

Proof for Lemma 2.10

Lemma 2.10

Proof.

We prove it by induction on i:

$i = 0$:

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

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

$\implies$ 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: $\square$

Proof for Lemma 2.10

(continued...)

Write

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

Proof for Lemma 2.10

(continued...)

Write

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

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

Proof for Lemma 2.10

(continued...)

Write

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

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

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

Proof for Lemma 2.10

(continued...)

Write

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

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

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

Proof for Lemma 2.10

(continued...)

Write

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

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

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 $\square$

Proof for Lemma 2.10

(continued...)

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

Proof for Lemma 2.10

(continued...)

By Lemma 2.8, $x_1, x_2, \cdots, x_K, x_{K+1}, x_{K+2} \in \{0, M\}$ 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, so $i = K+1$ holds $\square$

Proof for Remark 2.11

Remark 2.11

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:

Proof for Remark 2.11

Remark 2.11

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:

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

Proof for Remark 2.11

Remark 2.11

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:

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

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

Proof for Remark 2.11

Remark 2.11

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 $0 \leq i \leq n-k-1$

Proof for Remark 2.11

Remark 2.11

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 $0 \leq i \leq n-k-1$ and

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

$\square$

Proof for Theorem 2.12

Theorem 2.12

Proof.

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

Proof for Theorem 2.12

Theorem 2.12

Proof.

Therefore, $D^{(n-1)-i}(\vec{a})$ is in the $(n-k)$-cycle
By Lemma 2.6, we obtain $\max D^j(\vec{a}) = \max D^k(\vec{a}) = M$ for all $j = k, k+1, \cdots, n-1$

Proof for Theorem 2.12

Theorem 2.12

Proof.

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

Proof for Theorem 2.12

Theorem 2.12

Proof.

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

Proof for Theorem 2.12

Theorem 2.12

Proof.

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

Proof for Theorem 2.12

Theorem 2.12

Proof.

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

□

Proof for Theorem 2.12

(continued...)

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

Proof for Theorem 2.12

(continued...)

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

$\Longrightarrow$ 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 $\square$

Proof for Remark 2.13

Remark 2.13

Proof.

Let $M > 1$ be an integer

Proof for Remark 2.13

Remark 2.13

Proof.

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

Proof for Remark 2.13

Remark 2.13

Proof.

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

Proof for Remark 2.13

Remark 2.13

Proof.

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

Proof for Remark 2.13

Remark 2.13

Proof.

Let $M > 1$ be an integer and $\vec{a} = (M, 0, 1, \cdots, 1, 1) \in A_N$
Choose $\vec{b} = D(\vec{a}) \in A_N$
$\implies \vec{b} = (M, 1, 0, \cdots, 0, M-1)$
Note that $\max \vec{a} = \max \vec{b} = M$

Proof for Remark 2.13

Remark 2.13

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 $\square$

Proof for Lemma 2.15

Lemma 2.15

Proof.

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

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

Proof for Lemma 2.15

Lemma 2.15

Proof.

Let $\gcd \vec{a} = d$
Write $\vec{a} = d\vec{b}$ with $\gcd \vec{b} = 1$
Note that $d > 0$ and $D(\vec{a}) = D(d\vec{b}) = dD(\vec{b})$

Proof for Lemma 2.15

Lemma 2.15

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

Proof for Lemma 2.15

Lemma 2.15

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 $\gcd \vec{a} \mid D^n(\vec{a})$ $\square$

Proof for Corollary 2.16

Corollary 2.16

Proof.

It follows from Theorem 2.12 and Lemma 2.15 □

Proof for Lemma 2.18

Lemma 2.18

Proof.

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

Proof for Lemma 2.18

Lemma 2.18

Proof.

It suffices to show that $\gcd D^r(\vec{a}) \mid \gcd D^s(\vec{a})$
Given nonnegative integers r, s with $r \leq s$

Proof for Lemma 2.18

Lemma 2.18

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 $r < s$

Proof for Lemma 2.18

Lemma 2.18

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

Proof for Lemma 2.18

Lemma 2.18

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 $\gcd D^r(\vec{a}) = d$

Proof for Lemma 2.18

Lemma 2.18

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 $D^r(\vec{a}) \in A_N$

Proof for Lemma 2.18

Lemma 2.18

Proof.

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

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

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 $D^r(\vec{a}) \in A_N$

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

Proof for Lemma 2.18

Lemma 2.18

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

Proof for Lemma 2.18

Lemma 2.18

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

Proof for Lemma 2.18

Lemma 2.18

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

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

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

Proof for Lemma 2.19

Lemma 2.19

Proof.

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

We may assume that $r \leq s$

Proof for Lemma 2.19

Lemma 2.19

Proof.

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

We may assume that $r \leq s$

If $r = s$, then it is trivial

Proof for Lemma 2.19

Lemma 2.19

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

Proof for Lemma 2.19

Lemma 2.19

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 $D^s(\vec{a})$:

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

Proof for Lemma 2.19

Lemma 2.19

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 □

Proof for Lemma 2.19

(continued...)

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

Proof for Lemma 2.19

(continued...)

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

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

Proof for Lemma 2.19

(continued...)

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

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

Proof for Theorem 3.2

Theorem 3.2

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 $\vec{a}$

Proof for Theorem 3.2

Theorem 3.2

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

Proof for Theorem 3.2

Theorem 3.2

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

Proof for Theorem 3.2

Theorem 3.2

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

Proof for Theorem 3.2

Theorem 3.2

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
$\Longrightarrow$ We have the following two cases:
Case 1: $M = 0$
Case 2: $M > 0$ $\square$

Proof for Theorem 3.2

(continued...)

Case 1: $M = 0$

Proof for Theorem 3.2

(continued...)

Case 1: $M = 0$

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

Proof for Theorem 3.2

(continued...)

Case 1: $M = 0$

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

$\implies$

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

Proof for Theorem 3.2

(continued...)

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

Proof for Theorem 3.2

(continued...)

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 $n - k$

Proof for Theorem 3.2

(continued...)

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 $n - k$

$\therefore k \leq n - 1$

Proof for Theorem 3.2

(continued...)

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 $n - 1 = k$

Proof for Theorem 3.2

(continued...)

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 $n - k = 1$

Proof for Theorem 3.2

(continued...)

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

Proof for Theorem 3.2

(continued...)

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

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

$\square$

Proof for Theorem 3.2

(continued...)

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

Proof for Theorem 3.2

(continued...)

$\Longrightarrow$ 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 $\vec{b}$

Proof for Theorem 3.2

(continued...)

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

Proof for Theorem 3.2

(continued...)

$\implies$ 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

Proof for Theorem 3.2

(continued...)

$\implies$ 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: $M>0$

Proof for Theorem 3.2

(continued...)

$\implies$ 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: $M > 0$

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

Proof for Theorem 3.2

(continued...)

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

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

Hence, we are done

Case 2: $M>0$

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

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

Proof for Theorem 3.2

(continued...)

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

Proof for Theorem 3.2

(continued...)

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

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

Proof for Theorem 3.2

(continued...)

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

Proof for Theorem 3.2

(continued...)

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

Proof for Theorem 3.2

(continued...)

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

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

Proof for Theorem 3.2

(continued...)

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

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

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

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

Proof for Theorem 3.2

(continued...)

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

Proof for Theorem 3.2

(continued...)

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

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

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

Proof for Theorem 3.2

(continued...)

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

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

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

Proof for Theorem 3.2

(continued...)

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

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

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 $\vec{b}$

$\square$

Proof for Theorem 3.2

(continued...)

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

Proof for Theorem 3.2

(continued...)

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

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

Hence, we complete this proof $\square$

Proof for Lemma 3.4

Lemma 3.4

Proof.

