Available online at www.sciencedirect.com
ScienceDirect
00 (2024) 1–34

# Periods of strongly connected multivariate digraphs[1]

Chengyang Qian[a], Yaokun Wu[a], Yinfeng Zhu[b]

[a]School of Mathematical Sciences and MOE-LSC, Shanghai Jiao Tong University, Shanghai 200240, CHINA
[b]Institute of Natural Sciences and Mathematics, Ural Federal University, Ekaterinburg 620000, RUSSIA

**Abstract**

For any positive integer $t$, a $t$-variable digraph on a set $K$ is a map $f$ from $K^t$ to $K$. As a qualitative counterpart of going from Markov chains to higher-order Markov chains, Wu, Xu and Zhu suggested in 2017 a study of $t$-variable digraphs, viewing usual digraphs as 1-variable digraphs. Each strongly connected digraph has a period; this fact indeed extends to all strongly connected $t$-variable digraphs. Let $\mathcal{PS}(t)$ denote the set of all periods of strongly connected $t$-variable digraphs, let $g(t)$ be its Frobenius number, namely the largest nonnegative integer that is not a member of $\mathcal{PS}(t)$, and let $n(t)$ be its Sylvester number, namely the number of positive integers outside of $\mathcal{PS}(t)$. We provide new estimates for $g(t)$ and $n(t)$. We also find that $\mathcal{PS}(t) \cap \{1, 2, \ldots, 4t-1\}$ is $\{1, 8\}$ and $\{1\}$ when $t \in \{3, 4\}$ and $t \geq 5$, respectively.

*Keywords:* cyclic decomposition, deflation set, diagonal position, discrete box, height, $t$-difference set
*2000 MSC:* 68R15, 05A18, 05B40, 05C45

**Contents**



[1]The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

## 1. Introduction

Let $K$ be a set. A digraph $D$ with vertex set $K$ can be thought of as the map $f$ from $K$ to $2^K$ such that, for every vertex $v$ of $D$, $f(v)$ is equal to the set of out-neighbors of $v$ in $D$. Let $t$ be a positive integer. One can then call any map $f$ from $K^t$ to $2^K$ a **$t$-variable digraph** on its vertex set $\mathrm{V}_f \doteq K$. Multivariate digraphs thus obtained, also referred to as **$t$-hydras**, represent a generalization of **hy**pergraphs and **di**g**ra**phs; see [WXZ17, p. 5]. Let $f$ be a $t$-variable digraph on $K$. We call $f$ **trivial** provided $f(v) = \emptyset$ for all $v \in K^t$. The **Markov operator** of $f$, denoted by $M_f$, is the map from $(2^K)^t$ to $(2^K)^t$ such that $M_f(A_1, \dots, A_t) = (A_2, \dots, A_t, \bigcup_{(v_1,\dots,v_t)\in A_1\times\cdots\times A_t} f(v_1, \dots, v_t))$ for all $A_1, \dots, A_t \subseteq K$ [WXZ17, p. 4]. Note that Markov operators of $t$-variable digraphs are nothing but Boolean $t$-linear maps, which were proposed by Wu, Xu and Zhu [WXZ16, § 3.2] as a model of a nonparametric version of order-$t$ Markov chains. Let $\mathbb{N}$ stand for the set of all positive integers and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For any integer $k$, we write $[k]$ for the set of elements of $\mathbb{N}$ that are not bigger than $k$, and we use $\langle k\rangle$ for the set of elements of $\mathbb{N}_0$ that are not bigger than $k$. For any $v, u \in K^t$, let $\mathrm{RI}_f(v, u)$ denote the set of $n \in \mathbb{N}_0$ such that $u \in M_f^n(v)$; we call each $n \in \mathrm{RI}_f(v, u)$ a **reachable index** of $f$ from $v$ to $u$. The $t$-variable digraph $f$ is **strongly connected** whenever $\mathrm{RI}_f(v, u) \neq \emptyset$ for all $v, u \in K^t$. The **diameter** of $f$ is the minimum number $d \in \mathbb{N}_0$ such that for any $v, u \in K^t$ it holds $\mathrm{RI}_f(v, u) \cap \langle d\rangle \neq \emptyset$. The **period** of $f$ is the greatest common divisor of $\bigcup_{v\in K^t} \mathrm{RI}_f(v, v)$. For every $k \in \mathbb{N}$, let $\mathcal{P}(k, t)$ stand for the set of all possible periods of strongly connected nontrivial $t$-variable digraphs on a set of $k$ elements. In the notation $\mathcal{P}(k, t)$, we may view $k$ as the space parameter and $t$ as the time parameter for the set of periods. Accordingly, let us adopt the notation $\mathcal{PS}(t)$ and $\mathcal{PT}(k)$ for $\bigcup_{k\in\mathbb{N}} \mathcal{P}(k, t)$ and $\bigcup_{t\in\mathbb{N}} \mathcal{P}(k, t)$, respectively.

Let $p$ be a positive integer. We write $\mathbb{Z}/p\mathbb{Z}$ for the finite ring of integers modulo $p$. Throughout the paper, we use $i + p\mathbb{Z}$ to represent a residue class in $\mathbb{Z}/p\mathbb{Z}$ while $i + p\mathbb{N}$ stands for the set $\{i + pj : j \in \mathbb{N}\} \subseteq \mathbb{Z}$. An **interval** in $\mathbb{Z}/p\mathbb{Z}$ of length $s \in [p]$ is a set of the form $\{i + p\mathbb{Z}, i + 1 + p\mathbb{Z}, \dots, i + s - 1 + p\mathbb{Z}\} \in \binom{\mathbb{Z}/p\mathbb{Z}}{s}$, which we denote by $[i + p\mathbb{Z}, i + s - 1 + p\mathbb{Z}]$. When $s < p$, we can tell from the underlying set of this interval its left endpoint $i + p\mathbb{Z}$ and right endpoint $i + s - 1 + p\mathbb{Z}$. When $s = p$, we have to read from its notation $[i + p\mathbb{Z}, i + s - 1 + p\mathbb{Z}]$ the two endpoints. We mention that $[1 + 5\mathbb{Z}, 5\mathbb{Z}] = [2 + 5\mathbb{Z}, 1 + 5\mathbb{Z}] = \mathbb{Z}/5\mathbb{Z}$ and that $[3 + 5\mathbb{Z}, 3 + 5\mathbb{Z}]$ is a singleton set but not the whole set $\mathbb{Z}/5\mathbb{Z}$. If we are clear from the context that we are working in $\mathbb{Z}/p\mathbb{Z}$, we may safely write $[i + p\mathbb{Z}, i + s - 1 + p\mathbb{Z}]$ as $[i, i + s - 1]$. Let $\Phi$ be a map defined on $\mathbb{Z}/p\mathbb{Z}$. For any $i \in \mathbb{Z}/p\mathbb{Z}$, we often use $\Phi_i$ for $\Phi(i)$. For any integer $i$, we often simplify the notation $\Phi_{i+p\mathbb{Z}}$ to $\Phi_i$ when the parameter $p$ is clear from the context. When $I$ is an interval of $\mathbb{Z}/p\mathbb{Z}$ of length $s$ with given left endpoint $\ell$ and right endpoint $r$, we often think of $\Phi_I$ as the product set $\Phi_\ell \times \Phi_{\ell+1} \times \cdots \times \Phi_r$ and refer to it as a **$\Phi$-interval of length** $s$. Note that in $\mathbb{Z}/5\mathbb{Z}$, we have $[1 + 5\mathbb{Z}, 5\mathbb{Z}] = [2 + 5\mathbb{Z}, 1 + 5\mathbb{Z}]$ surely; but for any $\Phi$ defined on $\mathbb{Z}/5\mathbb{Z}$, $\Phi_{[1,5]} = \Phi_1 \times \cdots \times \Phi_5$ may not be equal to $\Phi_{[2,1]} = \Phi_2 \times \cdots \times \Phi_6$. For any $I \subseteq \mathbb{Z}$, $\Phi_I$ is often used interchangeably with $\Phi_{I+p\mathbb{Z}}$. In the same manner, when discussing a subset of $\mathbb{Z}/p\mathbb{Z}$, we may sometimes directly write a subset $S$ of $\mathbb{Z}$ to refer to $\{i + p\mathbb{Z} : i \in S\} \subseteq \mathbb{Z}/p\mathbb{Z}$, simply to simplify our notation. The cyclicity theorem for digraphs claims that each digraph $f$ with finite diameter and positive period $p$ looks like a $p$-cycle, namely there is a map Loc from $\mathrm{V}_f$ to $\mathbb{Z}/p\mathbb{Z}$ and a positive integer $M$ such that for all $u, v \in \mathrm{V}_f$ it holds $\mathrm{RI}_f(u, v) \setminus [M] = i + p\mathbb{N} \setminus [M]$ for the unique integer $i \in \langle p - 1\rangle$ satisfying $i + p\mathbb{Z} = \mathrm{Loc}(v) - \mathrm{Loc}(u)$. Note that the period of a strongly connected digraph is also named as its index of imprimitivity and a strongly connected digraph with period 1 is called a primitive digraph [BR91, § 3.4][Haw13, § 17.2]. It turns out that the cyclicity theorem extends to general $t$-hydras [WXZ17, Theorem 10], which explains why the concept of periods of hydras is fundamental for a study of multivariate graph theory.

**Definition 1.1** (Cyclic decomposition [WXZ17, Section 3])**.** Let $t, p \in \mathbb{N}$, let $K$ be a set and let $X$ be a subset of $K^t$. A **cyclic decomposition** of $(X, K, t)$ with **period** $p$ is a map $\Phi$ from $\mathbb{Z}/p\mathbb{Z}$ to $2^K \setminus \emptyset$ such that $\Phi_{[j,j+t-1]} = \prod_{i\in\langle t-1\rangle} \Phi_{j+i}$, $j \in [p]$, is a partition of $X$. We refer to $t$ as the **order** of the cyclic decomposition $\Phi$. A cyclic decomposition of $(X, K, t)$ is **discrete** if its period is $|X|$. Let $\mathcal{U}$ stand for the set of triples $(p, |K|, t)$ such that there is a cyclic decomposition of $(K^t, K, t)$ with period $p$.

**Theorem 1.2** ([WXZ17, Theorem 13])**.** *For any nonempty set $K$ and any $p, t \in \mathbb{N}$, it holds $(p, |K|, t) \in \mathcal{U}$ if and only if there exists a strongly connected nontrivial $t$-variable digraph on the vertex set $K$ with period $p$. Especially, for any $(p, k, t) \in \mathbb{N}^3$, it holds $p \in \mathcal{P}(k, t)$ if and only if $(p, k, t) \in \mathcal{U}$.*

*Example* 1.3 ([WXZ17, p. 16]). It holds that $8 \in \mathcal{P}(2, 4) \subseteq \mathcal{PS}(4)$. Indeed, the map $\Phi$ from $\mathbb{Z}/8\mathbb{Z}$ to $2^{[4]} \setminus \emptyset$ given below is a cyclic decomposition of $([2]^4, [2], 4)$:

$$\Phi_i = \begin{cases} \{1\}, & \text{if } i = 1, 2, 4, \\ \{2\}, & \text{if } i = 5, 6, 8, \\ \{1, 2\}, & \text{if } i = 3, 7. \end{cases}$$

Note that this construction also appears in [CKMS17a, § 5] and [CKMS17b, § 2.3]. Some more interesting facts about this construction $\Phi$ will be revealed in Example 8.6.

So far, we have briefly illustrated how our investigation into multivariate graph theory leads us to the study of cyclic decomposition [WXZ17]. Let us demonstrate in Theorem 1.4 some simple sample results from [WXZ17]. Both the Sylvester number and the Frobenius number are important parameters for numerical semigroups, which are subsets of the set of positive integers with some structural constraints [ADGS20, BCDF20, RGS09]. We can extend their definitions for general subsets of $\mathbb{N}$ here. For each set $M \subseteq \mathbb{N}$, the **Sylvester number** of $M$, denoted by $\mathrm{n}_M$, is the size of $\mathbb{N} \setminus M$, and the **Frobenius number** of $M$, denoted by $\mathrm{g}_M$, is defined to be $\max \mathbb{N}_0 \setminus M$. When $\mathrm{n}_M = \infty$, we surely use the convention that $\mathrm{g}_M = \infty$. We mention that different authors may have different conventions and some may refer to $\mathrm{g}_M + 1$ as the Frobenius-Schur index of $M$ [BR91, p. 72]. It is clear that $\mathrm{n}_{\mathcal{PS}(1)} = \mathrm{g}_{\mathcal{PS}(1)} = 0$.

**Theorem 1.4.** *(a) [WXZ17, Theorem 15] $\mathrm{g}_{\mathcal{PS}(t)} < \infty$ for all $t \in \mathbb{N}$.*

*(b) [WXZ17, Proposition 16] It holds for every integer $t \geq 2$ that $\mathcal{PS}(t) \cap [2, 2t-1] = \emptyset$, and so $\mathrm{g}_{\mathcal{PS}(t)} \geq 2t - 1$.*

*(c) [WXZ17, Theorem 22] We have $\mathcal{PS}(2) = \mathbb{N} \setminus \{2, 3, 5, 6, 7\}$. Henceforth, $\mathrm{n}_{\mathcal{PS}(2)} = 5$ and $\mathrm{g}_{\mathcal{PS}(2)} = 7$.*

It is time to introduce the new results to be established in this paper. Theorems 1.5 and 1.6 improve our earlier work in [WXZ17, Proposition 18] and even the relevant result announced in [WXZ17, p. 15]. We report Theorem 1.7 and Corollary 1.8 as quantitative counterparts of Theorem 1.4 (a). In 2017 we were only attempting to calculate $\mathcal{PS}(t) \cap [3t - 2]$ [WXZ17, p. 15]. By a complete reexamination of our long reasoning chain constructed in 2017, we can now present Theorem 1.9 and its slightly more streamlined proof.

**Theorem 1.5.** *Let $t \geq 2$ be an integer. Then $\{2^t - 1, 2^t - 2, \dots, 2^t - \lfloor \frac{t}{2} \rfloor\} \setminus \mathcal{PS}(t) \neq \emptyset$. Henceforth, $\mathrm{g}_{\mathcal{PS}(t)} \geq 2^t - \lfloor \frac{t}{2} \rfloor$.*

**Theorem 1.6.** *(a) For every integer $t \geq 2$, it holds $[2, 2^{\lceil \sqrt{2t} \rceil} - 1] \cap \mathcal{PS}(t) = \emptyset$.*

*(b) For every integer $t \geq 4$ and every $p \in \mathcal{PS}(t) \setminus \{1\}$ with $t \nmid p$, it holds $p \geq 2^{\lceil 2\sqrt{t} \rceil}$.*

*(c) It holds $\mathrm{n}_{\mathcal{PS}(t)} \geq \left\lfloor \frac{t-1}{t} (2^{\lceil 2\sqrt{t} \rceil} - 2^{\lceil \sqrt{2t} \rceil}) \right\rfloor + 2^{\lceil \sqrt{2t} \rceil} - 2$ for all integers $t \geq 2$.*

**Theorem 1.7.** *Let $t \in \mathbb{N}$ and let $k$ be the minimum integer satisfying $k \geq 3$ and $\gcd(t, 3^t - 2^t, \dots, k^t - (k-1)^t) = \gcd(t, 3^t - 2^t, 4^t - 2^t, \dots, k^t - 2^t) = 1$. Then $(t-1)(k^t - (k-1)^t - 1) + 3^t + \mathbb{N}_0 \subseteq \mathcal{PS}(t)$, namely $\mathrm{g}_{\mathcal{PS}(t)} \leq (t-1)(k^t - (k-1)^t - 1) + 3^t - 1$.*

**Corollary 1.8.** *Let $t \geq 2$ be an integer and let $k$ be its largest prime factor. Then,*

$$\mathrm{g}_{\mathcal{PS}(t)} \leq \begin{cases} (t-1)(3^t - 2^t - 1) + 3^t - 1, & \textit{if } t \textit{ is a prime or a power of } 2, \\ (t-1)(k^t - (k-1)^t - 1) + 3^t - 1, & \textit{else.} \end{cases}$$

**Theorem 1.9.** *It holds for each $t \in \mathbb{N}$ that* $\mathcal{PS}(t) \cap [4t - 1] = \begin{cases} [3], & \textit{if } t = 1, \\ \{1, 4\}, & \textit{if } t = 2, \\ \{1, 8\}, & \textit{if } t = 3, 4, \\ \{1\}, & \textit{if } t \geq 5. \end{cases}$

The remainder of the paper is organized as follows. In Section 2 we define deflation numbers and then make use of an ingenious idea of Alon et al. [ABHK02, Theorem 1] to get a lower bound estimate of periods in terms of deflation numbers. Section 3 presents the concepts of $t$-difference set and diagonal positions. By looking into diagonal positions, we can establish a lower bound estimate of deflation numbers via our estimate of the minimum size of a

$t$-difference set. This work, along with the work in Section 2 enables us to prove Theorems 1.5 and 1.6 in Section 3. We next turn to upper bounds of Frobenius numbers, and thus we need to design cyclic decompositions. Our main tool will be so-called rooted cyclic decomposition and we shall prove Theorem 1.7 and Corollary 1.8 in Section 4. We introduce the idea of height and obtain some basic properties of it in Section 5. Section 6 prepares two technical results on diagonal positions. As a touchstone for all our tools developed so far for understanding the periods of hydras, we determine in Section 7 all possible periods $\leq 4t-1$ of $t$-hydras, namely we deduce Theorem 1.9 there. We conclude this paper with some further questions and remarks in Section 8.