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

Proof for Lemma 3.4

Lemma 3.4

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 $k \le s \le n - 1$

Proof for Lemma 3.4

Lemma 3.4

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:

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

□

Proof for Lemma 3.4

Proof.

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

$\Longrightarrow D^{r+1}(\vec{a^c}) = mD^{s+1}(\vec{b})$ which completes this proof $\square$

Proof for Remark 3.5

Remark 3.5

Proof.

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

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

Proof for Remark 3.5

Remark 3.5

Proof.

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

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

$\implies s+1 = n$

Proof for Remark 3.5

Remark 3.5

Proof.

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

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

$\implies s+1 = n$

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

Proof for Lemma 3.6

Lemma 3.6

Proof.

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

Proof for Lemma 3.6

Lemma 3.6

Proof.

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

"$\Rightarrow$" Suppose the condition holds

Proof for Lemma 3.6

Lemma 3.6

Proof.

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

"$\Rightarrow$" Suppose the condition holds

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

Proof for Lemma 3.6

Lemma 3.6

Proof.

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

"$\Rightarrow$" Suppose the condition holds

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

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

Proof for Lemma 3.6

Lemma 3.6

Proof.

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

"$\Rightarrow$" Suppose the condition holds

$$\begin{aligned}
&\Longrightarrow \exists\, k \le r \le n-1 \text{ such that } \vec{a^c} = D^r(\vec{a}) \\
&\Longrightarrow D(\vec{a}) = D(\vec{a^c}) = D(D^r(\vec{a})) = D^{r+1}(\vec{a}) \\
&\Longrightarrow n-1 \le r, \text{ since } D^0(\vec{a}) = \vec{a}, D(\vec{a}), \cdots, \\
&D^k(\vec{a}), \cdots, D^r(\vec{a}), \cdots, D^{n-1}(\vec{a}) \text{ are all distinct}
\end{aligned}$$

Proof for Lemma 3.6

Lemma 3.6

Proof.

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

"$\Rightarrow$" Suppose the condition holds

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

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

$\Longrightarrow$ $n-1 \leq r$, 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, $r = n-1$

Proof for Lemma 3.6

Lemma 3.6

Proof.

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

"$\Rightarrow$" Suppose the condition holds

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

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

$\Longrightarrow n-1 \leq r$, 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, $r = n-1$

$\Longrightarrow n = r+1$

Proof for Lemma 3.6

Lemma 3.6

Proof.

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

"$\Rightarrow$" Suppose the condition holds

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

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

$\Longrightarrow \ n-1 \le r$, 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, $r = n-1$

$\Longrightarrow \ n = r+1$

Then, we have:

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

$\square$

Proof for Lemma 3.6

(continued...)

"$\Rightarrow$" **Claim:** $k = 0$

Proof.

If not, suppose $k \geq 1$

Proof for Lemma 3.6

(continued...)

"$\Rightarrow$" **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

Proof for Lemma 3.6

(continued...)

"$\Rightarrow$" **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 $(*)$

Proof for Lemma 3.6

(continued...)

"$\Rightarrow$" **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

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

$\Longrightarrow \ n \leq k$ which is a contradiction to $n > k$ $\square$

Proof for Lemma 3.6

(continued...)

"$\Rightarrow$" **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

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

$\Longrightarrow \; n \leq k$ which is a contradiction to $n > k$ $\square$

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

Proof for Lemma 3.6

(continued...)

"$\Rightarrow$" **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
$\Longrightarrow$ $n-1 \leq k-1$, by $(*)$
$\Longrightarrow$ $n \leq k$ which is a contradiction to $n > k$ $\square$

By **Claim** and $(*)$, we obtain $\vec{a} = D^0(\vec{a}) = D(\vec{a^c})$
$\Longrightarrow$ $\forall 1 \leq i \leq N, a_i = M - a_i$

Proof for Lemma 3.6

(continued...)

"$\Rightarrow$" **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 $n > k$ $\square$

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

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

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

$\square$

Proof for Lemma 3.6

(continued...)

$$\text{“}\Rightarrow\text{”} \quad \Longrightarrow \; M = \max \vec{a} = \frac{M}{2}$$

Proof for Lemma 3.6

(continued...)

$$\text{“}\Rightarrow\text{”} \quad \Longrightarrow \quad M = \max \vec{a} = \frac{M}{2}$$
$$\Longrightarrow \quad M = 0$$

Proof for Lemma 3.6

(continued...)

$$\text{“}\Rightarrow\text{”} \quad \Longrightarrow \quad M = \max \vec{a} = \frac{M}{2}$$

$$\Longrightarrow \quad M = 0$$

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

Proof for Lemma 3.6

(continued...)

$$
\begin{aligned}
\text{“}\Rightarrow\text{”} \quad & \Longrightarrow \ M = \max \vec{a} = \frac{M}{2} \\
& \Longrightarrow \ M = 0 \\
& \because 0 \leq a_1, a_2, \cdots, a_N \leq M = 0 \\
& \therefore a_1 = a_2 = \cdots = a_N = 0
\end{aligned}
$$

Proof for Lemma 3.6

(continued...)

$$
\begin{aligned}
\text{“}\Rightarrow\text{”} \quad & \Longrightarrow \quad M = \max \vec{a} = \frac{M}{2} \\
& \Longrightarrow \quad M = 0 \\
& \because 0 \le a_1, a_2, \cdots, a_N \le M = 0 \\
& \therefore a_1 = a_2 = \cdots = a_N = 0 \\
& \Longrightarrow \quad \vec{a} = \vec{\mathbf{0}}
\end{aligned}
$$

Proof for Lemma 3.6

(continued...)

$$
\begin{aligned}
\text{“}\Rightarrow\text{”} \quad & \implies M = \max \vec{a} = \frac{M}{2} \\
& \implies M = 0 \\
& \because 0 \leq a_1, a_2, \cdots, a_N \leq M = 0 \\
& \therefore a_1 = a_2 = \cdots = a_N = 0 \\
& \implies \vec{a} = \vec{\mathbf{0}}
\end{aligned}
$$

“$\Leftarrow$” Suppose $\vec{a} = \vec{\mathbf{0}}$

Proof for Lemma 3.6

(continued...)

"$\Rightarrow$" $\implies M = \max \vec{a} = \dfrac{M}{2}$

$\implies M = 0$

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

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

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

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

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

Proof for Lemma 3.6

(continued...)

"$\Rightarrow$" $\Longrightarrow M = \max \vec{a} = \dfrac{M}{2}$

$\Longrightarrow M = 0$

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

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

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

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

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

$\Longrightarrow M = 0$

Proof for Lemma 3.6

(continued...)

"$\Rightarrow$" $\Longrightarrow\ M = \max \vec{a} = \dfrac{M}{2}$

$\Longrightarrow\ M = 0$

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

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

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

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

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

$\Longrightarrow\ M = 0$

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

Proof for Lemma 3.6

(continued...)

"$\Rightarrow$" $\implies M = \max \vec{a} = \dfrac{M}{2}$

$\implies M = 0$

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

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

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

"$\Leftarrow$" 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

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

□

Proof for Lemma 3.6

(continued...)

"$\Leftarrow$" $\Longrightarrow$ the period of $\vec{a}$ is $(1-0)=1$

Proof for Lemma 3.6

(continued...)

"$\Leftarrow$" $\Longrightarrow$ 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

$\square$

Proof for Lemma 3.7

Lemma 3.7

Proof.

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

Proof for Lemma 3.7

Lemma 3.7

Proof.

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

(a)

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

Proof for Lemma 3.7

Lemma 3.7

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

$\square$

Proof for Lemma 3.7

(continued...)

(b) Note that

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

and

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

□

Proof for Lemma 3.7

(continued...)