*Remark* 1.10. This work, mostly done in 2017, aims to further our research in [WXZ17] on determining the structure of $\mathcal{PS}(t)$, namely the periods of $t$-hydras. We should mention that the term 'period' is also used in a way quite different from what we discuss in this paper; the same term may refer to some countable class of complex numbers defined by algebraic integrals, which has been widely studied in mathematics and physics [KZ01]. On the other hand, we have recently noticed that the active study of universal partial cycles in the field of combinatorics on words is indeed a study of cyclic decomposition with some constraints, which is closely related to the study of universal partial words [CK20, CKMS17a, CKMS17b, FGK+23, GGH+18, GS18, SK01]. Partial word was introduced by Berstel and Boasson [BB99]. Chen, Kitaev, Mütze, and Sun [CKMS17a, CKMS17b] introduced the notion of universal partial words, a generalization of universal words and De Bruijn sequences. In their terminology, a cyclic decomposition $\Phi$ of $(K^t, K, t)$ with period $p$ such that $\Phi_i \in \{K\} \cup \binom{K}{1}$ for all $i \in \mathbb{Z}/p\mathbb{Z}$ is called a **cyclic universal partial word over $K$ of length $t$ and period $p$**. When $|K| = 2$, such a construction is named a **binary cyclic universal partial word of length $t$ and period $p$**. Note that Example 1.3 gives a binary cyclic universal partial word of length 4 and period 8. We will say a bit more on this aspect in Section 8.

## 2. Lower bound of the Frobenius number: Deflation number

**Definition 2.1** (Deflation number and deflation set)**.** Let $K$ be a set, let $t \in \mathbb{N}$, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $p$. Let

$$\Phi^{\#}_{<} \doteq \left|\{i \in \langle t-1\rangle : \Phi_i \neq K\}\right|,$$

and let

$$\Phi^{i}_{<} \doteq \{j \in \langle t-1\rangle : \Phi_{i+j} \neq K\}.$$

for every $i \in \mathbb{Z}/p\mathbb{Z}$. We name $\Phi^{\#}_{<}$ the **deflation number** of $\Phi$ and $\Phi^{i}_{<}$ the ***i*th deflation set** of $\Phi$.

Prior to proving our results on the deflation number of a cyclic decomposition, we prepare some notations that will be used throughout our analysis of cyclic decompositions.

**Definition 2.2** (Location)**.** Let $K$ be a set, $t \in \mathbb{N}$, $X \subseteq K^t$, and let $\Phi$ be a cyclic decomposition of $(X, K, t)$ with period $p$. For any word $y$ over $K$, say $y = y_0y_1\cdots y_m \in K^{m+1}$, we define $\mathrm{Loc}_\Phi(y)$ to be the set

$$\{j :\ y_0y_1\cdots y_m \in \Phi_j \times \cdots \times \Phi_{j+m}\} \subseteq \mathbb{Z}/p\mathbb{Z}.$$

We may sometimes just consider $\mathrm{Loc}_\Phi$ as the map restricted on $X \subseteq K^t$, which is then a map from $X$ to $\mathbb{Z}/p\mathbb{Z}$, when we identify $\mathbb{Z}/p\mathbb{Z}$ with $\binom{\mathbb{Z}/p\mathbb{Z}}{1}$. Although we may use the notation $\mathrm{Loc}_\Phi$ in different contexts, we consistently refer to it as the **location function** of $\Phi$.

*Remark* 2.3. Let $K$ be a set, $t \in \mathbb{N}$, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $p$. Assume that $A$ is a subset of $K$ satisfying $\mathrm{Loc}_\Phi(a^t) = j \in \mathbb{Z}/p\mathbb{Z}$ for all $a \in A$. It is easy to see that $\mathrm{Loc}_\Phi(x) = j$ for all $x \in A^t$. We thus adopt the notation $\mathrm{Loc}_\Phi(A^t)$ for this common value $j \in \mathbb{Z}/p\mathbb{Z}$.

After Definition 2.2 we should immediately write down the following most obvious fact about the relation between location function and cyclic decomposition, though we will need it explicitly only in Sections 5 and 7.

**Lemma 2.4.** *Let $K$ be a set, let $t$ and $s$ be two integers satisfying $1 \leq s \leq t-1$ and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$. For any $x \in K^{t-s}$, it holds that $\bigsqcup_{i\in \mathrm{Loc}_\Phi(x)} \Phi_{[i-s,i-1]} = \bigsqcup_{i\in \mathrm{Loc}_\Phi(x)} \Phi_{[i+t-s,i+t-1]} = K^s$.*

*Proof.* Since $\Phi$ is a cyclic decomposition of $(K^t, K, t)$, we have $\bigsqcup_{i\in \mathrm{Loc}_\Phi(x)}(\Phi_{[i-s,i-1]} \times x) = K^s \times x$ and $\bigsqcup_{i\in \mathrm{Loc}_\Phi(x)}(x \times \Phi_{[i+t-s,i+t-1]}) = x \times K^s$. Deleting the common factor $x$ from both sides of the two equalities yields the result. □

Let $p \in \mathbb{N}$ and let $\Phi$ be a map defined on $\mathbb{Z}/p\mathbb{Z}$. If there exists $\ell \in \mathbb{Z}/p\mathbb{Z}$ such that $\Psi_i = \Phi_{\ell+i}$ for all $i \in \mathbb{Z}/p\mathbb{Z}$, we say that $\Psi$ is a **translation** of $\Phi$; if there exists $\ell \in \mathbb{Z}/p\mathbb{Z}$ such that $\Psi_i = \Phi_{\ell-i}$ for all $i \in \mathbb{Z}/p\mathbb{Z}$, we say that $\Psi$ is a **reflection** of $\Phi$. We call two maps $\Phi$ and $\Psi$ defined on $\mathbb{Z}/p\mathbb{Z}$ **equivalent** provided they are translations or reflections of each other; in other words, modulo the dihedral symmetry of the $p$-cycle, $\Phi$ and $\Psi$ are essentially the same. If $\Phi$ is a cyclic decomposition of $(K^t, K, t)$ with period $p$, then any map on $\mathbb{Z}/p\mathbb{Z}$ which is equivalent to $\Phi$ is surely still a cyclic decomposition of $(K^t, K, t)$ with period $p$. Lemma 2.5 shows that $\Phi^{\#}_{<} = \Psi^{\#}_{<}$ whenever $\Phi$ and $\Psi$ are equivalent. We note that a slightly weaker version of Lemma 2.5 is also reported by Chen et al. [CKMS17b, Lemma 14].

**Lemma 2.5.** *Let $K$ be a set, and let $t$ and $p$ be two positive integers. Let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $p$. If $\Phi_i = K$ for some $i \in [p]$, then $\Phi_{i-t} = \Phi_{i+t} = K$.*

*Proof.* Suppose for the sake of contradiction that $\Phi_{i-t} \neq K$. This allows us to find $y \in (K \setminus \Phi_{i-t}) \times \Phi_{[i-t+1,i-1]}$. Clearly, $\mathrm{Loc}_\Phi(y) \neq i-t$. From $\Phi_i = K$ and $\Phi_{[\mathrm{Loc}_\Phi(y)+1,\mathrm{Loc}_\Phi(y)+t-1]} \cap \Phi_{[i-t+1,i-1]} \neq \emptyset$ we derive that $\Phi_{[\mathrm{Loc}_\Phi(y)+1,\mathrm{Loc}_\Phi(y)+t]} \cap \Phi_{[i-t+1,i]} \neq \emptyset$. By the definition of a cyclic decomposition, this then implies $\mathrm{Loc}_\Phi(y) = i - t$, which is a desired contradiction.

Let $\Psi_{i+j} = \Phi_{i-j}$ for all $j \in \mathbb{Z}/p\mathbb{Z}$. It is clear that $\Psi$ is again a cyclic decomposition of $(K^t, K, t)$ with period $p$. Applying what we obtain above on the cyclic decomposition $\Psi$ gives that $\Phi_{i+t} = \Psi_{i-t} = K$. □

**Corollary 2.6.** *Let $K$ be a set, $t, p \in \mathbb{N}$ and $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $p$.*

*(a) If $\Phi_i = K$ for some $i \in [p]$, then $\Phi_{i+\gcd(p,t)} = K$.*

*(b) If $p \geq 2$ and $\gcd(p, t) = 1$, then $\Phi_i \neq K$ holds for all $i \in \mathbb{Z}/p\mathbb{Z}$.*

*Proof.* Invoking Bézout's identity [Gra24], we can find $a, b \in \mathbb{Z}$ such that $ap + bt = \gcd(p, t)$. Let us assume the existence of an index $i \in [p]$ for which $\Phi_i = K$. Thanks to Lemma 2.5, $\Phi_i = K$ should guarantee that $\Phi_{i+\gcd(p,t)} = \Phi_{i+ap+bt} = \Phi_{i+bt} = K$. This confirms (a).

We proceed to validate (b). Let us assume the opposite that $\Phi_i = K$ for some $i \in \mathbb{Z}/p\mathbb{Z}$. It follows from (a) and $\gcd(p, t) = 1$ that $\Phi_j = K$ for all $j \in \mathbb{Z}/p\mathbb{Z}$. As $p \geq 2$ and $\Phi$ is a cyclic decomposition, we find that $\Phi_1 \times \cdots \times \Phi_t = K^t$ and $\Phi_2 \times \cdots \times \Phi_{t+1} = K^t$ must be disjoint, which is absurd. □

Throughout the paper, we use $\sqcup$ for disjoint union.

**Definition 2.7** (Discrete box and subbox)**.** Let $t$ be a positive integer. For any $t$ nonempty sets $A_1, \ldots, A_t$, we call $A \doteq A_1 \times A_2 \times \cdots \times A_t$ a ***t*-dimensional discrete box**. For any set $B \doteq B_1 \times B_2 \times \cdots \times B_t$ satisfying $\emptyset \neq B \subseteq A$, we name it a **subbox** of $A$, and we define the **deflation number of** $B$ **in** $A$, denoted by $\mathrm{DM}(A_1, \ldots, A_t; B_1, \ldots, B_t)$, as $\left|\{i \subseteq [t] : B_i \subsetneq A_i\}\right|$. Two subboxes $B = B_1 \times B_2 \times \cdots \times B_t$ and $C = C_1 \times C_2 \times \cdots \times C_t$ of a box $A = A_1 \times A_2 \times \cdots \times A_t$ are said to be **dichotomous** relative to $A$ provided there is $i \in [t]$ such that $B_i \sqcup C_i = A_i$; a collection of pairwise dichotomous subboxes of a box $A$ is called a **suit** of $A$ [KP08, p. 2].

**Theorem 2.8.** *Let $A \doteq A_1 \times A_2 \times \cdots \times A_t$ be a $t$-dimensional discrete box. Assume that $A = \bigsqcup_{j\in[p]} B^j$, where $B^j \doteq B^j_1 \times \cdots \times B^j_t$ and $\mathrm{DM}(A_1, \ldots, A_t; B^j_1, \ldots, B^j_t) = d_j$ for each $j \in [p]$. Then, it holds*

$$\sum_{j\in[p]} 2^{-d_j} \geq 1, \tag{1}$$

*with equality if and only if $\{B^1, \ldots, B^p\}$ is a suit of $A$.*

*Proof.* For each $i \in [t]$ and $I \subseteq [p]$ such that $\Sigma_{i,I} \doteq (\bigcap_{j\in I} B^j_i) \setminus (\bigcup_{j\in[p]\setminus I} B^j_i) \neq \emptyset$, we fix one element $\sigma_{i,I} \in \Sigma_{i,I}$. Replacing $B^j_i$ by $\{\sigma_{i,I} : \Sigma_{i,I} \neq \emptyset, j \in I\}$ and $A_i$ by $\bigcup_{j\in[p]} B^j_i$, we see that one can safely assume that $A_1, \ldots, A_t$ are all finite sets.

Let $O(A) \doteq \left\{C_1 \times \cdots \times C_t \subseteq A : \prod_{j\in[t]} |C_j| \equiv 1 \pmod 2\right\}$. For every $j \in [p]$, we further define $O(A, B^j) \doteq \left\{C \in O(A) : |C \cap B^j| \equiv 1 \pmod 2\right\}$.

Take $j \in [p]$ and assume that $\{\alpha_1^j < \cdots < \alpha_{d_j}^j\} = \{i \in [t] : B_i^j \neq A_i\}$. Let $I_1^j, \ldots, I_{d_j}^j$ be $d_j$ sets such that $I_r^j \in \binom{A_r}{2}$ and $|I_r^j \cap B_r^j| = 1$ for all $r \in [d_j]$. For every $C \in O(A)$, it is a member of a set of $2^{d_j}$ elements from $O(A)$, namely $C^{B_j;x_1,\ldots,x_{d_j}}, x_1, \ldots, x_{d_j} \in \{0, 1\}$, where $C^{B_j;x_1,\ldots,x_{d_j}} = C_1^{B_j;x_1,\ldots,x_{d_j}} \times \cdots \times C_t^{B_j;x_1,\ldots,x_{d_j}}$ with

$$C_i^{B_j;x_1,\ldots,x_{d_j}} = \begin{cases} C_i, & \text{if } C_i = A_i, \\ C_i, & \text{if } i = \alpha_r^j \text{ and } x_r = 0, \\ C_i \triangle I_r^j, & \text{if } i = \alpha_r^j \text{ and } x_r = 1. \end{cases}$$

Surely, among this group of $2^{d_j}$ elements from $O(A)$, exactly one of them falls inside $O(A, B^j)$. Essentially, we now have an action of the group $(\mathbb{Z}/2\mathbb{Z})^{t-d_j}$ on $O(A)$, each orbit of it having size $2^{d_j}$ and intersecting with $O^j(A)$ exactly once. This then tells us that

$$\frac{|O(A, B^j)|}{|O(A)|} = \frac{1}{2^{d_j}}. \tag{2}$$

For each $C \in O(A)$, $C \cap B^1, C \cap B^2, \ldots, C \cap B^p$ surely form a partition of it, and so at least one of them is of odd size. This means that

$$\bigcup_{j \in [p]} O(A, B^j) = O(A). \tag{3}$$

Putting together Eqs. (2) and (3), we get $\sum_{j\in[p]} 2^{-d_j}|O(A)| = \sum_{j\in[p]}|O(A, B^j)| \geq |O(A)|$, and thus (1) follows.

Equality holds in (1) if and only if the union on the left-hand side of Eq. (3) is a disjoint union. Hence, it remains to show for any $\{j, j'\} \in \binom{[p]}{2}$ that $O(A, B^j) \cap O(A, B^{j'}) = \emptyset$ if and only if there exists $i \in [t]$ such that $B_i^j \sqcup B_i^{j'} = A_i$. Assume that there does not exist any $i \in [t]$ such that $B_i^j \sqcup B_i^{j'} = A_i$. For any $i \in [t]$, we choose $C_i$ to be a set $\{x_i\} \subseteq B_i^j \cap B_i^{j'}$ whenever $B_i^j \cap B_i^{j'} \neq \emptyset$, while we choose $C_i$ to be a set $\{x_i, y_i, z_i\}$ such that $x_i \in B_i^j$, $y_i \in B_i^{j'}$ and $z_i \in A_i \setminus (B_i^j \cup B_i^{j'})$ whenever $B_i^j \cup B_i^{j'} \neq A_i$ and $B_i^j \cap B_i^{j'} = \emptyset$. It is clear that $C_1 \times \cdots \times C_t \in O(A, B^j) \cap O(A, B^{j'})$. Assume that there exists $i \in [t]$ such that $B_i^j \sqcup B_i^{j'} = A_i$. Then, for any subbox $C$ of $A$ with $|C \cap B^j| \equiv |C \cap B^{j'}| \equiv 1 \pmod 2$, we have $|C_i| = |C_i \cap B_i^j| + |C_i \cap B_i^{j'}| \equiv 1 + 1 \equiv 0 \pmod 2$, showing that $O(A, B^j) \cap O(A, B^{j'}) = \emptyset$. □

**Corollary 2.9.** *If a t-dimensional discrete box admits a partition into p subboxes with deflation numbers at least d, then* $p \geq 2^d$.

*Proof.* This is straightforward from (1), an inequality reported in Theorem 2.8. □

*Remark* 2.10. Recall the map $\Phi$ constructed in Example 1.3. One can check that $B^j \doteq \Phi_{[j+1,j+4]}$, $j \in \mathbb{Z}/8\mathbb{Z}$, gives a partition of $[2]^4$ into eight subboxes, and $\mathrm{DM}([2],[2],[2],[2]; \Phi_{j+1}, \Phi_{j+2}, \Phi_{j+3}, \Phi_{j+4}) = 3$ for all $j \in \mathbb{Z}/8\mathbb{Z}$. Observe that $8 = 2^3$, which says that the bounds in Theorem 2.8 and Corollary 2.9 are both tight.

**Theorem 2.11.** *Let K be a set and take* $t \in \mathbb{N}$. *Let* $\Phi$ *be a cyclic decomposition of* $(K^t, K, t)$ *with period p. Then it holds* $p \geq 2^{\Phi^\#_<}$.