(b)

$$= (|a_2 - a_3|, \cdots, |a_N - a_1|, |a_1 - a_2|)$$

Proof for Lemma 3.7

(continued...)

(b)

$$= (|a_2 - a_3|, \cdots, |a_N - a_1|, |a_1 - a_2|)$$

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

Proof for Lemma 3.7

(continued...)

(b)

$$= (|a_2 - a_3|, \cdots, |a_N - a_1|, |a_1 - a_2|)$$

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

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

$\square$

Proof for Remark 3.8

Remark 3.8

Proof.

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

Proof for Remark 3.8

Remark 3.8

Proof.

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

$\implies 2y = 0$

Proof for Remark 3.8

Remark 3.8

Proof.

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

$$\implies 2y = 0$$

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

Proof for Remark 3.8

Remark 3.8

Proof.

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

$$\implies 2y = 0$$

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

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

Proof for Remark 3.8

Remark 3.8

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

Proof for Remark 3.9

Remark 3.9

Proof.

"$\Rightarrow$" It is trivial

"$\Leftarrow$" Suppose the condition holds

Proof for Remark 3.9

Remark 3.9

Proof.

"$\Rightarrow$" It is trivial

"$\Leftarrow$" Suppose the condition holds

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

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

Proof for Remark 3.9

Remark 3.9

Proof.

"$\Rightarrow$" It is trivial

"$\Leftarrow$" 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 $c = 0$:

Proof for Remark 3.9

Remark 3.9

Proof.

"$\Rightarrow$" It is trivial

"$\Leftarrow$" 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 $c = 0$:

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

Proof for Remark 3.9

Remark 3.9

Proof.

"$\Rightarrow$" It is trivial

"$\Leftarrow$" 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 $c = 0$:
$\Longrightarrow \mathscr{L}(c\vec{x} + \vec{y}) = \mathscr{L}(\vec{\mathbf{0}} + \vec{y}) = \mathscr{L}(\vec{y})$ and
$c\mathscr{L}(\vec{x}) + \mathscr{L}(\vec{y}) = \vec{\mathbf{0}} + \mathscr{L}(\vec{y}) = \mathscr{L}(\vec{y})$

Proof for Remark 3.9

Remark 3.9

Proof.

"$\Rightarrow$" It is trivial

"$\Leftarrow$" 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 $c = 0$:

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

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

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

$\square$

Proof for Lemma 3.10

Lemma 3.10

Proof.

We prove it by induction on i:

$i = 0$:

Proof for Lemma 3.10

Lemma 3.10

Proof.

We prove it by induction on i:

$i = 0$:

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

Proof for Lemma 3.10

Lemma 3.10

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, $i = K + 1$:

Proof for Lemma 3.10

Lemma 3.10

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:

Proof for Lemma 3.10

Lemma 3.10

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:

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

Proof for Lemma 3.10

Lemma 3.10

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

Proof for Lemma 3.10

(continued...)

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

By induction, we complete this proof $\square$

Proof for Lemma 3.11

Lemma 3.11

Proof.

We prove it by induction on i:

$i = 0$:

Proof for Lemma 3.11

Lemma 3.11

Proof.

We prove it by induction on i:

$i = 0$:

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

Proof for Lemma 3.11

Lemma 3.11

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, $i = K + 1$:

Proof for Lemma 3.11

Lemma 3.11

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:

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

Proof for Lemma 3.11

Lemma 3.11

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

Proof for Lemma 3.11

(continued...)

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

□

Proof for Lemma 3.11

(continued...)

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

By induction, we complete this proof $\square$

Proof for Lemma 3.12

Lemma 3.12

Proof.

We prove it by induction on i:

Proof for Lemma 3.12

Lemma 3.12

Proof.

We prove it by induction on i:

$i = 0$: It is trivial

Proof for Lemma 3.12

Lemma 3.12

Proof.

We prove it by induction on i:

$i = 0$: It is trivial

Suppose $i = K$ holds

Then, $i = K + 1$:

Proof for Lemma 3.12

Lemma 3.12

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 □

Proof for Theorem 3.13

Theorem 3.13

Proof.

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

Proof for Theorem 3.13

Theorem 3.13

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 $1 \leq i \leq N$

Proof for Theorem 3.13

Theorem 3.13

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 $2 \leq i \leq N$

Proof for Theorem 3.13

Theorem 3.13

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 $\vec{e}_i = T^{N-i+1}(\vec{e}_1)$ □

□

Proof for Theorem 3.13

(continued...)

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

(continued...)

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

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

□

Proof for Theorem 3.13

(continued...)

(a) Given $\vec{b} \in (\mathbb{Z}_2)^N$
Finally, we must show that $D^r(\vec{b}) = D^s(\vec{b})$:

Proof for Theorem 3.13

(continued...)

(a) 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 $\mathbb{Z}_2$

Proof for Theorem 3.13

(continued...)

(a) 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

$$\vec{b} = c_1\vec{e}_1 + c_2\vec{e}_2 + \cdots + c_N\vec{e}_N$$

Then, we have:

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

$\square$

Proof for Theorem 3.13

(continued...)

(a)

$$= c_1 D^r(\vec{e}_1) + c_2 D^r(\vec{e}_2) + \cdots + c_N D^r(\vec{e}_N)$$
$$= c_1 D^s(\vec{e}_1) + c_2 D^s(\vec{e}_2) + \cdots + c_N D^s(\vec{e}_N),$$

by **Claim**

$$= c_1 \mathscr{D}^s(\vec{e}_1) + c_2 \mathscr{D}^s(\vec{e}_2) + \cdots + c_N \mathscr{D}^s(\vec{e}_N)$$
$$= \mathscr{D}^s(c_1\vec{e}_1 + c_2\vec{e}_2 + \cdots + c_N\vec{e}_N),$$ by Lemma 3.11
$$= \mathscr{D}^s(\vec{b})$$
$$= D^s(\vec{b})$$

□

Proof for Theorem 3.13

(continued...)

(b) Given $i \in \mathbb{N}$ with $2 \leq i \leq N$
It suffices to show that the period of $\vec{e}_i$ is equal to the period of $\vec{e}_1$:

Proof for Theorem 3.13

(continued...)

(b) Given $i \in \mathbb{N}$ with $2 \leq i \leq N$
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 $\vec{e}_1 = n - k$

Proof for Theorem 3.13

(continued...)

(b) Given $i \in \mathbb{N}$ with $2 \leq i \leq N$
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 $\vec{e}_1 = n - k$
$\implies D^0(\vec{e}_1) = \vec{e}_1, D(\vec{e}_1), D^2(\vec{e}_1), \cdots, D^{n-1}(\vec{e}_1)$ are all distinct

Proof for Theorem 3.13

(continued...)

(b) Given $i \in \mathbb{N}$ with $2 \leq i \leq N$
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 $\vec{e}_1 = n - k$
$\implies D^0(\vec{e}_1) = \vec{e}_1, D(\vec{e}_1), D^2(\vec{e}_1), \cdots, D^{n-1}(\vec{e}_1)$ are all distinct and $D^n(\vec{e}_1) = D^k(\vec{e}_1)$

Proof for Theorem 3.13

(continued...)

(b) Given $i \in \mathbb{N}$ with $2 \leq i \leq N$
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 $\vec{e}_1 = n - k$
$\implies D^0(\vec{e}_1) = \vec{e}_1, D(\vec{e}_1), D^2(\vec{e}_1), \cdots, D^{n-1}(\vec{e}_1)$ are all distinct and $D^n(\vec{e}_1) = D^k(\vec{e}_1)$
By **(a)**, we know that $D^n(\vec{e}_i) = D^k(\vec{e}_i)$ $(*)$
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

$\square$

Proof for Theorem 3.13

(continued...)

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

Proof.

If not, suppose $\exists\, a, b \in \mathbb{Z}$ with $0 \leq a < b \leq n-1$ such that
$D^a(\vec{e}_i) = D^b(\vec{e}_i)$
$\implies T^{i-1}(D^a(\vec{e}_i)) = T^{i-1}(D^b(\vec{e}_i))$
$\implies D^a(T^{i-1}(\vec{e}_i)) = D^b(T^{i-1}(\vec{e}_i))$, by Lemma 3.7(b)
$\implies D^a(\vec{e}_1) = D^b(\vec{e}_1)$ 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 □

□

Proof for Theorem 3.13

(continued...)

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

Proof for Theorem 3.13

(continued...)

(b) By **Claim** and $(*)$, the period of $\vec{e}_i$ is equal to $n-k$
$\implies$ the period of $\vec{e}_i$ is equal to the period of $\vec{e}_1$

Proof for Theorem 3.13

(continued...)

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

Proof for Theorem 3.13

(continued...)

(b) 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

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

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

□

Proof for Theorem 3.13

(continued...)

(c) 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 $\vec{a}$

Proof for Theorem 3.13

(continued...)

(c) 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 $\vec{b}$

Proof for Theorem 3.13

(continued...)

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

Proof for Theorem 3.13

(continued...)

(c) 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 $\vec{b}$
$\implies D^n(\vec{b}) = D^k(\vec{b})$
Moreover, the period of $\vec{e}_1$ is $n' - k'$

Proof for Theorem 3.13

(continued...)

(c) 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 $\vec{b}$

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

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

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

Proof for Theorem 3.13

(continued...)

(c) 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 $\vec{b}$
$\implies D^n(\vec{b}) = D^k(\vec{b})$
Moreover, the period of $\vec{e}_1$ is $n' - k'$
$\implies D^{n'}(\vec{e}_1) = D^{k'}(\vec{e}_1)$
By **(a)**, we obtain $D^{n'}(\vec{b}) = D^{k'}(\vec{b})$

Proof for Theorem 3.13

(continued...)

(c) 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 $\vec{b}$
$\implies D^n(\vec{b}) = D^k(\vec{b})$
Moreover, the period of $\vec{e}_1$ is $n' - k'$
$\implies D^{n'}(\vec{e}_1) = D^{k'}(\vec{e}_1)$
By **(a)**, we obtain $D^{n'}(\vec{b}) = D^{k'}(\vec{b})$
Take $\vec{\boldsymbol{b}} = D^{k+k'}(\vec{b})$

Proof for Theorem 3.13

(continued...)

(c) 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 $\vec{b}$

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

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

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

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 $D^{n'-k'}(\vec{\boldsymbol{b}}) = \vec{\boldsymbol{b}}$

$\implies$

$$\vec{\boldsymbol{b}} = D^{n'-k'}(\vec{\boldsymbol{b}}) = D^{(n-k)q+r}(\vec{\boldsymbol{b}}) = D^r(D^{(n-k)q}(\vec{\boldsymbol{b}}))$$

$$= D^r(\vec{\boldsymbol{b}}), \text{ by Lemma 3.12}$$

$\square$

Proof for Theorem 3.13

(continued...)

(c) $\implies D^{k+k'}(\vec{b}) = D^{k+k'+r}(\vec{b})$

Proof for Theorem 3.13

(continued...)

(c) $\implies D^{k+k'}(\vec{b}) = D^{k+k'+r}(\vec{b})$

Write $k' = (n-k)q_0 + r_0$, where q_0, r_0 are nonnegative integers with $0 \leq r_0 < n-k$

$\implies$

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

and

$\square$

Proof for Theorem 3.13

(continued...)

(c)

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

Proof for Theorem 3.13

(continued...)

(c)

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

Then, we have:

$$\begin{aligned} D^{k+r_0+r}(\vec{b}) &= D^{k+k'+r}(\vec{b}) \\ &= D^{k+k'}(\vec{b}) \\ &= D^{k+r_0}(\vec{b}) \end{aligned} \qquad (*')$$

$\square$

Proof for Theorem 3.13

(continued...)

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

Proof for Theorem 3.13

(continued...)

(c) 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

Proof for Theorem 3.13

(continued...)

(c) Note that $k + r_0 \leq k + r_0 + r < k + r_0 + (n-k) = n + r_0$
$\implies k + r_0 \leq k + r_0 + r \leq (n-1) + r_0$, 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

Proof for Theorem 3.13

(continued...)

(c) Note that $k + r_0 \le k + r_0 + r < k + r_0 + (n-k) = n + r_0$
$\implies k + r_0 \le k + r_0 + r \le (n-1) + r_0$, 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 $n-k$

Proof for Theorem 3.13

(continued...)

(c) Note that $k + r_0 \leq k + r_0 + r < k + r_0 + (n - k) = n + r_0$ $\implies k + r_0 \leq k + r_0 + r \leq (n-1) + r_0$, 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 $n - k$
Then, we have:
$D^{k+r_0}(\vec{b}), D^{k+r_0+1}(\vec{b}), \cdots, D^{k+r_0+r}(\vec{b}), \cdots, D^{(n-1)+r_0}(\vec{b})$ are all distinct

Proof for Theorem 3.13

(continued...)

(c) Note that $k + r_0 \le k + r_0 + r < k + r_0 + (n - k) = n + r_0$
$\implies k + r_0 \le k + r_0 + r \le (n-1) + r_0$, 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 $n - k$
Then, we have:
$D^{k+r_0}(\vec{b}), D^{k+r_0+1}(\vec{b}), \cdots, D^{k+r_0+r}(\vec{b}), \cdots, D^{(n-1)+r_0}(\vec{b})$
are all distinct
By $(*')$, we conclude that $k + r_0 = k + r_0 + r$

Proof for Theorem 3.13

(continued...)

(c) Note that $k + r_0 \leq k + r_0 + r < k + r_0 + (n - k) = n + r_0$
$\implies k + r_0 \leq k + r_0 + r \leq (n - 1) + r_0$, 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 $n - k$
Then, we have:
$D^{k+r_0}(\vec{b}), D^{k+r_0+1}(\vec{b}), \cdots, D^{k+r_0+r}(\vec{b}), \cdots, D^{(n-1)+r_0}(\vec{b})$
are all distinct
By $(*')$, we conclude that $k + r_0 = k + r_0 + r$
$\implies r = 0$
Hence, we complete this proof

$\square$

Proof for Lemma 3.14

Lemma 3.14

Proof.

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

Proof for Lemma 3.14

Lemma 3.14

Proof.

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

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

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

□

Proof for Lemma 3.14

(continued...)

(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:

Proof for Lemma 3.14

(continued...)

(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

Proof for Lemma 3.14

(continued...)

(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, $r = K + 1$:

Proof for Lemma 3.14

(continued...)

(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, $r = K + 1$:

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

□

□

Proof for Lemma 3.14

(continued...)

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

(continued...)

$$= \mathscr{I}^2 + \mathscr{I}\mathscr{T}^{2^K} + \mathscr{T}^{2^K}\mathscr{I} + (\mathscr{T}^{2^K})^2$$
$$= \mathscr{I} + \mathscr{T}^{2^K} + \mathscr{T}^{2^K} + \mathscr{T}^{2^{K+1}}$$
$$= \mathscr{I} + \mathscr{T}^{2^{K+1}}, \text{ since } \mathscr{T}(\mathbb{Z}_2) \subseteq \mathbb{Z}_2$$

So, $r = K + 1$ holds □

Proof for Lemma 3.14

(continued...)