*Proof.* According to Lemma 2.5, for each $i \in [p]$, $\Phi_{[i+1,i+t]}$ constitutes a subbox of $K^t$ with deflation number $\Phi^\#_<$. Note that $\Phi_{[i+1,i+t]}$, $i \in [p]$, form a partition of $K^t$. Henceforth, Corollary 2.9 claims that $p \geq 2^{\Phi^\#_<}$, as wanted. □

*Remark* 2.12. In the course of establishing Theorem 2.11 in 2016, we were led to the statement of Corollary 2.9. It looks so simple that we always expected to find a proof in a few lines. But we got stuck with it for several months and so we wrote to some friends in different countries for possible help. We had no progress until one day when we suddenly ran into the paper by Saks [Sak02]. According to him, at the August 1999 meeting at MIT that was held to celebrate Kleitman's 65th birthday, a problem due to Kearnes and Kiss [KK99] was presented in the open problem session, and then a wonderful four-person team solved this problem during the conference [ABHK02]. Actually, our Corollary 2.9 for $d = t$ coincides with the result conjectured by Kearnes and Kiss and proved by Alon, Bohman, Holzman and Kleitman. Our proof of (1) in Theorem 2.8, of course, is simply following the proof of [ABHK02, Theorem 1] by Alon et al. The characterization of the equality case in Theorem 2.8 is essentially the same with [GKP04, Theorem 2] and [KP08, Theorem 2.1].

## 3. Lower bound of deflation number: Difference set and diagonal position

**Definition 3.1** ($t$-difference set)**.** For every set $S$ of integers, we write $\partial_S$ for the set $\{j - i : i, j \in S, i \leq j\}$ and name it the **difference set** of $S$. For any $t \in \mathbb{N}$, we call $S \subseteq [t]$ a **$t$-difference set** provided $\partial_S = \langle t-1 \rangle = \partial_{[t]}$, and we write $\Upsilon(t)$ to denote the smallest size of a $t$-difference set. Note that $[t]$ is itself a $t$-difference set, so $\Upsilon(t)$ is well-defined. Also note that $S \subseteq [t]$ is a $t$-difference set if and only if $t - \partial_S = [t]$.

**Lemma 3.2.** *(a) It holds* $\Upsilon(1) = 1 = \left\lceil \sqrt{2 \times 1 - \frac{7}{4}} + \frac{1}{2} \right\rceil = \left\lceil 2\sqrt{1} \right\rceil - 1$.

*(b) It holds* $\Upsilon(t) \geq \left\lceil \sqrt{2t - \frac{7}{4}} + \frac{1}{2} \right\rceil$ *for every* $t \in \mathbb{N}$.

*(c) It holds* $\Upsilon(t) \leq \left\lceil 2\sqrt{t} \right\rceil - 1$ *for every* $t \in \mathbb{N}$.

*(d) It holds* $\Upsilon(t) = \left\lceil \sqrt{2t - \frac{7}{4}} + \frac{1}{2} \right\rceil$ *for every* $t \in [10]$ *and* $\Upsilon(11) = 6 > 5 = \sqrt{2 \times 11 - \frac{7}{4}} + \frac{1}{2}$.

*Proof.* (a). This is trivial.

(b). Thanks to (a), we assume $t \geq 2$. Take a $t$-difference set $S$. From $\binom{|S|}{2} \geq |\partial_S \setminus \{0\}| = t - 1$ we can obtain $|S| \geq \left\lceil \sqrt{2t - \frac{7}{4}} + \frac{1}{2} \right\rceil$, as desired.

(c). According to (a), we only consider the case of $t \geq 2$. For every $m \in [t-1]$, we define $f_{m,t} \doteq \left\lceil \frac{t}{m} \right\rceil - 1 \in \mathbb{N}$ and

$$S_{m,t} \doteq [m] \sqcup \{t - jm : j \in \langle f_{m,t} - 1 \rangle\}. \tag{4}$$

Take $m \in [t-1]$. Note that

$$m f_{m,t} + m \geq t > m f_{m,t}. \tag{5}$$

For every $i \in \langle m-1 \rangle$, from $1, i+1 \in S_{m,t}$ we get $i \in \partial_{S_{m,t}}$. For each $i \in [t-1] \setminus [t-1-m f_{m,t}]$, it holds that $0 \leq t-1-i < m f_{m,t}$ and $\frac{t-i}{m} \leq 1 + \lfloor \frac{t-i-1}{m} \rfloor$, which then imply $t - m\left\lfloor \frac{t-1-i}{m} \right\rfloor \in S_{m,t}$ and $t - i - m\left\lfloor \frac{t-i-1}{m} \right\rfloor \in [m] \subseteq S_{m,t}$, respectively, thus obtaining $[t-1] \setminus [t-1-m f_{m,t}] \subseteq \partial_{S_{m,t}}$. (5) claims that $t - 1 \geq m f_{m,t} \geq t - m$ and so it holds $\partial_{S_{m,t}} = \langle t-1 \rangle$.

Let $n$ and $m$ be positive integers such that $m + n = \left\lceil 2\sqrt{t} \right\rceil - 1$ and that $n - m \in \{0, -1\}$. It follows from (5) that $m f_{m,t} < t$ and so we have $|S_{m,t}| = m + f_{m,t}$. Moreover, it holds

$$m(n+1) \geq \left(\frac{m+n+1}{2}\right)^2 - \frac{1}{4} \geq \left(\frac{2\sqrt{t}}{2}\right)^2 - \frac{1}{4} = t - \frac{1}{4}. \tag{6}$$

Considering that both $m(n+1)$ and $t$ are integers, (6) indeed gives $m(n+1) \geq t$. Therefore, it holds that $f_{m,t} = \left\lceil \frac{t}{m} \right\rceil - 1 \leq n$. Now the proof is completed by noting that $|S_{m,t}| = m + f_{m,t} \leq m + n = \left\lceil 2\sqrt{t} \right\rceil - 1$.

(d). It holds that $\left\lceil \sqrt{2t - \frac{7}{4}} + \frac{1}{2} \right\rceil = \left\lceil 2\sqrt{t} \right\rceil - 1$ for every $t \in [9] \setminus \{7\}$. In view of (b) and (c), we only need to check (d) for $t \in \{7, 10, 11\}$. It follows from (b) that $\Upsilon(7) \geq 4$ and $\Upsilon(10) \geq 5$. Recall the definition of $S_{m,t}$ in Eq. (4). When $t \in \{7, 10\}$, it holds that $\partial_{S_{2,t}} = \langle t-1 \rangle$ and $|S_{2,t}| = 2 + f_{2,t} = \begin{cases} 4, \text{if } t = 7 \\ 5, \text{if } t = 10. \end{cases}$ Consequently, we find that $\Upsilon(7) = 4$ and $\Upsilon(10) = 5$. It follows from (c) that $\Upsilon(11) \leq 6$. However, a computer enumeration shows that $\partial_S \neq \langle 10 \rangle$ for every $S \in \binom{[11]}{5}$. Thereby, we arrive at $\Upsilon(11) = 6$, as desired. □

**Definition 3.3** (Diagonal positions)**.** Let $K$ be a set, $t \in \mathbb{N}$, $\{k^t : k \in K\} \subseteq X \subseteq K^t$, and let $\Phi$ be a cyclic decomposition of $(X, K, t)$ with period $p$. The **diagonal positions** for $\Phi$, denoted by $\mathrm{Diag}_\Phi$, are defined to be $\{\mathrm{Loc}_\Phi(k^t) : k \in K\}$, which is a nonempty subset of $\mathbb{Z}/p\mathbb{Z}$.

We digress to mention that diagonal positions have been a useful perspective to analyze cyclic decompositions in [WXZ17], as we will also see shortly in Lemma 3.5. Here is a sample result from [WXZ17], which we will appeal to in Sections 5 to 7.

**Lemma 3.4.** *Let $K$ be a set, let $t$ and $p$ be positive integers, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $p$. Then the following statements hold.*

*(a) [WXZ17, Lemma 51(c)] For all $i, j \in \mathrm{Diag}_\Phi$, it holds $i - j \notin \{1 + p\mathbb{Z}, 2 + p\mathbb{Z}, \ldots, t - 1 + p\mathbb{Z}\}$.*

*(b) It holds $|\mathrm{Diag}_\Phi| \le \lfloor \frac{p}{t} \rfloor$.*

*(c) [WXZ17, Lemma 51(d)] If $p \ge 2$, then $\mathrm{Diag}_\Phi$ contains at least two elements.*

*Proof.* (a) and (c) have been proved in [WXZ17, Lemma 51]. Note that they were claimed there with the additional assumption of the finiteness of $K$. However, the result holds true for general $K$ whenever it is valid for finite $K$. To see this, we only need to notice that the statement of the result allows us to assume, without loss of generality that, for every $J \subseteq \mathbb{Z}/p\mathbb{Z}$, $(\bigcap_{i\in J} \Phi_i) \setminus (\bigcup_{i\in[p]\setminus J} \Phi_i)$ contains at most one element. With this assumption, we are reduced to the case of $|K| < \infty$.

It follows from (a) that $i + \langle t - 1\rangle$, where $i$ runs through $\mathrm{Diag}_\Phi$, are pairwise disjoint subsets of $\mathbb{Z}/p\mathbb{Z}$. This proves (b). □

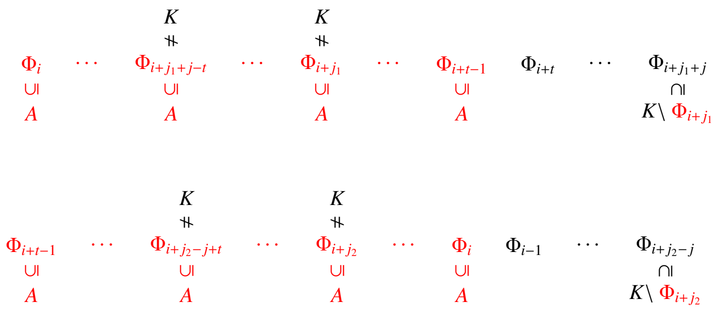


Figure 1: $j_1$ and $j_2$ as claimed in Lemma 3.5 (a). Note that $j \ge \max\{t - j_1, j_2 + 1\}$.

**Lemma 3.5.** *Let $K$ be a set and let $t \in \mathbb{N}$. For any cyclic decomposition $\Phi$ of $(K^t, K, t)$ with period $p \ge 2$, the following statements are valid.*

*(a) Take $i \in \mathrm{Diag}_\Phi$ and let $A \doteq \bigcap_{k\in\langle t-1\rangle} \Phi_{i+k} \neq \emptyset$. Then for every $j \in [t]$, there exist two (possibly equal) elements $j_1, j_2 \in \Phi^i_<$ such that $\Phi_{i+j_1} \cap \Phi_{i+j+j_1} = \Phi_{i+j_2} \cap \Phi_{i-j+j_2} = \emptyset$, that $\Phi_{i+j+j_1} \cap A = \Phi_{i-j+j_2} \cap A = \emptyset$ and that $\{j + j_1 - t, -j + j_2 + t\} \subseteq \Phi^i_< \subseteq \langle t - 1\rangle$.*

*(b) It holds $\Phi^\#_< \ge \frac{t}{\gcd(p,t)} \Upsilon(\gcd(p, t)) \ge \frac{t}{\gcd(p,t)} \left\lceil \sqrt{2\gcd(p, t) - \frac{7}{4}} + \frac{1}{2} \right\rceil$.*

*Proof.* (a). It follows from Theorem 1.4 (b) that $p \ge 2t > t \ge j$ and so, as $\Phi$ is a cyclic decomposition of $(K^t, K, t)$ with period $p$, we obtain $\Phi_{[i,i+t-1]} \cap \Phi_{[i+j,i+j+t-1]} = \emptyset$. This implies the existence of $j_1 \in \langle t - 1\rangle$ such that

$$\Phi_{i+j_1} \cap \Phi_{i+j+j_1} = \emptyset. \tag{7}$$

Since $A \subseteq \Phi_{i+j_1}$ we read from Eq. (7) that $\Phi_{i+j+j_1} \cap A = \emptyset$ and so $j + j_1 \notin \langle t - 1\rangle$. In view of Lemma 2.5, to show that $\{j_1, j + j_1 - t\} \subseteq \Phi^i_<$ we need to demonstrate $\Phi_{i+j_1} \neq K \neq \Phi_{i+j+j_1}$ and $j + j_1 - t \in \langle t - 1\rangle$. From $\Phi_{i+j+j_1} \neq \emptyset \neq \Phi_{i+j_1}$ we derive from Eq. (7) that $\Phi_{i+j_1} \neq K \neq \Phi_{i+j+j_1}$. Given $j_1 \in \langle t - 1\rangle$, $j \in [t]$ and $j + j_1 \notin \langle t - 1\rangle$, it is evident that $j + j_1 - t \in \langle t - 1\rangle$.

Let $\Psi$ be a reflection of $\Phi$ defined by $\Psi_\ell = \Phi_{2i+t-1-\ell}$ for all $\ell \in \mathbb{Z}/p\mathbb{Z}$. Note that $i \in \mathrm{Diag}_\Phi \cap \mathrm{Diag}_\Psi$ and $A = \bigcap_{k\in\langle t-1\rangle} \Phi_{i+k} = \bigcap_{k\in\langle t-1\rangle} \Psi_{i+k}$. What we have obtained above on the existence of $j_1$ is summarized on the top of Fig. 1. Replacing $\Phi$ by $\Psi$ then yields the bottom of Fig. 1, which demonstrates the existence of the required $j_2$.

(b). We put $\tau \doteq \gcd(p, t)$. When $\tau = 1$, we are done by Theorem 1.4 (b), Corollary 2.6 (b), and Lemma 3.2 (a). Let us proceed with the case of $\tau \ge 2$.

Pick $i \in \mathrm{Diag}_\Phi$ and let $T \doteq \tau - \partial_{\Phi^i_< \cap \langle \tau-1\rangle}$. For every $j \in [\tau]$, (a) ensures the existence of $j_2 \in \Phi^i_<$ such that $-j + j_2 + \tau = -(j + t - \tau) + j_2 + t \in \Phi^i_<$. It follows that $0 \le j_2 < -j + j_2 + \tau \le \tau - 1$, indicating that $j = \tau - (-j + j_2 + \tau) + j_2 \in T$. Consequently, we find that $T \supseteq [\tau]$, implying that $\partial_{\Phi^i_< \cap \langle \tau-1\rangle} = [\tau]$. By the definition of $\Upsilon$, this means that $|\Phi^i_< \cap \langle \tau - 1\rangle| \ge \Upsilon(\tau)$. Finally, the proof is completed by applying Corollary 2.6 (a) and Lemma 3.2 (b). □

**Corollary 3.6.** *Let $K$ be a set, let $t$ be a positive integer, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $p \ge 2$. For any $i \in \mathrm{Diag}_\Phi$, it holds $\Phi_{i-1} \cap \Phi_i = \Phi_{i+t-1} \cap \Phi_{i+t} = \emptyset$.*

*Proof.* This is obtained from Lemma 3.5 (a) by putting $j \doteq 1$. □

**Corollary 3.7.** *Let $K$ be a set, let $t \ge 2$ be an integer, and let $s \doteq \lfloor \frac{t}{2} \rfloor$. Let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period at least 2. Then, for every $j \in \mathbb{N}$ it holds $\Phi_{[j+1,j+s]} \ne K^s$.*

*Proof.* We assume without loss of generality that $1 \in \mathrm{Diag}_\Phi$ and that $A \doteq \bigcap_{j\in[t]} \Phi_j \ne \emptyset$. Corollary 3.6 shows that $\Phi_1 \ne K$ and $\Phi_t \ne K$. Therefore, it is sufficient to check that $\Phi_{[j+1,j+s]} \ne K^s$ for every $j \in [t-s-1] \subseteq [s]$.

We assume on the contrary that there exists $j \in [s]$ such that $\Phi_{[j+1,j+s]} = K^s$. By substituting $i \doteq 1$ and $j \doteq t - s$ in Lemma 3.5 (a), we derive the existence of $j_1, j_1' \in \Phi^1_<$ such that $j_1 - j_1' = s$. Since $\Phi_{[j+1,j+s]} = K^s$, it holds either $j + s < j_1' < j_1$ or $j_1' < j_1 \le j$. By symmetry, we assume that $j_1' < j_1 \le j$. Since $j \le s$ and $j_1' \ge 1$, it holds $s = j_1 - j_1' \le j - 1 < s$. This is a contradiction. □

**Lemma 3.8.** *For any positive integer $t$ and any $p \in \mathcal{PS}(t) \setminus \{1\}$, it holds that $p \ge 2^{\frac{t}{\gcd(p,t)}\left\lceil \sqrt{2\gcd(p,t) - \frac{7}{4}} + \frac{1}{2} \right\rceil}$.*

*Proof.* It follows from Theorem 2.11 and Lemma 3.5 (b) that $p \ge 2^{\Phi^\#_<} \ge 2^{\frac{t}{\gcd(p,t)}\left\lceil \sqrt{2\gcd(p,t) - \frac{7}{4}} + \frac{1}{2} \right\rceil}$. □

**Lemma 3.9.** *Let $t$ be a positive integer. If $p \in \mathcal{PS}(t) \setminus \{1\}$ and $\gcd(p,t) = 1$, then $p \ge 2^t$.*

*Proof.* It follows from $\gcd(p,t) = 1$ that

$$\frac{t}{\gcd(p,t)}\left\lceil \sqrt{2\gcd(p,t) - \frac{7}{4}} + \frac{1}{2} \right\rceil = t.$$

Therefore, the result is immediate from Lemma 3.8. □

*Proof of Theorem 1.5.* It is clear that we can pick $q \in \{2^t - 1, 2^t - 2, \dots, 2^t - \lfloor \frac{t}{2} \rfloor\}$ such that $\gcd(q,t) = 1$. Since $2^t > q > 1$, we then conclude from Lemma 3.9 $q \notin \mathcal{PS}(t)$, as wanted. □

*Proof of Theorem 1.6.* Take $p \in \mathcal{PS}(t) \setminus \{1\}$ and then set $\tau \doteq \gcd(p,t)$.