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

(continued...)

$$= \mathscr{I}^2 + \mathscr{I}\mathscr{T}^{2^K} + \mathscr{T}^{2^K}\mathscr{I} + (\mathscr{T}^{2^K})^2$$
$$= \mathscr{I} + \mathscr{T}^{2^K} + \mathscr{T}^{2^K} + \mathscr{T}^{2^{K+1}}$$
$$= \mathscr{I} + \mathscr{T}^{2^{K+1}}, \text{ since } \mathscr{T}(\mathbb{Z}_2) \subseteq \mathbb{Z}_2$$

So, $r = K + 1$ holds $\square$

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

Proof for Lemma 3.14

(continued...)

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

(continued...)

$$= \mathscr{I}^2 + \mathscr{I}\mathscr{T}^{2^K} + \mathscr{T}^{2^K}\mathscr{I} + (\mathscr{T}^{2^K})^2$$
$$= \mathscr{I} + \mathscr{T}^{2^K} + \mathscr{T}^{2^K} + \mathscr{T}^{2^{K+1}}$$
$$= \mathscr{I} + \mathscr{T}^{2^{K+1}}, \text{ since } \mathscr{T}(\mathbb{Z}_2) \subseteq \mathbb{Z}_2$$

So, $r = K + 1$ holds $\square$

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

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

Proof for Lemma 3.14

(continued...)

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

(continued...)

$$= \mathscr{I}^2 + \mathscr{I}\mathscr{T}^{2^K} + \mathscr{T}^{2^K}\mathscr{I} + (\mathscr{T}^{2^K})^2$$
$$= \mathscr{I} + \mathscr{T}^{2^K} + \mathscr{T}^{2^K} + \mathscr{T}^{2^{K+1}}$$
$$= \mathscr{I} + \mathscr{T}^{2^{K+1}}, \text{ since } \mathscr{T}(\mathbb{Z}_2) \subseteq \mathbb{Z}_2$$

So, $r = K + 1$ holds $\square$

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 $\square$

Proof for Theorem 3.15

Theorem 3.15

Proof.

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

Proof for Theorem 3.15

Theorem 3.15

Proof.

By Lemma 2.1, we may assume that the period of $\vec{a}$ is $n-k$
Note that $2^r \equiv 0 \pmod{N}$

Proof for Theorem 3.15

Theorem 3.15

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 $\vec{a}$

Proof for Theorem 3.15

Theorem 3.15

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 $\vec{b}$

Proof for Theorem 3.15

Theorem 3.15

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 $k \leq s \leq n-1$
$\because$

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

$\square$

Proof for Theorem 3.15

(continued...)

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

Proof for Theorem 3.15

(continued...)

$$= \mathscr{I} + \mathscr{I}(\vec{b})$$
$$= \mathscr{I}(\vec{b}) + \mathscr{I}(\vec{b})$$
$$= \vec{\mathbf{0}}, \text{ since } \mathscr{I}(\vec{b}) \in (\mathbb{Z}_2)^6$$

$\therefore$

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

$\square$

Proof for Theorem 3.15

(continued...)

$$
\begin{aligned}
&= m\vec{\mathbf{0}} \\
&= \vec{\mathbf{0}}
\end{aligned}
$$

Proof for Theorem 3.15

(continued...)

$$= m\vec{\mathbf{0}}$$
$$= \vec{\mathbf{0}}$$

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

Proof for Theorem 3.15

(continued...)

$$= m\vec{\mathbf{0}}$$
$$= \vec{\mathbf{0}}$$

On the other hand, we know that
$D(\vec{\mathbf{0}}) = D(0, 0, \cdots, 0) = (0, 0, \cdots, 0) = \vec{\mathbf{0}} = D^0(\vec{\mathbf{0}})$
$\Longrightarrow$ the period of $\vec{\mathbf{0}}$ is $1 - 0 = 1$ and the 1-cycle of $\vec{\mathbf{0}}$ is $\vec{\mathbf{0}}$

Proof for Theorem 3.15

(continued...)

$$= m\vec{\mathbf{0}}$$
$$= \vec{\mathbf{0}}$$

On the other hand, we know that
$D(\vec{\mathbf{0}}) = D(0, 0, \cdots, 0) = (0, 0, \cdots, 0) = \vec{\mathbf{0}} = D^0(\vec{\mathbf{0}})$
$\implies$ 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 $\vec{\mathbf{0}}$ $\square$

Proof for Theorem 4.1

Theorem 4.1

Proof.

Given $\vec{a} \in A_6$

Proof for Theorem 4.1

Theorem 4.1

Proof.

Given $\vec{a} \in A_6$

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

Proof for Theorem 4.1

Theorem 4.1

Proof.

Given $\vec{a} \in A_6$

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

$\Longrightarrow$

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

$\square$

Proof for Theorem 4.1

(continued...)

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

Proof for Theorem 4.1

(continued...)

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

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

Proof for Theorem 4.1

(continued...)

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

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

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 $\square$

Proof for Lemma 4.2

Lemma 4.2

Proof.

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

Proof for Lemma 4.2

Lemma 4.2

Proof.

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

$$\mathbf{(0,0,0,0,0,0)}$$

$\rightarrow$: a Ducci process

$\square$

Proof for Lemma 4.2

Lemma 4.2

Proof.

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

$$
\begin{array}{ccc}
(0,1,0,1,0,1) & & (1,0,1,0,1,0) \\
\searrow & & \swarrow \\
& (1,1,1,1,1,1) & \\
& \downarrow & \\
& \mathbf{(0,0,0,0,0,0)} & \\
& \circlearrowleft &
\end{array}
$$

$\rightarrow$: a Ducci process

$\square$

Proof for Lemma 4.2

(continued...)

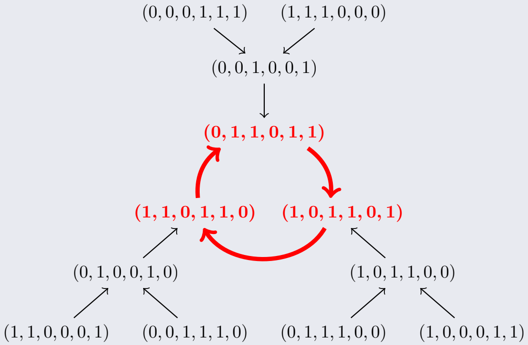
$$\begin{tikzcd} & (0,1,1,0,1,1) \arrow[dr, bend left] & \\ (1,1,0,1,1,0) \arrow[ur, bend left] & & (1,0,1,1,0,1) \arrow[ll, bend left] \end{tikzcd}$$

$\rightarrow$: a Ducci process

$\square$

Proof for Lemma 4.2

(continued...)



$\longrightarrow$: a Ducci process

$\square$

Proof for Lemma 4.2

(continued...)

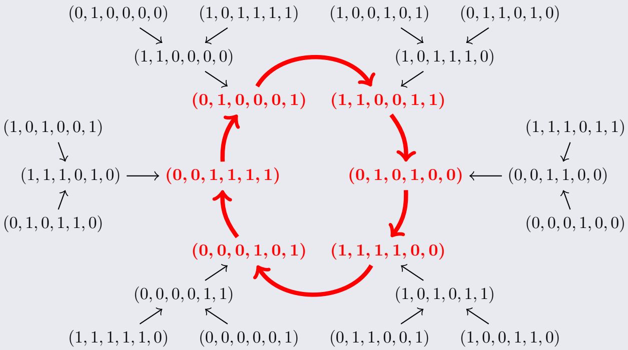
$$
\begin{tikzcd}
(0,1,0,0,0,1) \arrow[r, bend left] & (1,1,0,0,1,1) \arrow[d, bend left] \\
(0,0,1,1,1,1) \arrow[u, bend left] & (0,1,0,1,0,0) \arrow[d, bend left] \\
(0,0,0,1,0,1) \arrow[u, bend left] & (1,1,1,1,0,0) \arrow[l, bend left]
\end{tikzcd}
$$

$\rightarrow$: a Ducci process

$\square$

Proof for Lemma 4.2

(continued...)