When $\tau = 1$, it follows from $t \ge 2$ and Lemma 3.9 that $p \ge 2^t$, and hence $p \ge 2^{\lceil \sqrt{2t} \rceil}$ when $t \ge 2$ and $p \ge 2^{\lceil 2\sqrt{t} \rceil}$ when $t \ge 4$. This verifies (a) and (b) when $\tau = 1$.

When $\tau \ge 2$, it holds that

$$\begin{aligned}
\frac{t}{\tau}\left\lceil \sqrt{2\tau - \frac{7}{4}} + \frac{1}{2} \right\rceil &= \frac{t}{\tau}\left\lceil \sqrt{2\tau - \frac{7}{4} + \sqrt{2\tau - \frac{7}{4}} + \frac{1}{4}} \right\rceil \qquad (8)\\
&\ge \frac{t}{\tau}\left\lceil \sqrt{2\tau - \frac{7}{4} + \sqrt{2\times 2 - \frac{7}{4}} + \frac{1}{4}} \right\rceil \qquad (\text{By } \tau \ge 2)\\
&= \frac{t}{\tau}\left\lceil \sqrt{2\tau} \right\rceil\\
&\ge \left\lceil \frac{\sqrt{2}t}{\sqrt{\tau}} \right\rceil. \qquad (\text{By } \tfrac{t}{\tau} \in \mathbb{N})
\end{aligned}$$

Since $\tau \le t$, we can finish a proof of (a) by applying (8) and Lemma 3.8.

In the case that $t \nmid p$, it holds $\tau \leq \frac{t}{2}$. Henceforth, when $\tau \geq 2$, we obtain from (8) that $\frac{t}{\tau}\left\lceil \sqrt{2\tau - \frac{7}{4}} + \frac{1}{2} \right\rceil \geq \left\lceil \frac{\sqrt{2}t}{\sqrt{\frac{t}{2}}} \right\rceil = \left\lceil 2\sqrt{t} \right\rceil$ and so (b) follows from Lemma 3.8.

It follows from (a) and (b) that $\mathcal{PS}(t) \cap [2, 2^{\lceil \sqrt{2t} \rceil} - 1] = \mathcal{PS}(t) \cap \left( [2^{\lceil \sqrt{2t} \rceil}, 2^{\lceil 2\sqrt{t} \rceil}] \setminus (t\mathbb{Z}) \right) = \emptyset$. Therefore, it holds $\mathrm{n}_{\mathcal{PS}(t)} \geq \left| [2, 2^{\lceil \sqrt{2t} \rceil} - 1] \right| + \left| [2^{\lceil \sqrt{2t} \rceil}, 2^{\lceil 2\sqrt{t} \rceil}] \setminus (t\mathbb{Z}) \right| \geq 2^{\lceil \sqrt{2t} \rceil} - 2 + \left\lfloor \frac{t-1}{t} (2^{\lceil 2\sqrt{t} \rceil} - 2^{\lceil \sqrt{2t} \rceil}) \right\rfloor$, hence proving (c). □

## 4. Upper bound of the Frobenius number: Rooted cyclic decomposition

Wu, Xu and Zhu introduced strong cyclic decomposition [WXZ17, p. 21] as a means of constructing a large cyclic decomposition by assembling several smaller combinatorial structures. We adapt it slightly to define rooted cyclic decompositions below.

**Definition 4.1** (Rooted cyclic decomposition)**.** Let $K$ be a set, $t \in \mathbb{N}$ and $X \subseteq K^t$. We say that a cyclic decomposition $\Phi$ of $(X, K, t)$ has $r \in K$ as its **root** provided $\Phi_i = \{r\}$ for all $i \in [t-1]$. A cyclic decomposition is **rooted** if it has a root. We define $\mathcal{P}^*(X, K, t)$ to be the set of periods of those cyclic decompositions of $(X, K, t)$; for any $r \in K$, we define $\mathcal{P}^*(X, K, t, r)$ to be the set of periods of those cyclic decompositions of $(X, K, t)$ rooted at $r$. We further define $\mathcal{P}^*(k, t) \doteq \mathcal{P}^*([k]^t, [k], t, 1)$ and $\mathcal{PS}^*(t) \doteq \bigcup_{k=1}^{\infty} \mathcal{P}^*(k, t)$.

We list in Lemma 4.2 some results from [WXZ17] about rooted cyclic decompositions. The statements in Lemmas 4.2 (a), 4.2 (c) and 4.2 (d) are weaker than the corresponding ones from [WXZ17]. These weaker claims are already sufficient for our application in this paper and save us from delving into more technical details.

**Lemma 4.2.** *(a) [WXZ17, Lemma 41] It holds $k^t \in \mathcal{P}^*(k, t)$ for all $k, t \in \mathbb{N}$.*

*(b) [WXZ17, Lemma 42(b)] Let $k_1$ and $k_2$ be two integers such that $1 < k_1 \leq k_2$. Then $\mathcal{P}^*(k_1, t) \subseteq \mathcal{P}^*(k_2, t)$ for every $t \in \mathbb{N}$.*

*(c) [WXZ17, Lemma 45] Let $K$ be a set and let $t \in \mathbb{N}$. Let $X$ and $Y$ be two disjoint subsets of $K^t$. Then $\mathcal{P}^*(X, K, t, r) + \mathcal{P}^*(Y, K, t, r) \subseteq \mathcal{P}^*(X \sqcup Y, K, t, r)$ for every $r \in K$.*

*(d) [WXZ17, Lemma 48] Let $t \geq 2$ be an integer. Then $3^t - 2^t + tc \in \mathcal{P}^*([c+3]^t \setminus [c+2]^t, [c+3], t, 1)$ holds for every nonnegative integer $c$.*

For any sets $Y, Z$ and any element $y$, let

$$\tau_{y,Y}(Z) = \begin{cases} Z, & \text{if } y \notin Z, \\ Z \cup Y, & \text{if } y \in Z. \end{cases}$$

That is, the map $\tau_{y,Y}$ applied on $Z$ substitutes $y$ with $\{y\} \cup Y$ whenever $y \in Z$.

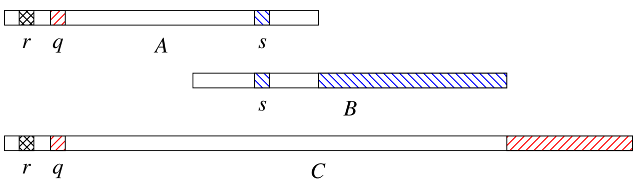



Figure 2: Proof of Lemma 4.3.

**Lemma 4.3.** *Let $A$, $B$ and $C$ be three sets satisfying $C \supseteq A \cup B$ and $A \cap B \neq \emptyset$.*

*(a) Assume that $A \setminus B \neq \emptyset$. For every $t \in \mathbb{N}$, it holds $\mathcal{P}^*(A^t \setminus (A \setminus B)^t, A, t) \subseteq \mathcal{P}^*(C^t \setminus (C \setminus B)^t, C, t)$.*

*(b) Assume $|A \setminus B| \geq 2$. Then, for every $t \in \mathbb{N}$ and $r \in A \setminus B$, it holds $\mathcal{P}^*(A^t \setminus (A \setminus B)^t, A, t, r) \subseteq \mathcal{P}^*(C^t \setminus (C \setminus B)^t, C, t, r)$.*

*Proof.* We only prove (b), and a proof of (a) can be given in the same manner. Let $\Phi$ be a cyclic decomposition of $(A^t \setminus (A \setminus B)^t, A, t)$ with period $p$ and rooted at $r$. Take $s \in A \cap B$ and $q \in (A \setminus B) \setminus \{r\}$. It is not hard to check that the map $\Psi$ with $\Psi_i = \tau_{s,B\setminus A} \circ \tau_{q,C\setminus(A\cup B)}(\Phi_i)$ for all $i \in \mathbb{Z}/p\mathbb{Z}$ is a cyclic decomposition of $(C^t \setminus (C \setminus B)^t, C, t)$ with period $p$ and rooted at $r$; see Fig. 2. Therefore, it holds $p \in \mathcal{P}^*(C^t \setminus (C \setminus B)^t, C, t, r)$. □

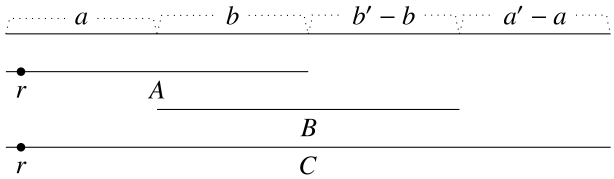



Figure 3: Proof of Lemma 4.4.

**Lemma 4.4.** *Consider $a, a', b, b' \in \mathbb{N}$ satisfying $2 \le a \le a'$ and $b \le b'$. Then it holds that $\mathcal{P}^*([a+b]^t \setminus [a]^t, [a+b], t, 1) \subseteq \mathcal{P}^*([a'+b']^t \setminus [a']^t, [a'+b'], t, 1)$.*

*Proof.* Let $A$, $B$ and $C$ be three sets satisfying $|A\setminus B| = a$, $|A\cap B| = b$, $|B\setminus A| = b'-b$, $C \supseteq A\cup B$ and $|C\setminus(A\cup B)| = a'-a$. Take $r \in A\setminus B$. Obviously, it holds $\mathcal{P}^*([a+b]^t \setminus [a]^t, [a+b], t, 1) = \mathcal{P}^*(A^t \setminus (A\setminus B)^t, A, t, r)$ and $\mathcal{P}^*([a'+b']^t \setminus [a']^t, [a'+b'], t, 1) = \mathcal{P}^*(C^t \setminus (C \setminus B)^t, C, t, r)$; see Fig. 3. The proof is now completed by applying Lemma 4.3 (b). □

For any $t, k \in \mathbb{N}$, let us define

$$\mathcal{Q}^*(k,t) \doteq \bigcup_{q=2}^{\infty} \mathcal{P}^*([q+k]^t \setminus [q]^t, [q+k], t, 1) \text{ and } \mathcal{QS}^*(t) \doteq \bigcup_{k=1}^{\infty} \mathcal{Q}^*(k,t). \tag{9}$$

**Lemma 4.5.** *Let $t$, $k_1$ and $k_2$ be three positive integers. Then the following hold true.*

*(a)* $\mathcal{Q}^*(k_1, 1) = [k_1]$.

*(b)* $\mathcal{Q}^*(k_1, t) \subseteq \mathcal{Q}^*(k_1+k_2, t)$.

*(c)* $\mathcal{Q}^*(k_1, t) + \mathcal{Q}^*(k_2, t) \subseteq \mathcal{Q}^*(k_1+k_2, t)$.

*Proof.* (a). For any $q \in \mathbb{N}$ and any $s \in [k_1]$, we can find disjoint nonempty sets $\Phi_1, \ldots, \Phi_s$ whose union is $[q+k_1]\setminus[q]$. It thus follows that $\mathcal{P}^*([q+k_1] \setminus [q], [q+k_1], 1, 1) = [k_1]$ for any $q \in \mathbb{N}$. The claim is now immediate from Eq. (9).

(b). For every $q \ge 2$, setting $a = a' = q$, $b = k_1$ and $b' = k_1 + k_2$ in Lemma 4.4 yields that $\mathcal{P}^*([q+k_1]^t \setminus [q]^t, [q+k_1], t, 1) \subseteq \mathcal{P}^*([q+k_1+k_2]^t \setminus [q]^t, [q+k_1+k_2], t, 1)$. According to Eq. (9), we obtain $\mathcal{Q}^*(k_1, t) \subseteq \mathcal{Q}^*(k_1+k_2, t)$.

(c). Let $p_1 \in \mathcal{Q}^*(k_1, t)$ and $p_2 \in \mathcal{Q}^*(k_2, t)$. Then there exist two integers $k_1' \ge k_1 + 2$ and $k_2' \ge k_2 + 2$ such that $p_1 \in \mathcal{P}^*([k_1']^t \setminus [k_1' - k_1]^t, [k_1'], t, 1)$ and $p_2 \in \mathcal{P}^*([k_2']^t \setminus [k_2' - k_2]^t, [k_2'], t, 1)$, respectively. Let $k' \doteq k_1' + k_2' \ge 6$. In light of Lemma 4.4, we then find that

$$\begin{cases} p_1 \in \mathcal{P}^*([k_1'+k_2'-k_2]^t \setminus [k_1'-k_1+k_2'-k_2]^t, [k_1'+k_2'-k_2], t, 1) = \mathcal{P}^*([k'-k_2]^t \setminus [k'-k_1-k_2]^t, [k'], t, 1), \\ p_2 \in \mathcal{P}^*([k_1'+k_2']^t \setminus [k_1'+k_2'-k_2]^t, [k_1'+k_2'], t, 1) = \mathcal{P}^*([k']^t \setminus [k'-k_2]^t, [k'], t, 1). \end{cases}$$

Finally, an application of Lemma 4.2 (c) shows that $p_1 + p_2 \in \mathcal{P}^*([k']^t \setminus [k'-k_1-k_2]^t, [k'], t, 1) \subseteq \mathcal{Q}^*(k_1+k_2, t)$. □

**Lemma 4.6.** *It holds $\mathcal{PS}^*(t) + \mathcal{QS}^*(t) \subseteq \mathcal{PS}^*(t)$ for all $t \in \mathbb{N}$.*

*Proof.* Take $p \in \mathcal{PS}^*(t)$ and $q \in \mathcal{QS}^*(t)$. Then we can find three integers $k_1$, $k_2$ and $k_3$ such that $k_1 \ge 1$, $k_2 > k_3 \ge 2$,

$$p \in \mathcal{P}^*([k_1]^t, [k_1], t, 1) \text{ and } q \in \mathcal{P}^*([k_2]^t \setminus [k_3]^t, [k_2], t, 1). \tag{10}$$

Let $k \doteq \max(k_1, k_3)$ and $k' \doteq k_2 + k - k_3$. By Lemma 4.2 (b), Eq. (10) gives $p \in \mathcal{P}^*([k]^t, [k], t, 1)$; substituting $a \doteq k_3$, $a' \doteq k$ and $b = b' \doteq k_2 - k_3$ in Lemma 4.4, it follows from Eq. (10) that $q \in \mathcal{P}^*([k']^t \setminus [k]^t, [k'], t, 1)$. Accordingly, as a consequence of Lemma 4.2 (c), $p + q \in \mathcal{P}^*([k]^t, [k], t, 1) \subseteq \mathcal{PS}^*(t)$, as desired. □

For any positive integers $d$ and $t$, the $t$-dimensional **De Bruijn digraph** on the symbol set $[d]$, denoted by $\mathrm{B}(d,t)$, is the digraph with vertex set $[d]^t$ and arc set $[d]^{t+1}$, where each arc $(s_1,\dots,s_{t+1})\in[d]^{t+1}$ has the initial vertex $(s_1,\dots,s_t)$ and the terminal vertex $(s_2,\dots,s_{t+1})$.

**Lemma 4.7** ([WXZ17, Lemma 47]). *Let $d\geq 2$ and $t\geq 2$ be two integers, and let $X\doteq[d+1]^t\setminus[d]^t$. Then there exists a discrete cyclic decomposition $\Delta$ of $(X,[d+1],t)$ such that $\Delta_i=\{d+1\}$ for all $i\in[2t-1]\setminus\{t\}$ and that $\Delta_t=\{d\}$.*

*Proof.* Let $H$ be the subdigraph of $\mathrm{B}(d+1,t-1)$ with vertex set $[d+1]^{t-1}$ and arc set $X$. Note that $H$ is strongly connected as for any two vertices $x=(x_1,\dots,x_{t-1})$ and $y=(y_1,\dots,y_{t-1})$ from $[d+1]^{t-1}$,

$$x\to(x_2,\dots,x_{t-1},d+1)\to(x_3,\dots,x_{t-1},d+1,y_1)\to(x_4,\dots,x_{t-1},d+1,y_1,y_2)\to\cdots\to(d+1,y_1,\dots,y_{t-2})\to y$$

is a walk from $x$ to $y$ in $H$. For each vertex $v$ of $\mathrm{B}(d+1,t-1)$, the number of arcs from $[d]^t$ with $v$ as the initial vertex is equal to the number of arcs from $[d]^t$ with $v$ as the terminal vertex. This implies that $H$ is Eulerian. For every $i\in[t]$, let $\sigma_i$ represent the word

$$(\underbrace{d+1,\dots,d+1}_{i-1},d,\underbrace{d+1,\dots,d+1}_{t-i})\in[d+1]^t,$$

and write $\Sigma$ for $\{\sigma_i:\ i\in[t]\}$. Note that going through the arcs $\sigma_t,\sigma_{t-1},\dots,\sigma_1$ in this order gives rise to a closed walk in $H$. We need to construct a discrete cyclic decomposition $\Delta$ of $(X,[d+1],t)$ satisfying $\{\sigma_t\}=\Delta_{[t]}$, that is, we aim to demonstrate the existence of an Eulerian cycle in $H$ containing the walk $\sigma_t,\sigma_{t-1},\dots,\sigma_1$. By the connectedness of $H$, this is ensured by the existence of an Eulerian cycle in $H-\Sigma$. In the case of $t=2$, the only arc of $H-\Sigma$ is the loop going from $d+1$ to itself and so we are done. As $H$ is Eulerian, it thus remains to illustrate that $H-\Sigma$ is strongly connected under the assumption of $t\geq 3$. Let

$$z\doteq(\underbrace{1,\dots,1}_{t-2},d+1)\in[d+1]^{t-1}.$$

Take $x=(x_1,\dots,x_{t-1})$ arbitrarily from $[d+1]^{t-1}$. We will construct in $H-\Sigma$ a walk $W_{x,z}$ from $x$ to $z$ and a walk $W_{z,x}$ from $z$ to $x$. For each $\ell\in\mathbb{N}_0$, let us designate by $W^\ell$ the set of all walks in $H-\Sigma$ of length $\ell$.