$\longrightarrow$: a Ducci process

Proof for Lemma 4.2

(continued...)

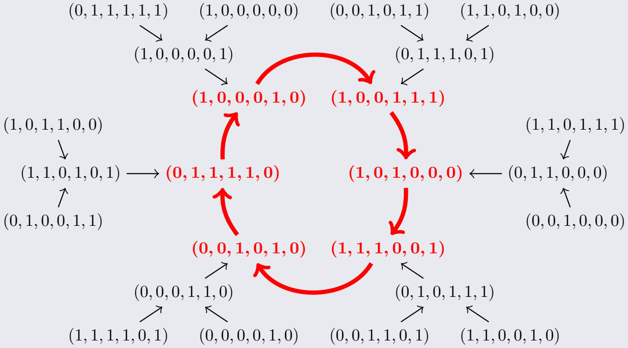
$$
\begin{tikzcd}
 & (1,0,0,0,1,0) \arrow[r, bend left] & (1,0,0,1,1,1) \arrow[dr] & \\
(0,1,1,1,1,0) \arrow[ur] & & & (1,0,1,0,0,0) \arrow[dl] \\
 & (0,0,1,0,1,0) \arrow[ul] & (1,1,1,0,0,1) \arrow[l, bend left] &
\end{tikzcd}
$$

$\rightarrow$: a Ducci process

$\square$

Proof for Lemma 4.2

(continued...)



$\longrightarrow$: a Ducci process

$\square$

Proof for Theorem 4.3

Theorem 4.3

Proof.

It follows from Theorem 3.2 and Lemma 4.2. □

Proof for Lemma 4.4

Lemma 4.4

Proof.

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

Proof for Lemma 4.4

Lemma 4.4

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 for Lemma 4.4

Lemma 4.4

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

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

□

□

Proof for Lemma 4.4

(continued...)

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 for Lemma 4.4

(continued...)

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

Proof for Lemma 4.4

(continued...)

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

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

Proof for Lemma 4.4

(continued...)

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

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

and

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

Proof for Lemma 4.4

(continued...)

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

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

and

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

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

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

Proof for Remark 4.7

Remark 4.7

Proof.

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

Proof for Remark 4.7

Remark 4.7

Proof.

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

Proof for Remark 4.7

Remark 4.7

Proof.

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

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

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

Proof for Lemma 4.8

Lemma 4.8

Proof.

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

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

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

Proof for Lemma 4.8

Lemma 4.8

Proof.

Write $\vec{a^c} = (b_1, b_2, \cdots, b_6)$
$\implies b_i = 1 - a_i, \forall\, i = 1, 2, \cdots, 6$
Given $\pi \in \mathcal{D}_6$
Note that

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

Proof for Lemma 4.8

Lemma 4.8

Proof.

Write $\vec{a^c} = (b_1, b_2, \cdots, b_6)$
$\implies b_i = 1 - a_i, \forall\, i = 1, 2, \cdots, 6$
Given $\pi \in \mathcal{D}_6$
Note that

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

and

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

Proof for Lemma 4.8

Lemma 4.8

Proof.

Write $\vec{a^c} = (b_1, b_2, \cdots, b_6)$
$\implies b_i = 1 - a_i, \forall\, i = 1, 2, \cdots, 6$
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

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

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

Proof for Lemma 4.9

Lemma 4.9

Proof.

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

Proof for Lemma 4.9

Lemma 4.9

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:

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

$\square$

Proof for Lemma 4.9

(continued...)

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

Proof for Lemma 4.9

(continued...)

Finally, we enumerate 13 equivalence classes of $(\mathbb{Z}_2)^6$:
By Lemma 4.8, it is reduced to write out $[(0,0,0,0,0,0)]$, $[(1,0,0,0,0,0)]$, $[(0,0,1,0,0,1)]$, $[(1,0,0,0,0,1)]$, $[(1,0,0,0,1,0)]$, $[(0,0,0,1,1,1)]$, $[(0,0,1,0,1,1)]$, $[(0,1,0,1,0,1)]$:

Proof for Lemma 4.9

(continued...)

Finally, we enumerate 13 equivalence classes of $(\mathbb{Z}_2)^6$:
By Lemma 4.8, it is reduced to write out $[(0,0,0,0,0,0)]$, $[(1,0,0,0,0,0)], [(0,0,1,0,0,1)], [(1,0,0,0,0,1)], [(1,0,0,0,1,0)]$, $[(0,0,0,1,1,1)], [(0,0,1,0,1,1)], [(0,1,0,1,0,1)]$:
$[(0,0,0,0,0,0)] = \{(0,0,0,0,0,0)\}$

Proof for Lemma 4.9

(continued...)

Finally, we enumerate 13 equivalence classes of $(\mathbb{Z}_2)^6$:
By Lemma 4.8, it is reduced to write out $[(0,0,0,0,0,0)]$, $[(1,0,0,0,0,0)], [(0,0,1,0,0,1)], [(1,0,0,0,0,1)], [(1,0,0,0,1,0)]$, $[(0,0,0,1,1,1)], [(0,0,1,0,1,1)], [(0,1,0,1,0,1)]$:
$[(0,0,0,0,0,0)] = \{(0,0,0,0,0,0)\}$
$[(1,0,0,0,0,0)] = \{(1,0,0,0,0,0), (0,1,0,0,0,0)$, $(0,0,1,0,0,0), (0,0,0,1,0,0), (0,0,0,0,1,0), (0,0,0,0,0,1)\}$

Proof for Lemma 4.9

(continued...)

Finally, we enumerate 13 equivalence classes of $(\mathbb{Z}_2)^6$:
By Lemma 4.8, it is reduced to write out $[(0,0,0,0,0,0)]$, $[(1,0,0,0,0,0)], [(0,0,1,0,0,1)], [(1,0,0,0,0,1)], [(1,0,0,0,1,0)]$, $[(0,0,0,1,1,1)], [(0,0,1,0,1,1)], [(0,1,0,1,0,1)]$:

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

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

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

Proof for Lemma 4.9

(continued...)

Finally, we enumerate 13 equivalence classes of $(\mathbb{Z}_2)^6$:
By Lemma 4.8, it is reduced to write out $[(0,0,0,0,0,0)]$, $[(1,0,0,0,0,0)], [(0,0,1,0,0,1)], [(1,0,0,0,0,1)], [(1,0,0,0,1,0)]$, $[(0,0,0,1,1,1)], [(0,0,1,0,1,1)], [(0,1,0,1,0,1)]$:

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

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

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

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

Proof for Lemma 4.9

(continued...)

Finally, we enumerate 13 equivalence classes of $(\mathbb{Z}_2)^6$:
By Lemma 4.8, it is reduced to write out $[(0,0,0,0,0,0)]$, $[(1,0,0,0,0,0)], [(0,0,1,0,0,1)], [(1,0,0,0,0,1)], [(1,0,0,0,1,0)]$, $[(0,0,0,1,1,1)], [(0,0,1,0,1,1)], [(0,1,0,1,0,1)]$:

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

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

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

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

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

Proof for Lemma 4.9

(continued..)

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

Proof for Lemma 4.9

(continued..)

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

Proof for Lemma 4.9

(continued..)

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

Proof for Theorem 4.10

Theorem 4.10

Proof.

$$\mathbf{(0,0,0,0,0,0)} \circlearrowleft$$

$\rightarrow$: a Ducci process

$\square$

Proof for Theorem 4.10

Theorem 4.10

Proof.

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

$\longrightarrow$: a Ducci process

$\square$

Proof for Theorem 4.10

Theorem 4.10

continued...

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

$$\circlearrowleft$$

$\rightarrow$: a Ducci process

$\square$

Proof for Theorem 4.10

Theorem 4.10

continued...

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

$\longrightarrow$: a Ducci process

$\square$

Proof for Theorem 4.10

Theorem 4.10

continued...

$$\begin{tikzcd}[column sep=large] \mathbf{(1,0,0,0,1,0)} \arrow[r, bend left] & \mathbf{(1,0,0,1,1,1)} \arrow[l, bend left] \end{tikzcd}$$

$\rightarrow$: a Ducci process

$\square$

Proof for Theorem 4.10

Theorem 4.10

continued...

$$
\begin{tikzcd}
(0,1,1,1,1,1) \arrow[dr] & & (1,0,0,0,0,0) \arrow[dl] & & & & (0,1,1,1,0,1) \arrow[dl] \\
& (0,1,1,1,0,1) \arrow[dr] & & & & (0,1,1,1,0,1) \arrow[dl] & \\
& & \color{red}{\mathbf{(1,0,0,0,1,0)}} \arrow[rr, bend left, red] & & \color{red}{\mathbf{(1,0,0,1,1,1)}} \arrow[ll, bend left, red] & &
\end{tikzcd}
$$

$\rightarrow$: a Ducci process

$\square$

Proof for Corollary 4.11

Corollary 4.11

Proof.

It follows from Theorem 3.2 and Theorem 4.10. $\square$

Proof for Theorem 4.12

Theorem 4.12

Proof.

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

Proof for Theorem 4.12

Theorem 4.12

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 $\vec{e}_1$

Proof for Theorem 4.12

Theorem 4.12

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

Proof for Theorem 4.12

Theorem 4.12

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

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

□

Proof for Theorem 4.12

(continued...)

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

Proof for Theorem 4.12

(continued...)

"$\Leftarrow$" By Remark 4.5(a) and Lemma 4.9, we know that $\vec{e}_1, D(\vec{e}_1), D^2(\vec{e}_1), D^3(\vec{e}_1)$ are all distinct
$\therefore$ the period of $\vec{e}_1$ is $(4-2)=2$

Proof for Theorem 4.12

(continued...)

"$\Leftarrow$" By Remark 4.5(a) and Lemma 4.9, we know that $\vec{e}_1, D(\vec{e}_1), D^2(\vec{e}_1), D^3(\vec{e}_1)$ 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: $r = 1$

Proof for Theorem 4.12

(continued...)

"$\Leftarrow$" By Remark 4.5(a) and Lemma 4.9, we know that $\vec{e}_1, D(\vec{e}_1), D^2(\vec{e}_1), D^3(\vec{e}_1)$ 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

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

Proof for Theorem 4.12

(continued...)

"$\Leftarrow$" By Remark 4.5(a) and Lemma 4.9, we know that
$\vec{e}_1, D(\vec{e}_1), D^2(\vec{e}_1), D^3(\vec{e}_1)$ 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

Proof for Theorem 4.12

(continued...)

"$\Leftarrow$" By Remark 4.5(a) and Lemma 4.9, we know that
$\vec{e}_1, D(\vec{e}_1), D^2(\vec{e}_1), D^3(\vec{e}_1)$ 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

$\square$

Proof for Theorem 4.2

(continued...)

"$\Leftarrow$" Case 2: $r = 2$

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

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

Proof for Theorem 4.2

(continued...)

"$\Leftarrow$" Case 2: $r = 2$

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

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

$\square$

Prepare for Lemma 2.6

Remark (2.4)

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

Proof

Prepare for Theorem 2.12

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

Prepare for Theorem 2.12

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

Prepare for Theorem 2.12

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

A remark about Lemma 2.8

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.

Prepare for Theorem 2.12

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 $\vec{a}$.

Prepare for Theorem 2.12

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

Prepare for Theorem 2.12

Remark (2.11)

In Lemma 2.10, we observe that:

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

Prepare for Theorem 2.12

Remark (2.11)

In Lemma 2.10, we observe that:

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

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

Proof

A property about the greatest common divisor of $\vec{a}$ in A_N

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 $\gcd D^r(\vec{a}) \mid \gcd D^s(\vec{a})$.

A property about the greatest common divisor of $\vec{a}$ in A_N

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

A property about the greatest common divisor of $\vec{a}$ in A_N

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

Example

$$\begin{aligned} \vec{a} &= (3,3,3,3,3,9) & \gcd \vec{a} &= 3 \\ D(\vec{a}) &= (0,0,0,0,6,6) & \gcd D(\vec{a}) &= 6 \\ D^2(\vec{a}) &= (0,0,0,6,0,6) & \gcd D^2(\vec{a}) &= 6 \\ D^3(\vec{a}) &= (0,0,6,6,6,6) & \gcd D^3(\vec{a}) &= 6 \\ &\vdots & &\vdots \end{aligned}$$

The greatest common divisor of $\vec{a}$ in the cycle of $\vec{a}$

Lemma (2.19)

Let $\vec{a} \in A_N$ *with* $\vec{a} \neq \vec{\mathbf{0}}$.

The greatest common divisor of $\vec{a}$ in the cycle of $\vec{a}$

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 $\vec{a}$.

The greatest common divisor of $\vec{a}$ in the cycle of $\vec{a}$

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

The greatest common divisor of $\vec{a}$ in the cycle of $\vec{a}$

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

Example

$$\vec{a} = (0,1,2,2,1,0) \qquad D^3(\vec{a}) = (1,0,1,1,0,1)$$

$$D(\vec{a}) = (1,1,0,1,1,0) \qquad D^4(\vec{a}) = (1,1,0,1,1,0)$$

$$D^2(\vec{a}) = (0,1,1,0,1,1) \qquad = D(\vec{a})$$

The converse of Lemma 2.6 and Lemma 2.19 may not be true even if put them together

Example (2.20)

$$\vec{e}_1 = (1,0,0,0,0,0) \in A_6$$
$$D(\vec{e}_1) = (1,0,0,0,0,1)$$
$$D^2(\vec{e}_1) = (1,0,0,0,1,0)$$
$$D^3(\vec{e}_1) = (1,0,0,1,1,1)$$
$$D^4(\vec{e}_1) = (1,0,1,0,0,0)$$
$$D^5(\vec{e}_1) = (1,1,1,0,0,1)$$
$$D^6(\vec{e}_1) = (0,0,1,0,1,0)$$
$$D^7(\vec{e}_1) = (0,1,1,1,1,0)$$
$$D^8(\vec{e}_1) = (1,0,0,0,1,0) = D^2(\vec{e}_1)$$

The converse of Lemma 2.6 and Lemma 2.19 may not be true even if put them together

Example (2.20)

$$\vec{e}_1 = (1,0,0,0,0,0) \in A_6$$
$$D(\vec{e}_1) = (1,0,0,0,0,1)$$
$$D^2(\vec{e}_1) = (1,0,0,0,1,0)$$
$$D^3(\vec{e}_1) = (1,0,0,1,1,1)$$
$$D^4(\vec{e}_1) = (1,0,1,0,0,0)$$
$$D^5(\vec{e}_1) = (1,1,1,0,0,1)$$
$$D^6(\vec{e}_1) = (0,0,1,0,1,0)$$
$$D^7(\vec{e}_1) = (0,1,1,1,1,0)$$
$$D^8(\vec{e}_1) = (1,0,0,0,1,0) = D^2(\vec{e}_1)$$

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

The converse of Lemma 2.6 and Lemma 2.19 may not be true even if put them together