Case 1. $x\notin[d]^{t-1}$.

We can choose $W_{x,z}\in W^{t+2}$ to be

$$x\to(x_2,\dots,x_{t-1},1)\to(x_3,\dots,x_{t-1},1,d+1)\to(x_4,\dots,x_{t-1},1,d+1,1)\to(x_5,\dots,x_{t-1},1,d+1,1,1)\to\cdots$$
$$\to(x_i,\dots,x_{t-1},1,d+1,\underbrace{1,\dots,1}_{i-3})\to\cdots\to(1,d+1,\underbrace{1,\dots,1}_{t-3})\to(d+1,\underbrace{1,\dots,1}_{t-2})\to(\underbrace{1,\dots,1}_{t-1})\to z$$

and $W_{z,x}\in W^t$ to be

$$z\to(\underbrace{1,\dots,1}_{t-3},d+1,1)\to(\underbrace{1,\dots,1}_{t-4},d+1,1,x_1)\to\cdots\to(d+1,1,x_1,\dots,x_{t-3})\to(1,x_1,\dots,x_{t-2})\to x.$$

Note that $d\geq 2$ and $t\geq 3$ together ensures that the first two arcs of $W_{x,z}$ and the last two arcs of $W_{z,x}$ do not belong to $\Sigma$.

Case 2. $x\in[d]^{t-1}$.

We can check that the two walks $W_{x,z}\in W^{t+1}$ and $W_{z,x}\in W^{t-1}$ are what we are seeking for, where

$$\begin{aligned}W_{x,z}\doteq x&\to(x_2,\dots,x_{t-1},d+1)\to(x_3,\dots,x_{t-1},d+1,1)\to(x_4,\dots,x_{t-1},d+1,1,1)\\&\to\cdots\to(x_i,\dots,x_{t-1},d+1,\underbrace{1,\dots,1}_{i-2})\to\cdots\to(d+1,\underbrace{1,\dots,1}_{t-2})\to(\underbrace{1,\dots,1}_{t-1})\to z\end{aligned}$$

and

$$W_{z,x}\doteq z\to(\underbrace{1,\dots,1}_{t-3},d+1,x_1)\to(\underbrace{1,\dots,1}_{t-4},d+1,x_1,x_2)\to\cdots\to(d+1,x_1,\dots,x_{t-2})\to x.$$

We have used $d\geq 2$ and $t\geq 3$ here to guarantee that the first arc of $W_{x,z}$ and the last arc of $W_{z,x}$ do not belong to $\Sigma$, as well as even the existence of the first arc in $W_{z,x}$. □

*Remark* 4.8. If we let $t = 1$, the result in Lemma 4.7 trivially fails. If $t = 2$ and $d = 1$, the map $\Phi \in [2]^{\mathbb{Z}/3\mathbb{Z}}$ given by $\Delta_1 = \{2\}, \Delta_2 = \{1\}$ and $\Delta_3 = \{2\}$ is surely a discrete cyclic decomposition of $([2]^2 \setminus \{11\}, [2], 2)$.

Let us explain that Lemma 4.7 does not extend to the case of $d = 1$ and $t \geq 3$. Indeed, assume to the contrary that there is a discrete cyclic decomposition $\Delta$ of $([2]^t \setminus [1]^t, [2], t)$ with $\Delta_{[2t-1]} = (\underbrace{2, \ldots, 2}_{t-1}, 1, \underbrace{2, \ldots, 2}_{t-1})$. Note that the period of $\Delta$ is $2^t - 1 \geq 2t + 1$. Comparing $\Delta_{[t]}$ and $\Delta_{[t+1,2t]}$ yields $\Delta_{2t} = \{2\}$. We thus find that $\Delta_{[t-1]} = \Delta_{[t+1,2t-1]} = \Delta_{[t+2,2t]}$ and so $\Delta_{[t+2,2t+1]} \in \{\Delta_{[t]}, \Delta_{[t+1,2t]}\}$, which is absurd.

In the statement of [WXZ17, Lemma 47], the condition $d \geq 2$ is missing. Let $\Sigma$ be the subset of $[d+1]^t$ as defined in the proof of Lemma 4.7. In the proof of [WXZ17, Lemma 47], the authors first obtain a discrete cyclic decomposition $Q$ on $[d+1]^t \setminus (\Sigma \cup \{(\underbrace{d+1, d+1, \ldots, d+1}_{t})\})$ and then claim that one can obtain a discrete cyclic decomposition $[d+1]^t \setminus \Sigma$ from $Q$. This claim is not valid when $d = 1$. Fortunately, whenever [WXZ17, Lemma 47] is used throughout [WXZ17], the condition of $d > 1$ is always fulfilled.

**Lemma 4.9** ([Bra42, Theorem 1])**.** *Let $a_1 < a_2 < \cdots < a_n$ be $n$ positive integers with $\gcd(a_1, a_2, \ldots, a_n) = 1$. Then it holds $(a_1 - 1)(a_n - 1) + \mathbb{N}_0 \subseteq a_1\mathbb{N}_0 + a_2\mathbb{N}_0 + \cdots + a_n\mathbb{N}_0$.*

**Lemma 4.10.** *Let $t$ be a positive integer and let $k$ be the minimum integer satisfying $k \geq 3$ and $\gcd(t, 3^t - 2^t, \ldots, k^t - (k-1)^t) = 1$. Then for every $p \geq (t-1)(k^t - (k-1)^t - 1) + 3^t - 2^t$, it holds $p \in \mathcal{QS}^*(t)$.*

*Proof.* When $t = 1$, it follows from Lemma 4.5 (a) that $\mathcal{QS}^*(t) = \mathbb{N}$. We assume in the sequel that $t \geq 2$.

Let $n = k - 1$, $a_1 = t$ and $a_i = (i+1)^t - i^t$ for every $i \in [k-1] \setminus \{1\}$. An application of Lemma 4.9 leads to

$$p \in (3^t - 2^t + t\mathbb{N}_0) + (3^t - 2^t)\mathbb{N}_0 + \cdots + (k^t - (k-1)^t)\mathbb{N}_0. \tag{11}$$

By Lemma 4.2 (d), we have $3^t - 2^t + tc \in \mathcal{Q}^*(1, t)$ for all $c \in \mathbb{N}_0$. It follows from Lemma 4.7 that $(d+1)^t - d^t \in \mathcal{P}^*([d+1]^t \setminus [d]^t, [d+1], t, 1) \subseteq \mathcal{Q}^*(1, t)$ for every $d = 2, \ldots, k-1$. This combined with Lemma 4.5 (c) implies that

$$(3^t - 2^t + t\mathbb{N}_0) + (3^t - 2^t)\mathbb{N}_0 + \cdots + (k^t - (k-1)^t)\mathbb{N}_0 \subseteq \mathcal{QS}^*(t).$$

Taking into account Eq. (11), this completes the proof. □

**Lemma 4.11.** *Let $t \in \mathbb{N}$ and let $k$ be the minimum integer satisfying $k \geq 3$ and $\gcd(t, 3^t - 2^t, \ldots, k^t - (k-1)^t) = \gcd(t, 3^t - 2^t, 4^t - 2^t, \ldots, k^t - 2^t) = 1$. Then $(t-1)(k^t - (k-1)^t - 1) + 3^t + \mathbb{N}_0 \subseteq \mathcal{PS}^*(t)$, namely $g_{\mathcal{PS}^*(t)} \leq (t-1)(k^t - (k-1)^t - 1) + 3^t - 1$.*

*Proof.* It holds

$$\begin{aligned} 2^t + ((t-1)(k^t - (k-1)^t - 1) + 3^t - 2^t + \mathbb{N}_0) &\subseteq \mathcal{P}^*(2, t) + \mathcal{QS}^*(t) && \text{(By Lemmas 4.2 (a) and 4.10)} \\ &\subseteq \mathcal{PS}^*(t) + \mathcal{QS}^*(t) \\ &\subseteq \mathcal{PS}^*(t), && \text{(By Lemma 4.6)} \end{aligned}$$

as wanted. □

*Proof of Theorem 1.7.* This follows directly from Lemma 4.11 and the fact that $\mathcal{PS}^*(t) \subseteq \mathcal{PS}(t)$ for all $t \in \mathbb{N}$. □

**Lemma 4.12.** *Let $t \geq 2$ be an integer, let $p$ be the largest prime divisor of $t$, and let $k \doteq \max(p, 3)$. Then $(t-1)(k^t - (k-1)^t - 1) + 3^t + \mathbb{N}_0 \subseteq \mathcal{PS}(t)$, namely $g_{\mathcal{PS}(t)} \leq (t-1)(k^t - (k-1)^t - 1) + 3^t - 1$.*

*Proof.* If $\gcd(t, 3^t - 2^t, \ldots, k^t - (k-1)^t) = 1$, we can employ Theorem 1.7 to conclude the proof. Thus, we may assume that $t'$ is a prime factor of $g \doteq \gcd(t, 3^t - 2^t, \ldots, k^t - (k-1)^t)$ and aim to derive a contradiction. Note that $t' \leq p \leq k$. If $t' \geq 3$, from $t' \mid g$ we deduce $t' \mid ((t')^t - (t'-1)^t)$, which is absurd. If $t' = 2$, from $t' \mid g$ we deduce $t' \mid (3^t - 2^t)$, which is again impossible. □

**Lemma 4.13.** *For each prime number $t$, it holds $(t-1)(3^t - 2^t - 1) + 3^t + \mathbb{N}_0 \subseteq \mathcal{PS}(t)$, namely $g_{\mathcal{PS}(t)} \leq (t-1)(3^t - 2^t - 1) + 3^t - 1$.*

*Proof.* Since $\gcd(t, 3^t - 2^t) = 1$, we can substitute $k \doteq 3$ in Theorem 1.7 to obtain the desired result. □

*Proof of Corollary 1.8.* Combine Lemmas 4.12 and 4.13. □

## 5. Height

**Definition 5.1** (Height)**.** Let $K$ be a set, let $t$ be a positive integer, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$. For any $a \in K$, let $\xi_{\Phi,a}$ be the set $\{s \in [t] : \bigsqcup_{j'=j-s}^{j} \Phi_{[j',j'+s-1]} = K^s\}$, where $j = \mathrm{Loc}_\Phi(a^t)$, and let

$$\mathrm{h}_{\Phi,a} = \begin{cases} 0, & \text{if } \xi_{\Phi,a} = \emptyset, \\ \max \xi_{\Phi,a}, & \text{else.} \end{cases}$$

We call $\mathrm{h}_{\Phi,a}$ the **height** of $a \in K$ in the cyclic decomposition $\Phi$. Assume that $A$ is a nonempty subset of $K$ satisfying $\mathrm{Loc}_\Phi(a^t) = \mathrm{Loc}_\Phi(b^t)$ for all $a, b \in A$. We adopt the notation $\mathrm{h}_{\Phi,A}$ for this common value of $\mathrm{h}_{\Phi,a}$, $a \in A$. Recall from Remark 2.3 a related notation of $\mathrm{Loc}_\Phi(A^t)$.

Lemma 5.2 provides several different characterizations of the height function of a cyclic decomposition of order $t \geq 2$. After that, we shall further develop some tools from the perspective of the height function that are useful in establishing nonexistence results for cyclic decompositions.

**Lemma 5.2.** *Let $K$ be a set, let $t, p \in \mathbb{N} \setminus \{1\}$, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $p$. Take $j \in \mathrm{Diag}_\Phi$, $A \in \binom{\bigcap_{i=j}^{j+t-1} \Phi_i}{>0}$ and $q \doteq \mathrm{h}_{\Phi,A} \leq t$. Let $\Sigma = \Phi_j \times \Phi_{j+1} \times \cdots \times \Phi_{j+t-q-1} \cup \cdots \cup \Phi_{j+q} \times \Phi_{j+q+1} \times \cdots \times \Phi_{j+t-1}$ and let $\Sigma' = \Phi_j \times \Phi_{j+1} \times \cdots \times \Phi_{j+t-q-2} \cup \cdots \cup \Phi_{j+q+1} \times \Phi_{j+q+2} \times \cdots \times \Phi_{j+t-1}$.*

- *(a) It holds $\mathrm{Loc}_\Phi(x) \cap (j + s + [t-s]) = \emptyset$ for every $s \in \langle t-1 \rangle$ and every $x \in A^{t-s}$.*
- *(b) For any $x \in A^{t-q}$, it holds that $\mathrm{Loc}_\Phi(x) \subseteq j + \langle q \rangle$; for any $y \in A^{t-q-1}$, it holds that $\mathrm{Loc}_\Phi(y) \setminus (j + \langle q+1 \rangle) \neq \emptyset$.*
- *(c) For any $x \in A^{t-q}$, it holds that $x \notin (\bigcup_{k \in \mathbb{Z}/p\mathbb{Z}} \Phi_k \times \Phi_{k+1} \times \cdots \times \Phi_{k+t-q-1}) \setminus \Sigma$; for any $y \in A^{t-q-1}$, it holds $y \in (\bigcup_{k \in \mathbb{Z}/p\mathbb{Z}} \Phi_k \times \Phi_{k+1} \times \cdots \times \Phi_{k+t-q-2}) \setminus \Sigma'$.*
- *(d) Let $\Psi_i \doteq \Phi_{2j+t-1-i}$ for every $i \in \mathbb{Z}/p\mathbb{Z}$. Then we have $\mathrm{h}_{\Psi,A} = \mathrm{h}_{\Phi,A} = q$.*
- *(e) Take $s \in \langle t-1 \rangle$ and $x \in A^{t-s}$. It holds $\mathrm{Loc}_\Phi(x) \subseteq j + \langle s \rangle$ if and only if $s \in \langle q \rangle$.*
- *(f) For every $s \in [t]$, $q \geq s$ if and only if $\bigsqcup_{j'=j-s}^{j} \Phi_{[j',j'+s-1]} = K^s$.*
- *(g) For every $s \in [t]$, $q \geq s$ if and only if $\bigsqcup_{j'=j-s}^{j} \Phi_{[t+j',t+j'+s-1]} = K^s$.*
- *(h) It holds that $\xi_{\Phi,a} = [\mathrm{h}_{\Phi,a}] = [\mathrm{h}_{\Phi,A}]$ for every $a \in A$.*

*Proof.* (a). According to Corollary 3.6, it follows from $j \in \mathrm{Diag}_\Phi$ that $\Phi_{j+t-1} \cap \Phi_{j+t} = \emptyset$. We pick $i \in [t-s]$. Then, from $x_i \in A \subseteq \Phi_{j+t-1}$ we obtain that $x_i \notin \Phi_{j+t}$. As a result, it holds $x \notin \Phi_{[j+t-i+1,j+2t-i-s]}$, and hence $j + t - i + 1 \notin \mathrm{Loc}_\Phi(x)$. We now see that $\mathrm{Loc}_\Phi(x) \cap [j+s+1, j+t] = \emptyset$, as desired.

(b). By Theorem 1.4 (b), we deduce from $t \geq 2$ that

$$q \in \langle t-1 \rangle. \tag{12}$$

Since $p \geq 2$, it follows from Theorem 1.4 (b) and Eq. (12) that

$$p \geq 2t \geq 2(q+1) > 2q+1 \geq q+1. \tag{13}$$

Take $\{j', j''\} \in \binom{[j-q-1,j]}{2}$. By Eq. (13), $p > q + 1 \geq |j'' - j'|$. Accordingly, we find that $\Phi_{[j',j'+t-1]} \cap \Phi_{[j'',j''+t-1]} = \emptyset$. Because $A \in \binom{\bigcap_{i=j}^{j+t-1} \Phi_i}{>0}$ and $j \in \mathrm{Diag}_\Phi$, it holds $\Phi_{[j'+q+1,j'+t-1]} \cap \Phi_{[j''+q+1,j''+t-1]} \supseteq A^{t-q-1} \neq \emptyset$. We thus arrive at

$$\Phi_{[j',j'+q]} \cap \Phi_{[j'',j''+q]} = \emptyset. \tag{14}$$

Making use of $A \in \binom{\bigcap_{i=j}^{j+t-1} \Phi_i}{>0}$ and $j \in \mathrm{Diag}_\Phi$ again, we find that

$$x \in A^{t-q} \subseteq \bigcap_{j'=j-q}^{j} \Phi_{[j'+q,j'+t-1]}. \tag{15}$$

Consequently, the definition of $\mathrm{h}_{\Phi,A}$ ensures that

$$\bigsqcup_{j'=j-q}^{j} \Phi_{[j',j'+q-1]} = K^q \tag{16}$$

and, in view of Eq. (14), that

$$\bigsqcup_{j'=j-q-1}^{j} \Phi_{[j',j'+q]} \subsetneq K^{q+1}. \tag{17}$$

By Eqs. (15) and (16), $K^q \times x \subseteq (\bigsqcup_{j'=j-q}^{j} \Phi_{[j',j'+q-1]}) \times (\bigcap_{j'=j-q}^{j} \Phi_{[j'+q,j'+t-1]}) \subseteq \bigsqcup_{j'=j-q}^{j} \Phi_{[j',j'+t-1]}$. This proves that $\mathrm{Loc}_\Phi(x) \subseteq j + \langle q\rangle$. By Eq. (17), $K^{q+1} \times y \nsubseteq \bigsqcup_{j'=j-q-1}^{j} \Phi_{[j',j'+t-1]}$, which implies that $\mathrm{Loc}_\Phi(y) \setminus (j + \langle q+1\rangle) \neq \emptyset$.