Example (2.20)

$$\vec{e}_1 = (1,0,0,0,0,0) \in A_6$$
$$D(\vec{e}_1) = (1,0,0,0,0,1)$$
$$D^2(\vec{e}_1) = (1,0,0,0,1,0)$$
$$D^3(\vec{e}_1) = (1,0,0,1,1,1)$$
$$D^4(\vec{e}_1) = (1,0,1,0,0,0)$$
$$D^5(\vec{e}_1) = (1,1,1,0,0,1)$$
$$D^6(\vec{e}_1) = (0,0,1,0,1,0)$$
$$D^7(\vec{e}_1) = (0,1,1,1,1,0)$$
$$D^8(\vec{e}_1) = (1,0,0,0,1,0) = D^2(\vec{e}_1)$$

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

The converse of Lemma 2.6 and Lemma 2.19 may not be true even if put them together

Example (2.20)

$$\vec{e}_1 = (1,0,0,0,0,0) \in A_6$$
$$D(\vec{e}_1) = (1,0,0,0,0,1)$$
$$D^2(\vec{e}_1) = (1,0,0,0,1,0)$$
$$D^3(\vec{e}_1) = (1,0,0,1,1,1)$$
$$D^4(\vec{e}_1) = (1,0,1,0,0,0)$$
$$D^5(\vec{e}_1) = (1,1,1,0,0,1)$$
$$D^6(\vec{e}_1) = (0,0,1,0,1,0)$$
$$D^7(\vec{e}_1) = (0,1,1,1,1,0)$$
$$D^8(\vec{e}_1) = (1,0,0,0,1,0) = D^2(\vec{e}_1)$$

$\Longrightarrow$ 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 $i = 0, 1, \cdots, 7$

The converse of Lemma 2.6 and Lemma 2.19 may not be true even if put them together

Example (2.20)

$$\begin{aligned}
\vec{e}_1 &= (1,0,0,0,0,0) \in A_6 \\
D(\vec{e}_1) &= (1,0,0,0,0,1) \\
D^2(\vec{e}_1) &= (1,0,0,0,1,0) \\
D^3(\vec{e}_1) &= (1,0,0,1,1,1) \\
D^4(\vec{e}_1) &= (1,0,1,0,0,0)
\end{aligned}
\qquad
\begin{aligned}
D^5(\vec{e}_1) &= (1,1,1,0,0,1) \\
D^6(\vec{e}_1) &= (0,0,1,0,1,0) \\
D^7(\vec{e}_1) &= (0,1,1,1,1,0) \\
D^8(\vec{e}_1) &= (1,0,0,0,1,0) \\
&= D^2(\vec{e}_1)
\end{aligned}$$

$\Longrightarrow$ 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 $\vec{e}_1$

A property about the complement of N-tuples in A_N

Lemma (3.4)

Let $\vec{a} = (a_1, a_2, \cdots, a_N) \in A_N$ *and* $\max \vec{a} = M$. *Suppose the cycle of* $\vec{a}$ *is similar to the cycle of* $\vec{b}$, *where* $\vec{b} \in (\mathbb{Z}_2)^6$ *and the period of* $\vec{b}$ *is equal to the period of* $\vec{a}$.

A property about the complement of N-tuples in A_N

Lemma (3.4)

Let $\vec{a} = (a_1, a_2, \cdots, a_N) \in A_N$ and $\max \vec{a} = M$. Suppose the cycle of $\vec{a}$ is similar to the cycle of $\vec{b}$, where $\vec{b} \in (\mathbb{Z}_2)^6$ 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

A property about the complement of N-tuples in A_N

Lemma (3.4)

Let $\vec{a} = (a_1, a_2, \cdots, a_N) \in A_N$ and $\max \vec{a} = M$. Suppose the cycle of $\vec{a}$ is similar to the cycle of $\vec{b}$, where $\vec{b} \in (\mathbb{Z}_2)^6$ 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

Example

$$\vec{a} = (0, 2, 4, 4, 2, 0) \qquad \vec{a^c} = (4, 2, 0, 0, 2, 4)$$

$$D(\vec{a}) = (2, 2, 0, 2, 2, 0) \qquad D(\vec{a^c}) = (2, 2, 0, 2, 2, 0)$$

$$D^2(\vec{a}) = (0, 2, 2, 0, 2, 2) \qquad D^2(\vec{a^c}) = (0, 2, 2, 0, 2, 2)$$

$$D^3(\vec{a}) = (2, 0, 2, 2, 0, 2) \qquad D^3(\vec{a^c}) = (2, 0, 2, 2, 0, 2)$$

$$D^4(\vec{a}) = (2, 2, 0, 2, 2, 0) = D(\vec{a}) \qquad D^4(\vec{a^c}) = (2, 2, 0, 2, 2, 0) = D(\vec{a^c})$$

A remark about the proof in Lemma 3.4

Remark (3.5)

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

Proof

Notations

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

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

for all $(x_1, x_2, \cdots, x_{N-1}, x_N) \in A_N$.

Notations

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.

Notations

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:
$\mathscr{D} = D\,|_{(\mathbb{Z}_2)^N}$, $\mathscr{T} = T\,|_{(\mathbb{Z}_2)^N}$, and

Notations

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:
$\mathscr{D} = D\,|_{(\mathbb{Z}_2)^N}$, $\mathscr{T} = T\,|_{(\mathbb{Z}_2)^N}$, and $\mathscr{D}^0 = \mathscr{T}^0 = \mathscr{I}$, where $\mathscr{I}$ is the identity on $(\mathbb{Z}_2)^N$.

A property about the complement of N-tuples in cycles

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* $\vec{a}$*.*

A property about the complement of N-tuples in cycles

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

A property about D and T

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

Prepare for Theorem 3.13

Remark (3.8)

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

Proof

Prepare for Theorem 3.13

Remark (3.9)

Let $\mathscr{L} : (\mathbb{Z}_2)^N \to (\mathbb{Z}_2)^N$ be a function.

Prepare for Theorem 3.13

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

A property about $\mathscr{T}$

Lemma (3.10)

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

Proof

A property about $\mathscr{D}$

Lemma (3.11)

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

Proof

Prepare for Theorem 3.13

Lemma (3.12)

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

Prepare for Theorem 3.13

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

Prepare for Theorem 3.15

Lemma (3.14)

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

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

Prepare for Theorem 3.15

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

Similar cycles of 6-tuples in A_6

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) $(0, 0, 0, 0, 0, 0)$.

Similar cycles of 6-tuples in A_6

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) $(0, 1, 1, 0, 1, 1), (1, 0, 1, 1, 0, 1), (1, 1, 0, 1, 1, 0)$.

Similar cycles of 6-tuples in A_6

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) $(0, 1, 0, 0, 0, 1), (1, 1, 0, 0, 1, 1), (0, 1, 0, 1, 0, 0),$
$(1, 1, 1, 1, 0, 0), (0, 0, 0, 1, 0, 1), (0, 0, 1, 1, 1, 1)$.

Similar cycles of 6-tuples in A_6

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

The complement of 6-tuples in $(\mathbb{Z}_2)^6$

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 $\vec{a^c}$.

The complement of 6-tuples in $(\mathbb{Z}_2)^6$

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

A property of the complement of 6-tuples 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

A property of the complement of 6-tuples 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

Similar cycles of Diffy Hexagons

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) $(0,0,0,0,0,0)$.

Similar cycles of Diffy Hexagons

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) $(0, 1, 1, 0, 1, 1)$.

Similar cycles of Diffy Hexagons

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

The period of Diffy N-gons

Let r, s be positive integers. Suppose that $N = 2^s$ and $\vec{e}_1 = (1, 0, \cdots, 0) \in A_N$.

The period of Diffy N-gons

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 $\vec{\mathbf{0}}$

The period of Diffy N-gons

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,

The period of Diffy N-gons

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.

The period of Diffy N-gons

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.

The period of Diffy N-gons

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).