(c). This is immediate from (b).

(d). By the symmetry between $\Sigma$ and $\Sigma'$ with respect to $\Psi$ and $\Phi$, (c) enables us to get this claim.

(e). We first consider the case of $s \in \langle q\rangle$. Pick $i \in \langle q - s\rangle$ and let $x = x_1x_2x_3$ where $x_1 \in A^i$, $x_2 \in A^{t-q}$ and $x_3 \in A^{q-s-i}$. The first part of (b) asserts that $\mathrm{Loc}_\Phi(x) + i \subseteq \mathrm{Loc}_\Phi(x_1) \subseteq j + \langle q\rangle$, and hence $\mathrm{Loc}_\Phi(x) \subseteq j + \langle q\rangle - i$ follows. Eq. (13) ensures that $p > 2q + 1$, and so we have $j + q + 1 \notin j + [-q, q] \supseteq (j + \langle q\rangle) \cup (j + [s - q, s])$, namely $(j+\langle q\rangle)\cap(j+[s-q, s]) = j+\langle s\rangle$. We thus obtain $\mathrm{Loc}_\Phi(x) \subseteq \bigcap_{i\in\langle q-s\rangle}(j+\langle q\rangle-i) \subseteq (j+\langle q\rangle)\cap(j+[s-q, s]) = j+\langle s\rangle$, as wanted.

Then we turn to the case of $s \in \langle t-1\rangle \setminus \langle q\rangle$. We fix $a \in A$ and put $x' = xa^{s-q-1} \in A^{t-q-1}$. By the second part of (b), we have $\mathrm{Loc}_\Phi(x') \nsubseteq j + \langle q + 1\rangle$. This along with (a) says that $\mathrm{Loc}_\Phi(x') \nsubseteq j + \langle t - 1\rangle \supseteq j + \langle s\rangle$. Since $x' = xa^{s-q-1}$, we are ready to conclude that $\mathrm{Loc}_\Phi(x) \nsubseteq j + \langle s\rangle$, completing a proof of (e).

(f) and (g). Since $t \geq 2$, Theorem 1.4 (b) tells us that $\bigsqcup_{j'=j-t}^{j} \Phi_{[j',j'+t-1]} \neq K^t$ and that $\bigsqcup_{j'=j-t}^{j} \Phi_{[j'+t,j'+2t-1]} \neq K^t$. By virtue of Eq. (12), we get both (f) and (g) for the case of $s = t$.

Take $s \in [t-1]$ and $x \in A^{t-s}$. It is obvious that $j+\langle s\rangle \subseteq \mathrm{Loc}_\Phi(x)$. Therefore, (e) says that $\mathrm{Loc}_\Phi(x) = j+\langle s\rangle$ if and only if $s \in \langle q\rangle$. It is evident that both (f) and (g) are now consequences of Lemma 2.4.

(h). Let $a \in A$. It follows from Definition 5.1 and (f) that $s \in \xi_{\Phi,a}$ for every $s \in [\mathrm{h}_{\Phi,a}]$. As a result, it holds $\xi_{\Phi,a} = [\mathrm{h}_{\Phi,a}]$. □

**Lemma 5.3.** *Let $K$ be a set and $\Phi$ be a cyclic decomposition of $(K^3, K, 3)$ with period $p \geq 3$. Let $j \in \mathrm{Diag}_\Phi$, $\ell \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{j, j+1, j+2\}$, $A \doteq \bigcap_{i=j}^{j+2} \Phi_i$ and $B \doteq \bigcap_{i=\ell}^{\ell+2} \Phi_i$. Assume that $\mathrm{h}_{\Phi,A} \geq 1$. Then the following hold.*

- *(a) If $\Phi_\ell \cap A \neq \emptyset$, then $\Phi_{\ell-1} \cap A = \Phi_{\ell+1} \cap A = \emptyset$.*
- *(b) $\Phi_{\ell-1} \cap \Phi_\ell \cap A = \Phi_\ell \cap \Phi_{\ell+1} \cap A = \emptyset$.*
- *(c) Assume $\Phi_\ell \cap A \neq \emptyset$. Then $\Phi_\ell \supseteq A$ provided either $\Phi_\ell \sqcup \Phi_{\ell+1} = K$ or $\Phi_\ell \sqcup \Phi_{\ell-1} = K$.*
- *(d) If $\mathrm{Diag}_\Phi = \{j, \ell\}$, then $\Phi_\ell = \Phi_{\ell+2} = B$.*
- *(e) If $\mathrm{Diag}_\Phi = \{j, \ell\}$ and $\mathrm{h}_{\Phi,B} \geq 1$, then $\Phi_\ell = \Phi_{\ell+2} = \Phi_{j-1} = \Phi_{j+3} = B$ and $\Phi_{\ell-1} = \Phi_{\ell+3} = \Phi_j = \Phi_{j+2} = A$.*

*Proof.* (a). The assumption of $\mathrm{h}_{\Phi,A} \geq 1$ allows us to substitute $s = 1$ in Lemma 5.2 (e) and then find that both $A^2 \cap \Phi_{[\ell-1,\ell]}$ and $A^2 \cap \Phi_{[\ell,\ell+1]}$ are empty. Since $\Phi_\ell \cap A \neq \emptyset$, we must have $\Phi_{\ell-1} \cap A = \Phi_{\ell+1} \cap A = \emptyset$.

(b). This is immediate from (a).

(c). We see from (a) that $\Phi_{\ell-1} \cap A = \Phi_{\ell+1} \cap A = \emptyset$. Henceforth, $\Phi_\ell \sqcup \Phi_{\ell+1} = K$ implies $\Phi_\ell = K \setminus \Phi_{\ell+1} \supseteq A$, and $\Phi_\ell \sqcup \Phi_{\ell-1} = K$ implies $\Phi_\ell = K \setminus \Phi_{\ell-1} \supseteq A$.

(d). By definition, we have $B \subseteq \Phi_\ell \cap \Phi_{\ell+2}$. So, as $A = K \setminus B$, it remains to show $\Phi_\ell \cap A = \Phi_{\ell+2} \cap A = \emptyset$.

Note that $\Phi_{[j,j+1]} \cap \Phi_{[j+1,j+2]} \supseteq A^2$ implies $\Phi_{j-1} \cap A \subseteq \Phi_{j-1} \cap \Phi_j = \emptyset$; in the same vein, we deduce from $\Phi_{[j,j+1]} \cap \Phi_{[j+1,j+2]} \supseteq A^2$ that $A \cap \Phi_{j+3} \subseteq \Phi_{j+2} \cap \Phi_{j+3} = \emptyset$.

By virtue of Lemma 3.4 (a), $\{j, j+1, j+2\} \cap \{\ell, \ell+1, \ell+2\} = \emptyset$. So, our task is to verify that $\Phi_\ell \cap A = \emptyset$ when $\ell - 1 \notin \{j, j+1, j+2\}$ and that $\Phi_{\ell+2} \cap A = \emptyset$ when $\ell + 3 \notin \{j, j+1, j+2\}$. But Corollary 3.6 implies that $\Phi_{\ell-1} \subseteq K \setminus \Phi_\ell \subseteq K \setminus B = A$ and $\Phi_{\ell+3} \subseteq K \setminus \Phi_{\ell+2} \subseteq K \setminus B = A$. This says that we can apply (a), replacing $\ell$ by $\ell - 1$ and $\ell + 3$ respectively, and then complete the proof.

(e). Recall from (d) that $\Phi_\ell = \Phi_{\ell+2} = B$. Taking into account $\ell \in \mathrm{Diag}_\Phi$ and $\mathrm{h}_{\Phi,B} \geq 1$, Lemma 5.2 (f) then tells us $\Phi_{\ell-1} = K \setminus \Phi_\ell = A$ while Lemma 5.2 (g) gives us $\Phi_{\ell+3} = K \setminus \Phi_{\ell+2} = A$.

Swapping the role of $j$ and $\ell$, the same argument shows that $\Phi_j = \Phi_{j+2} = A$ and $\Phi_{j-1} = \Phi_{j+3} = B$. □

**Lemma 5.4.** *Let $K$ be a set, let $t \geq 2$ be an integer, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$. Then it holds $\mathrm{h}_{\Phi,x} = \mathrm{h}_{\Phi,y}$ for any $x, y \in K$ satisfying $\mathrm{Loc}_\Phi(x^t) = \mathrm{Loc}_\Phi(y^t) + t$.*

*Proof.* Let $p$ be the period of $\Phi$. There is nothing to prove when $p = 1$. We thus assume $p > 1$. Let $\mathrm{h}_{\Phi,x} = q$, $\mathrm{h}_{\Phi,y} \doteq q'$, $j \doteq \mathrm{Loc}_\Phi(x^t)$ and $j' \doteq \mathrm{Loc}_\Phi(y^t) = j - t$. Note that

$$\begin{aligned}\bigsqcup_{\ell=j'-q}^{j'} \Phi_{[\ell+t,\ell+t+q-1]} &= \bigsqcup_{\ell=j'+t-q}^{j'+t} \Phi_{[\ell,\ell+q-1]} \\ &= \bigsqcup_{\ell=j-q}^{j} \Phi_{[\ell,\ell+q-1]} \\ &= K^q. && \text{(By Lemma 5.2 (f))}\end{aligned}$$

Consequently, Lemma 5.2 (g) allows us to get $q \leq q'$. By symmetry, we also have $q' \leq q$ and so the result follows. □

Whenever we have a ground set in mind, for each subset $K$ of that ground set, we use $\mathbb{1}_K$ to denote the characteristic function of $K$, whose domain is the implicit ground set that the reader should have no difficulty recognizing from the context.

**Lemma 5.5.** *Let $K$ be a set, let $t \geq 2$ be an integer, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with $\mathrm{h}_{\Phi,A} \geq 1$ for $A \doteq \bigcap_{i\in[t]} \Phi_i \neq \emptyset$. Then the following statements hold.*

*(a) There exists a nonempty subset $B$ of $K \setminus A$ such that it holds either*

$$\Phi_i = \begin{cases} K, & \text{if } -(\mathrm{h}_{\Phi,A} - 1) \leq i \leq -1 \\ B, & \text{if } i = 0 \\ K \setminus B, & \text{if } 1 \leq i \leq \mathrm{h}_{\Phi,A} \end{cases}$$

*or*

$$\Phi_i = \begin{cases} B, & \text{if } -(\mathrm{h}_{\Phi,A} - 1) \leq i \leq 0 \\ K \setminus B, & \text{if } i = 1 \\ K, & \text{if } 2 \leq i \leq \mathrm{h}_{\Phi,A}. \end{cases}$$

*(b) There exists a nonempty subset $C$ of $K \setminus A$ such that it holds either*

$$\Phi_{t+i} = \begin{cases} K, & \text{if } 2 \leq i \leq \mathrm{h}_{\Phi,A} \\ C, & \text{if } i = 1 \\ K \setminus C, & \text{if } -(\mathrm{h}_{\Phi,A} - 1) \leq i \leq 0 \end{cases}$$

*or*

$$\Phi_{t+i} = \begin{cases} C, & \text{if } 1 \leq i \leq \mathrm{h}_{\Phi,A} \\ K \setminus C, & \text{if } i = 0 \\ K, & \text{if } -(\mathrm{h}_{\Phi,A} - 1) \leq i \leq -1. \end{cases}$$

*Proof.* Let $p$ be the period of $\Phi$. From $\mathrm{h}_{\Phi,A} \geq 1$, we get that $p > 1$. By virtue of Lemma 5.2 (d), the two statements (a) and (b) have an apparent symmetry, which means that we only need to establish the validity of one of them, say (a).

Let $B \doteq \Phi_0 \neq \emptyset$. According to Lemma 5.2 (f), it follows from $\mathrm{h}_{\Phi,A} \geq 1$ that $\Phi_0 \sqcup \Phi_1 = K$, and so $\emptyset \neq \Phi_1 = K \setminus B$.

If $\mathrm{h}_{\Phi,A} \geq 2$, we know from Lemma 5.2 (f) that $\Phi_{[-1,0]} \sqcup \Phi_{[0,1]} \sqcup \Phi_{[1,2]} = K^2$. Since the deflation number of $\Phi_{[0,1]}$ in $K^2$ is 2, Theorem 2.8 implies that one of $\Phi_{-1}$ and $\Phi_2$ must be $K$. They cannot be equal to $K$ simultaneous, as it gives $\Phi_{[-1,0]} \cap \Phi_{[1,2]} \neq \emptyset$. Therefore, we find that (1) holds with equality. In view of Theorem 2.8 again, by checking the two 2-boxes $\Phi_{[-1,0]} = \Phi_{-1} \times B$ and $\Phi_{[1,2]} = (K \setminus B) \times \Phi_2$, we know that either $\Phi_{-1} \sqcup (K \setminus B) = K$ or $B \sqcup \Phi_2 = K$. To sum up, we have either $(\Phi_{-1}, \Phi_2) = (K, K \setminus B)$ or $(\Phi_{-1}, \Phi_2) = (B, K)$.

Case 1. $(\Phi_{-1}, \Phi_2) = (K, K \setminus B)$.

Assume that for some integer $r$ with $2 \leq r \leq \mathrm{h}_{\Phi,A} - 1$ we have known that $(\Phi_{-i}, \Phi_{1+i}) = (K, K \setminus B)$ for all $i \in [r-1]$. Let us show that $(\Phi_{-r}, \Phi_{1+r}) = (K, K \setminus B)$. Surely, whenever this can be accomplished, we have completed a proof of the lemma by induction.

For any $j' \in [-r, 1]$, let $d_{j'} = \mathrm{DM}(\Phi_{j'}, \ldots, \Phi_{j'+r}; K, \ldots, K)$. Note that

$$d_{-g} = \mathrm{DM}(\Phi_{-g}, \ldots, \Phi_{-g+r}; K, \ldots, K) = \mathrm{DM}(\underbrace{K, \ldots, K}_{g}, B, \underbrace{K \setminus B, \ldots, K \setminus B}_{r-g}; K, \ldots, K) = r - g + 1$$

for all $g \in \langle r-1 \rangle$. Moreover, we have

$$d_{-r} = \mathrm{DM}(\Phi_{-r}, \ldots, \Phi_0; K, \ldots, K) = \mathrm{DM}(\Phi_{-r}, \underbrace{K, \ldots, K}_{r-1}, B; K, \ldots, K) = 1 + \mathbb{1}_{\Phi_{-r} \neq K}$$

and

$$d_1 = \mathrm{DM}(\Phi_1, \ldots, \Phi_{1+r}; K, \ldots, K) = \mathrm{DM}(\underbrace{K \setminus B, \ldots, K \setminus B}_{r}, \Phi_{1+r}, ; K, \ldots, K) = r + \mathbb{1}_{\Phi_{1+r} \neq K}.$$

Applying Lemma 5.2 (f) for $s = r + 1 \leq \mathrm{h}_{\Phi,A}$ and $j = 1$, we find that $\bigsqcup_{j'=-r}^{1} \Phi_{[j', j'+r]} = K^{r+1}$. Then we further infer from Theorem 2.8 that

$$1 \leq \sum_{j'=-r}^{1} 2^{-d_{j'}} = 2^{-(r + \mathbb{1}_{\Phi_{1+r} \neq K})} + 2^{-(1 + \mathbb{1}_{\Phi_{-r} \neq K})} + (1 - 2^{-1} - 2^{-(r+1)}). \tag{18}$$

As $r \geq 2$, (18) holds only if $\mathbb{1}_{\Phi_{-r} \neq K} = 0$, namely $\Phi_{-r} = K$. Since $\Phi_{[-r,0]} \cap \Phi_{[1,1+r]} = \emptyset$, we obtain $\Phi_{1+r} \neq K$. Consequently, (18) holds with equality. Examining the two $(r+1)$-boxes, $\Phi_{[-r,0]}$ and $\Phi_{[1,1+r]}$, Theorem 2.8 now gives us $B \sqcup \Phi_{1+r} = \Phi_0 \sqcup \Phi_{1+r} = K$, as desired.

Case 2. $(\Phi_{-1}, \Phi_2) = (B, K)$.

To complete the proof, as in the last case, we need to show that $(\Phi_{-r}, \Phi_{1+r}) = (B, K)$ for any $r$ satisfying $2 \leq r \leq \mathrm{h}_{\Phi,A} - 1$, under the assumption that $(\Phi_{-i}, \Phi_{1+i}) = (B, K)$ for all $i \in [r-1]$.

For any $j' \in [-r, 1]$, let $d_{j'} = \mathrm{DM}(\Phi_{j'}, \ldots, \Phi_{j'+r}; K, \ldots, K)$. Note that

$$d_{-g} = \mathrm{DM}(\Phi_{-g}, \ldots, \Phi_{-g+r}; K, \ldots, K) = \mathrm{DM}(\underbrace{B, \ldots, B}_{g+1}, K \setminus B, \underbrace{K, \ldots, K}_{r-g-1}; K, \ldots, K) = g + 2$$

for all $g \in \langle r-1 \rangle$. Moreover, we have

$$d_{-r} = \mathrm{DM}(\Phi_{-r}, \ldots, \Phi_0; K, \ldots, K) = \mathrm{DM}(\Phi_{-r}, \underbrace{B, \ldots, B}_{r}; K, \ldots, K) = r + \mathbb{1}_{\Phi_{-r} \neq K}$$

and

$$d_1 = \mathrm{DM}(\Phi_1, \ldots, \Phi_{1+r}; K, \ldots, K) = \mathrm{DM}(K \setminus B, \underbrace{K, \ldots, K}_{r-1}, \Phi_{1+r}; K, \ldots, K) = 1 + \mathbb{1}_{\Phi_{1+r} \neq K}.$$

Applying Lemma 5.2 (f) for $s = r + 1 \leq \mathrm{h}_{\Phi,A}$ and $j = 1$, we find that $\bigsqcup_{j'=-r}^{1} \Phi_{[j', j'+r]} = K^{r+1}$. Then we further infer from Theorem 2.8 that

$$1 \leq \sum_{j'=-r}^{1} 2^{-d_{j'}} = 2^{-(1 + \mathbb{1}_{\Phi_{1+r} \neq K})} + 2^{-(r + \mathbb{1}_{\Phi_{-r} \neq K})} + (1 - 2^{-1} - 2^{-(r+1)}). \tag{19}$$

As $r \geq 2$, (19) holds only if $\mathbb{1}_{\Phi_{1+r} \neq K} = 0$, namely $\Phi_{1+r} = K$. Since $\Phi_{[-r,0]} \cap \Phi_{[1,r+1]} = \emptyset$, we obtain $\Phi_{-r} \neq K$. Consequently, (19) holds with equality. Having a look at the two $(r+1)$-boxes, $\Phi_{[-r,0]}$ and $\Phi_{[1,r+1]}$, Theorem 2.8 now gives us $\Phi_{-r} \sqcup (K \setminus B) = \Phi_{-r} \sqcup \Phi_1 = K$, as wanted. □

**Lemma 5.6.** *Let $K$ be a set, let $t$ be an integer with $t \geq 2$, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$. Let $j \in \mathrm{Diag}_\Phi$, and let $A \doteq \bigcap_{i=j}^{j+t-1} \Phi_i$. If $\mathrm{h}_{\Phi,A} \geq 1$, then there exist two nonempty subsets $D$ and $E$ of $K \setminus A$ such that either*

$$\begin{cases} \Phi_{[j-\mathrm{h}_{\Phi,A},\, j+\mathrm{h}_{\Phi,A}-1]} = K^{\mathrm{h}_{\Phi,A}-1} \times D \times (K \setminus D)^{\mathrm{h}_{\Phi,A}}, \\ \Phi_{[j+t-\mathrm{h}_{\Phi,A},\, j+t+\mathrm{h}_{\Phi,A}-1]} = K^{\mathrm{h}_{\Phi,A}-1} \times (K \setminus E) \times E^{\mathrm{h}_{\Phi,A}} \end{cases} \tag{20}$$

*or*

$$\begin{cases} \Phi_{[j-\mathrm{h}_{\Phi,A},\, j+\mathrm{h}_{\Phi,A}-1]} = (K \setminus D)^{\mathrm{h}_{\Phi,A}} \times D \times K^{\mathrm{h}_{\Phi,A}-1}, \\ \Phi_{[j+t-\mathrm{h}_{\Phi,A},\, j+t+\mathrm{h}_{\Phi,A}-1]} = E^{\mathrm{h}_{\Phi,A}} \times (K \setminus E) \times K^{\mathrm{h}_{\Phi,A}-1}. \end{cases} \tag{21}$$

*Proof.* It follows from Lemmas 2.5 and 5.5. □

**Lemma 5.7.** *Let $K$ be a set, let $t$ and $p$ be two positive integers, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $p$.*

*(a) If $t \geq 2$, then it holds $2\,\mathrm{h}_{\Phi,a} \leq t$ for every $a \in K$.*

*(b) If $t \geq 3$ and $p > 2t$, then it holds $\mathrm{h}_{\Phi,a} + \mathrm{h}_{\Phi,x} \leq t-1$ for every $a, x \in K$ with $\mathrm{Loc}_\Phi(a^t) \neq \mathrm{Loc}_\Phi(x^t)$.*

*Proof.* (a). Let $j \doteq \mathrm{Loc}_\Phi(a^t)$. We only need to consider the case of $\mathrm{h}_{\Phi,a} \geq 1$ and so we can make use of Lemma 5.6. If Eq. (20) holds, then we have $\Phi_{[j,j+\mathrm{h}_{\Phi,a}-1]} = (K \setminus B)^{\mathrm{h}_{\Phi,a}}$ and $\Phi_{[j+t-\mathrm{h}_{\Phi,a},j+t-2]} = K^{\mathrm{h}_{\Phi,a}-1}$, which gives $[j, j+\mathrm{h}_{\Phi,a}-1] \cap [j+t-\mathrm{h}_{\Phi,a}, j+t-2] = \emptyset$, namely either $\mathrm{h}_{\Phi,a} = 1$ or $j+\mathrm{h}_{\Phi,a}-1 \leq j+t-\mathrm{h}_{\Phi,a}-1$. If Eq. (21) holds, then we have $\Phi_{[j+1,j+\mathrm{h}_{\Phi,a}-1]} = K^{\mathrm{h}_{\Phi,a}-1}$ and $\Phi_{[j+t-\mathrm{h}_{\Phi,a},j+t-1]} = (K \setminus C)^{\mathrm{h}_{\Phi,a}}$, implying $[j+1, j+\mathrm{h}_{\Phi,a}-1] \cap [j+t-\mathrm{h}_{\Phi,a}, j+t-1] = \emptyset$, namely either $\mathrm{h}_{\Phi,a} = 1$ or $j+\mathrm{h}_{\Phi,a}-1 \leq j+t-\mathrm{h}_{\Phi,a}$. Because we have assumed $t \geq 2$, in both cases we have $2\,\mathrm{h}_{\Phi,a} \leq t$.

(b). Assume, by way of contradiction, that $\mathrm{h}_{\Phi,a} + \mathrm{h}_{\Phi,x} \geq t$. Without loss of generality, let $\mathrm{h}_{\Phi,a} \geq \mathrm{h}_{\Phi,x}$. As $t \geq 3$, we now conclude that $\mathrm{h}_{\Phi,a} \geq 2$. Let $j \doteq \mathrm{Loc}_\Phi(a^t) \in \mathrm{Diag}_\Phi$ and $A \doteq \bigcap_{i=j}^{j+t-1} \Phi_i$. Note that $\mathrm{h}_{\Phi,A} = \mathrm{h}_{\Phi,a} \geq 2$ and $p > 2t$. Therefore, we can apply Lemma 5.6 and find that either Eq. (20) or Eq. (21) must hold.

Using the fact that either the first line of Eq. (20) or the first line of Eq. (21) must be valid, we shall show that

$$\mathrm{Loc}_\Phi(x^t) = j - t. \tag{22}$$

Let $\Psi_i \doteq \Phi_{2j+t-1-i}$ for every $i \in \mathbb{Z}/p\mathbb{Z}$. Thanks to the symmetry between $\Phi$ and $\Psi$ as ensured by Lemma 5.2 (d), the fact that either the second line of Eq. (20) or the second line of Eq. (21) must be valid, which indeed are the counterpart of the fact on the first lines there by the symmetry between $\Phi$ and $\Psi$, will lead to $\mathrm{Loc}_\Psi(x^t) = \mathrm{Loc}_\Phi(x^t) = j - t$. But we then derive $j - t = \mathrm{Loc}_\Phi(x^t) = 2j - \mathrm{Loc}_\Psi(x^t) = j + t$ in $\mathbb{Z}/p\mathbb{Z}$, violating the assumption of $p > 2t$.

It is clear that our goal now is to establish Eq. (22). Before moving on, we digress to make two observations. Since $\mathrm{Loc}_\Phi(x^t) \neq j$, Lemma 3.4 (a) shows that

$$\mathrm{Loc}_\Phi(x^t) \notin [j-t+1, j+t-1]. \tag{23}$$

Lemma 5.2 (e), as well as $t - \mathrm{h}_{\Phi,x} \leq \mathrm{h}_{\Phi,a}$, implies that

$$\mathrm{Loc}_\Phi(x^{\mathrm{h}_{\Phi,a}}) \subseteq \mathrm{Loc}_\Phi(x^t) + \langle t - \mathrm{h}_{\Phi,a} \rangle. \tag{24}$$

Assume first that $x \notin B$. Then, Lemma 5.6 tells us that $x^{\mathrm{h}_{\Phi,a}} \in (K \setminus B)^{\mathrm{h}_{\Phi,a}} \subseteq \Phi_{[j,j+\mathrm{h}_{\Phi,a}-1]}$, and hence $j \in \mathrm{Loc}_\Phi(x^{\mathrm{h}_{\Phi,a}})$. This combined with Eq. (24) shows that $\mathrm{Loc}_\Phi(x^t) \in [j-t+\mathrm{h}_{\Phi,a}, j]$, which contradicts Eq. (23).

We now see that $x \in B$. It follows from Lemma 5.6 that $x^{\mathrm{h}_{\Phi,a}} \in B^{\mathrm{h}_{\Phi,a}} \subseteq \Phi_{[j-\mathrm{h}_{\Phi,a},j-1]}$, and hence $j - \mathrm{h}_{\Phi,a} \in \mathrm{Loc}_\Phi(x^{\mathrm{h}_{\Phi,a}})$. This, along with Eq. (24), gives $\mathrm{Loc}_\Phi(x^t) \in [j - \mathrm{h}_{\Phi,a} - (t - \mathrm{h}_{\Phi,a}), j - \mathrm{h}_{\Phi,a}] = [j-t, j-\mathrm{h}_{\Phi,a}]$. By virtue of Eq. (23) in addition, Eq. (22) is thus obtained, and so we are done. □

## 6. Two lemmas on diagonal positions

This section aims to establish two constraints on the diagonal positions of a cyclic decomposition in some special situations; see Lemmas 6.1 and 6.6. One is about the differences between elements from the diagonal positions, in the same spirit as Lemma 3.4 (c); and the other is about the size of the diagonal positions, just like Lemmas 3.4 (a) and 3.4 (b). Note that Lemma 6.1 has a short proof; but to reach Lemma 6.6, we will need several stepping stones (Lemmas 6.2, 6.4 and 6.5 and Corollary 6.3).

**Lemma 6.1.** *Let $K$ be a set, let $t$ be a positive integer, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$. If $\mathrm{Diag}_\Phi = \{i_1, i_2\} \in \binom{\mathbb{Z}/p\mathbb{Z}}{2}$, then $i_2 - i_1 \neq t + 1$.*

*Proof.* Let $A \doteq \bigcap_{i=i_1}^{i_1+t-1} \Phi_i$ and $B \doteq \bigcap_{i=i_2}^{i_2+t-1} \Phi_i$. It follows from $\mathrm{Diag}_\Phi = \{i_1, i_2\}$ that $A \sqcup B = K$. Based on Corollary 3.6, we have $\Phi_{i_1+t-1} \cap \Phi_{i_1+t} = \emptyset$ and $\Phi_{i_2-1} \cap \Phi_{i_2} = \emptyset$. Hence, $\Phi_{i_1+t} \subseteq K \setminus \Phi_{i_1+t-1} \subseteq K \setminus A = B$ and $\Phi_{i_2-1} \subseteq K \setminus \Phi_{i_2} \subseteq K \setminus B = A$. As both $\Phi_{i_1+t}$ and $\Phi_{i_2-1}$ are nonempty, the disjointness of $A$ and $B$ then illustrates that $i_1 + t \neq i_2 - 1$, or equivalently, $i_2 - i_1 \neq t + 1$. □

**Lemma 6.2.** *Let $K$ be a set, let $t$ and $p$ be integers with $\min\{t, p\} \geq 2$, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $p$. Let $I \subseteq \mathbb{Z}/p\mathbb{Z}$ be a set such that $\{i \in I : \ i - j \in \langle t-1 \rangle\} \neq \emptyset$ holds for every $j \in \mathbb{Z}/p\mathbb{Z}$. Then, there exists a map $\alpha$ from $I$ to $\mathbb{Z}$ such that $\sum_{i \in I} \alpha_i \mathbb{1}_{\Phi_i} = \mathbb{1}_K \in \mathbb{R}^K$.*

*Proof.* As we demonstrate in the proof of Lemma 3.4, there is no loss in assuming that $|K| < \infty$.

Let $G = \mathbb{Z}\mathbb{1}_K \cap (\sum_{i \in I} \mathbb{Z}\mathbb{1}_{\Phi_i})$, which is a cyclic subgroup of $\mathbb{Z}^{2^K}$ under vector addition. Let $g\mathbb{1}_K$ be the generator of this group $G$. If $g \in \{\pm 1\}$, then we are done. Otherwise, we can take $s$ to be the smallest prime factor of $g$. Note that $s = 2$ when $g = 0$. We now proceed to derive a contradiction.

It is clear that $t\mathbb{1}_K \in \mathrm{Span}_{\mathbb{Z}/s\mathbb{Z}}(\mathbb{1}_{\Phi_i} : \ i \in I)$ only if $t \equiv 0 \pmod{s}$. As a result, there exists a $\mathbb{Z}/s\mathbb{Z}$-linear function $f$ from $(\mathbb{Z}/s\mathbb{Z})^K$ to $\mathbb{Z}/s\mathbb{Z}$ satisfying

$$f(\mathbb{1}_A) = \sum_{a \in A} f(\mathbb{1}_{\{a\}}) \tag{25}$$

for every $A \subseteq K$, $f(\mathbb{1}_{\Phi_i}) = 0$ for every $i \in I$, and $f(\mathbb{1}_K) \neq 0$. For every $j \in \mathbb{Z}/p\mathbb{Z}$, we have

$$\prod_{j'=j}^{j+t-1} f(\mathbb{1}_{\Phi_{j'}}) = 0, \tag{26}$$

simply due to the existence of $i \in I$ with $i - j \in \langle t-1 \rangle$. Since $\Phi$ is a cyclic decomposition of $(K^t, K, t)$ with period $p$, from Eqs. (25) and (26) we derive $f(\mathbb{1}_K)^t = \sum_{j=1}^{p} \prod_{j'=j}^{j+t-1} f(\mathbb{1}_{\Phi_{j'}}) = 0$, contradicting the fact that $f(\mathbb{1}_K) \neq 0$. □

**Corollary 6.3.** *Let $K$ be a set, let $t$ be an integer with $t \geq 2$, let $\ell \in \mathbb{Z}/(3t\mathbb{Z})$, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $3t$. Then we cannot find a partition of $K$ into three nonempty subsets $A, B$ and $C$ such that $(\Phi_\ell, \Phi_{t+\ell}, \Phi_{2t+\ell}) = (C \sqcup B, A \sqcup C, B \sqcup A)$.*

*Proof.* Assume otherwise that the three sets $A, B$ and $C$ with the required property can be found. By Lemma 6.2, there exists $\beta \in \mathbb{Z}^{\{0,t,2t\}}$ such that $\mathbb{1}_A + \mathbb{1}_B + \mathbb{1}_C = \mathbb{1}_K = \sum_{i \in \{0,t,2t\}} \beta_i \mathbb{1}_{\Phi_{i+\ell}} = (\beta_{2t} + \beta_t)\mathbb{1}_A + (\beta_0 + \beta_{2t})\mathbb{1}_B + (\beta_t + \beta_0)\mathbb{1}_C$. Since $A, B, C$ are all nonempty and pairwise disjoint, an easy parity inspection on the values of $\beta$ says that this is impossible. □

**Lemma 6.4.** *Let $K$ be a set, let $t \geq 3$ be an integer, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $3t$ and $\mathrm{Diag}_\Phi = \{1, t+1, 2t+1\}$. Let $A \doteq \bigcap_{i=1}^{t} \Phi_i \neq \emptyset$ and $q \doteq \mathrm{h}_{\Phi,A}$. Assume that $q \in [t-2]$ and that*

$$\Phi_{[2t-q+1,2t+q]} = (K \setminus D)^q \times D \times K^{q-1}, \tag{27}$$

*where $D$ is a nonempty proper subset of $K$. Then the following statements hold true.*

*(a) The set $\mathrm{Loc}_\Phi(a^{t-q-1}) \setminus [q+2]$ is contained in $Y$ for all $a \in A$, where $Y = \{2t+1, t+2\} \cup \{2t+2, t+q+2\}$.*

*(b) If $\Phi_{2t+1} \cap A \neq \emptyset$, then $\mathrm{Loc}_\Phi(a^{t-q-1}) \setminus [q+2] \subseteq \{2t+1, t+2\}$ for all $a \in A$.*

*(c) If* $\Phi_{2t} \cap A \neq \emptyset$*, then* $\mathrm{Loc}_\Phi(a^{t-q-1}) \setminus [q+2] \subseteq \{2t+2, t+q+2\}$ *for all* $a \in A$*.*

*(d) It holds either* $\Phi_{2t} \cap A \neq \emptyset$ *or* $\Phi_{2t+1} \cap A \neq \emptyset$*, but not both.*

*Proof.* (a). By Lemma 5.2 (b) for $j = 1$, it actually happens that

$$\mathrm{Loc}_\Phi(a^{t-q-1}) \setminus [q+2] \neq \emptyset. \tag{28}$$

Let us arbitrarily choose an element

$$\theta_a \in \mathrm{Loc}_\Phi(a^{t-q-1}) \setminus [q+2]. \tag{29}$$

Let $I^{\underline{1}} = [q+2], I^{\underline{2}} = [q+3, t+1], I^{\underline{3}} = [t+3, t+q+1], I^{\underline{4}} = [t+q+3, 2t], I^{\underline{5}} = [2t+3, 2t+q+1]$ and $I^{\underline{6}} = [2t+q+2, 3t]$, where $I^{\underline{3}}$, $I^{\underline{4}}$ and $I^{\underline{5}}$ should be read as $\emptyset$ when $q = 1$, $q = t-2$, $q = 1$, respectively. Note that $[3t] = I^{\underline{1}} \cup I^{\underline{2}} \cup \{t+2\} \cup I^{\underline{3}} \cup \{t+q+2\} \cup I^{\underline{4}} \cup \{2t+1, 2t+2\} \cup I^{\underline{5}} \cup I^{\underline{6}} = Y \cup I^{\underline{1}} \cup I^{\underline{2}} \cup I^{\underline{3}} \cup I^{\underline{4}} \cup I^{\underline{5}} \cup I^{\underline{6}}$. In order to derive $\theta_a \in Y$, it suffices to demonstrate that $\theta_a \notin I^{\underline{1}} \cup I^{\underline{2}} \cup I^{\underline{3}} \cup I^{\underline{4}} \cup I^{\underline{5}} \cup I^{\underline{6}}$.

From $\theta_a \in \mathrm{Loc}_\Phi(a^{t-q-1})$ we deduce that

$$\Phi_{\theta_a+i} \cap A \supseteq \{a\} \neq \emptyset \tag{30}$$

for all $i \in \langle t-q-2 \rangle$. By Lemma 5.2 (b) for $j = 1$, we have $\mathrm{Loc}_\Phi(ba^{t-q-1}) \subseteq 1 + \langle q \rangle = [q+1]$ and $\mathrm{Loc}_\Phi(a^{t-q-1}b) \subseteq 1 + \langle q \rangle = [q+1]$ for all $b \in A$. It then follows from $\theta_a \notin [q+2]$ that $\theta_a - 1 \notin [q+1] \supseteq \mathrm{Loc}_\Phi(ba^{t-q-1})$ and $\theta_a \notin [q+2] \supseteq \mathrm{Loc}_\Phi(a^{t-q-1}b)$ for all $b \in A$. Taking into account $\theta_a \in \mathrm{Loc}_\Phi(a^{t-q-1})$ again, we see from them that

$$\Phi_{\theta_a-1} \cap A = \emptyset \text{ and } \Phi_{\theta_a+t-q-1} \cap A = \emptyset, \tag{31}$$

respectively.

It follows from Eq. (29) that $\theta_a \notin I^{\underline{1}}$. In view of Eq. (29) and $q \leq t-2$, an application of Lemma 5.2 (a) with $j \doteq 1$ and $s \doteq q+1$ leads to $\theta_a \notin I^{\underline{2}}$. According to Eqs. (30) and (31), we have $a \in \Phi_{\theta_a+t-q-2} \setminus \Phi_{\theta_a+t-q-1}$, and hence

$$\Phi_{\theta_a+t-q-2} \neq \Phi_{\theta_a+t-q-1}. \tag{32}$$

By Eq. (27), it holds that $\Phi_{2t-q+1} = \cdots = \Phi_{2t} = K \setminus D$, which together with Eq. (32) claims that it is impossible to have $\{\theta_a+t-q-2, \theta_a+t-q-1\} \subseteq [2t-q+1, 2t]$. This implies that $\theta_a \notin I^{\underline{3}}$. Applying Corollary 3.6 with $i \doteq 2t+1$ yields $\Phi_{2t} \cap \Phi_{2t+1} = \emptyset \not\supseteq \{a\}$. Henceforth, Eq. (30) tells us that

$$\theta_a + \langle t-q-2 \rangle \not\supseteq \{2t, 2t+1\}. \tag{33}$$

If $I^{\underline{4}} \neq \emptyset$, we would have $q \in [t-3]$ and thus

$$\bigcap_{i \in I^{\underline{4}}} (i + \langle t-q-2 \rangle) = \{2t, 2t+1\}. \tag{34}$$

Putting together Eqs. (33) and (34), we see that $\theta_a \notin I^{\underline{4}}$. Eq. (27) tells us that $\Phi_{2t+2} = \cdots = \Phi_{2t+q} = K$. But a look at Eq. (31) also gives $\Phi_{\theta_a-1} \neq K$, which then leads to $\theta_a \notin I^{\underline{5}}$. It follows from Eq. (31) that $\emptyset \neq A = A \setminus \Phi_{\theta_a+t-q-1} = (\bigcap_{i \in [t]} \Phi_i) \setminus \Phi_{\theta_a+t-q-1}$. Therefore, it holds that $\theta_a + t - q - 1 \notin [t] \pmod{3t}$, showing that $\theta_a \notin [2t+q+2, 3t+q+1] \supseteq I^{\underline{6}}$. This completes the proof of (a).

(b). If $\Phi_{2t+1} \cap A \neq \emptyset$ holds, then Eq. (31) shows that $\theta_a - 1 \neq 2t+1$ and $\theta_a + t - q - 1 \neq 2t+1$, hence $\theta_a \notin \{2t+2, t+q+2\}$ follows. This along with (a) and Eq. (29) gives (b).

(c). If it holds $\Phi_{2t} \cap A \neq \emptyset$, then Eq. (27) tells us that $\Phi_{2t+1-q} \cap A = \cdots = \Phi_{2t} \cap A \neq \emptyset$. A comparison with Eq. (31) gives us $\theta_a - 1 \neq 2t$ and $\theta_a + t - q - 1 \neq 2t + 1 - q$, namely $\theta_a \notin \{2t+1, t+2\}$. Utilizing (a) and Eq. (29) additionally, we now obtain (c).

(d). Since $q \geq 1$, Lemma 5.2 (f) implies that $\Phi_{2t} \sqcup \Phi_{2t+1} = K \supseteq A$. From $q \in [t-2]$ and $t \geq 3$ we see that $\{t+2, 2t+1\}$ and $\{t+q+2, 2t+2\}$ are disjoint subsets of $[3t]$, and so can be viewed as disjoint subsets of $\mathbb{Z}/(3t\mathbb{Z})$ as well. Therefore, thanks to Eq. (28), a combination of (b) and (c) proves (d). □

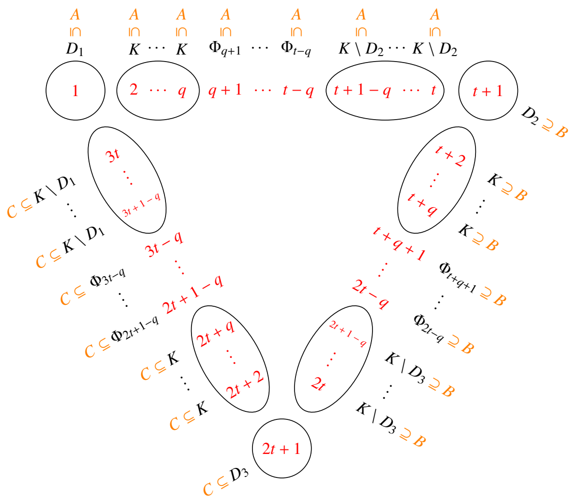


Figure 4: The cyclic decomposition Φ appeared in Lemma 6.5 and in Case 2 of the proof of Lemma 6.6.

**Lemma 6.5.** *Let $K$ be a set, let $t$ be an integer with $t \geq 3$, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $3t$. Let us assume that $\mathrm{Diag}_\Phi = \{1, t+1, 2t+1\}$ and that $\mathrm{h}_{\Phi,x}$ takes a constant value $q \in [\lfloor \frac{t-1}{2} \rfloor] \subseteq [t-2]$ for all $x \in K$. Let $A = \bigcap_{i\in[t]} \Phi_i$, $B = \bigcap_{i\in[t+1,2t]} \Phi_i$, and $C = \bigcap_{i\in[2t+1,3t]} \Phi_i$, which surely constitute a partition of $K$ into three nonempty subsets. Let $D_1$, $D_2$, and $D_3$ be three nonempty proper subsets of $K$ such that*

$$\Phi_{[1-q,q]} = (K \setminus D_1)^q \times D_1 \times K^{q-1}, \Phi_{[t-q+1,t+q]} = (K \setminus D_2)^q \times D_2 \times K^{q-1}, \Phi_{[2t-q+1,2t+q]} = (K \setminus D_3)^q \times D_3 \times K^{q-1}. \quad (35)$$

*A pictorial description of $\Phi$ is given in Fig. 4. The following statements hold true.*

*(a)* $(\Phi_1, \Phi_{t+1}, \Phi_{2t+1}) = (D_1, D_2, D_3) \neq (A \sqcup B, B \sqcup C, C \sqcup A)$.

*(b)* $(\Phi_1, \Phi_{t+1}, \Phi_{2t+1}) = (D_1, D_2, D_3) \neq (A, B \sqcup C, C \sqcup A)$.

*(c)* $(\Phi_1, \Phi_{t+1}, \Phi_{2t+1}) = (D_1, D_2, D_3) \neq (A, B \sqcup C, C)$.

*(d)* $(\Phi_1, \Phi_{t+1}, \Phi_{2t+1}) = (D_1, D_2, D_3) \neq (A, B, C)$.

*Proof.* (a). If $(D_1, D_2, D_3) = (A\sqcup B, B\sqcup C, C\sqcup A)$, we can read from Eq. (35) that $(\Phi_1, \Phi_{t+1}, \Phi_{2t+1}) = (A\sqcup B, B\sqcup C, C\sqcup A)$, violating Corollary 6.3.

(b). We assume by way of contradiction that $(D_1, D_2, D_3) = (A, B \sqcup C, C \sqcup A)$. Then Eq. (35) tells us that

$$\Phi_{[1-q,q]} = (C \sqcup B)^q \times A \times K^{q-1}, \Phi_{[t-q+1,t+q]} = A^q \times (B \sqcup C) \times K^{q-1}, \Phi_{[2t-q+1,2t+q]} = B^q \times (C \sqcup A) \times K^{q-1}. \quad (36)$$

Pick $a \in A$, and we aim to show that $\mathrm{Loc}_\Phi(a^{t-q-1}) \setminus [q+2] = \emptyset$, which contradicts Lemma 5.2 (b). By Eq. (36), we have $\Phi_{2t+1} \cap A = (C \sqcup A) \cap A = A \neq \emptyset$. Note that $q \in [t-2]$, and that Eq. (35) implies Eq. (27). Therefore, we can apply Lemma 6.4 (b) and derive that $\mathrm{Loc}_\Phi(a^{t-q-1}) \setminus [q+2] \subseteq \{t+2, 2t+1\}$. To complete the proof, we need to demonstrate that neither $2t+1$ nor $t+2$ falls inside $\mathrm{Loc}_\Phi(a^{t-q-1})$.

For this purpose, we should pay attention to the subsequent easy consequences of Eq. (36):

$$\Phi_{[3t-q,3t]} \cap \Phi_{[t+1,t+q+1]} \supseteq (C \times (C \sqcup B)^q) \cap ((B \sqcup C) \times K^{q-1} \times B) = C \times (B \sqcup C)^{q-1} \times B \neq \emptyset, \quad (37)$$

$$\Phi_{[2t-q+1,2t]} \cap \Phi_{[t+1,t+q]} = B^q \cap ((B \sqcup C) \times K^{q-1}) = B^q \neq \emptyset. \quad (38)$$

Note that we have used $\Phi_{3t-q} \supseteq C$ and that $\Phi_{t+q+1} \supseteq B$ in Eq. (37).

Observe that $\emptyset = \Phi_{[2t+1,3t]} \cap \Phi_{[q+2,t+q+1]} = (\Phi_{[2t+1,3t-q-1]} \cap \Phi_{[q+2,t]}) \times (\Phi_{[3t-q,3t]} \cap \Phi_{[t+1,t+q+1]})$. In light of Eq. (37), it holds $\Phi_{[2t+1,3t-q-1]} \cap \Phi_{[q+2,t]} = \emptyset$. Therefore, from $a^{t-q-1} \in \Phi_{[q+2,t]}$ we then infer that $a^{t-q-1} \notin \Phi_{[2t+1,3t-q-1]}$, namely $2t+1 \notin \mathrm{Loc}_\Phi(a^{t-q-1})$.

Finally, let us consider

$$\emptyset = \Phi_{[t+2,2t+1]} \cap \Phi_{[q+2,t+q+1]} = (\Phi_{[t+2,2t-q]} \cap \Phi_{[q+2,t]}) \times (\Phi_{[2t-q+1,2t]} \cap \Phi_{[t+1,t+q]}) \times (\Phi_{2t+1} \cap \Phi_{t+q+1}).$$

In light of Eq. (38), this results in

$$\emptyset = (\Phi_{[t+2,2t-q]} \cap \Phi_{[q+2,t]}) \times (\Phi_{2t+1} \cap \Phi_{t+q+1}). \tag{39}$$

Note that

$$a^{t-q-1} \in \Phi_{[q+2,t]} \text{ and } a \in B \sqcup A = \Phi_{2t+1}. \tag{40}$$

As the last step of the proof, let us assume $t+2 \in \mathrm{Loc}_\Phi(a^{t-q-1})$ and derive a contradiction. It follows from $t+2 \in \mathrm{Loc}_\Phi(a^{t-q-1})$ that

$$a^{t-q-1} \in \Phi_{[t+2,2t-q]}, \tag{41}$$

and hence, as $t+q+1 \in [t+2, 2t-q]$, we obtain

$$a \in \Phi_{t+q+1}. \tag{42}$$

By Eqs. (40) to (42), we have $a^{t-q} \in (\Phi_{[t+2,2t-q]} \cap \Phi_{[q+2,t]}) \times (\Phi_{2t+1} \cap \Phi_{t+q+1})$, which is a desired contradiction with Eq. (39).

(c). Assume by way of contradiction that $(D_1, D_2, D_3) = (A, B \sqcup C, C)$. Then it follows from Eq. (35) that

$$\Phi_{[1-q,q]} = (C \sqcup B)^q \times A \times K^{q-1}, \Phi_{[t-q+1,t+q]} = A^q \times (B \sqcup C) \times K^{q-1} \text{ and } \Phi_{[2t-q+1,2t+q]} = (B \sqcup A)^q \times C \times K^{q-1}. \tag{43}$$

Case 1. It holds $q = 1$.

Let $\Psi_i \doteq \Phi_{1-i}$ for all $i \in \mathbb{Z}/(3t\mathbb{Z})$. Then $\Psi$ is a cyclic decomposition of $(K^t, K, t)$ with period $3t$. Moreover, we have

$$\bigcap_{i\in[t]} \Psi_i = \bigcap_{i\in[2t+1,3t]} \Phi_i = C, \bigcap_{i\in[t+1,2t]} \Psi_i = \bigcap_{i\in[t+1,2t]} \Phi_i = B, \bigcap_{i\in[2t+1,3t]} \Psi_i = \bigcap_{i\in[t]} \Phi_i = A,$$

and

$$\Psi_{[0,1]} = \Phi_1 \times \Phi_0 = A \times (C \sqcup B), \Psi_{[t,t+1]} = \Phi_{t+1} \times \Phi_t = (B \sqcup C) \times A, \Psi_{[2t,2t+1]} = \Phi_{2t+1} \times \Phi_{2t} = C \times (B \sqcup A).$$

Therefore, $\Psi$ satisfies Eq. (35) with $(D_1, D_2, D_3) = (C, B \sqcup A, A \sqcup C)$, violating (b).

Case 2. It holds $q \geq 2$.

Pick $a \in A$. Since $2 \leq q \leq t-2$ and $\Phi_{2t} \cap A = (B \sqcup A) \cap A = A \neq \emptyset$, we can apply Lemma 6.4 (c) to find that $\mathrm{Loc}_\Phi(a^{t-q-1}) \setminus [q+2] \subseteq \{2t+2, t+q+2\}$. We proceed to show that $\mathrm{Loc}_\Phi(a^{t-q-1}) \cap \{2t+2, t+q+2\} = \emptyset$, which will be a desired contradiction with Lemma 5.2 (b) for $j = 1$.

Because of $\Phi_{t+q+1} \supseteq B$ and $q \geq 2$, we can infer from Eq. (43) that

$$\Phi_{[2t-q+1,2t+1]} \cap \Phi_{[0,q]} = ((B \sqcup A)^q \times C) \cap ((C \sqcup B) \times A \times K^{q-1}) = B \times A \times (B \sqcup A)^{q-2} \times C \neq \emptyset, \tag{44}$$

$$\Phi_{[t+1,t+q+1]} \cap \Phi_{[0,q]} \supseteq ((B \sqcup C) \times K^{q-1} \times B) \cap ((C \sqcup B) \times A \times K^{q-1}) = (B \sqcup C) \times A \times K^{q-2} \times B \neq \emptyset. \tag{45}$$

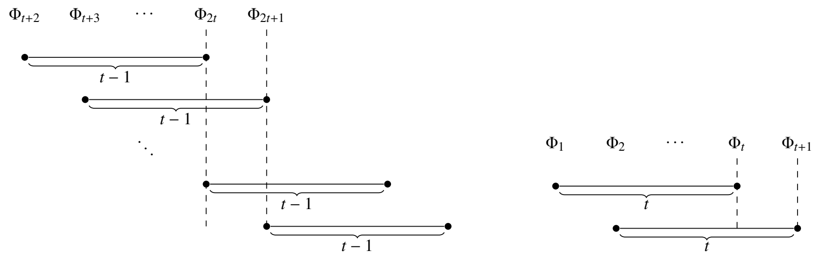
Notice that $\emptyset = \Phi_{[2t-q+1,3t-q]} \cap \Phi_{[0,t-1]} = (\Phi_{[2t-q+1,2t+1]} \cap \Phi_{[0,q]}) \times (\Phi_{[2t+2,3t-q]} \cap \Phi_{[q+1,t-1]})$. In view of Eq. (44), this implies $\Phi_{[2t+2,3t-q]} \cap \Phi_{[q+1,t-1]} = \emptyset$. Since $a^{t-q-1} \in A^{t-q-1} \subseteq \Phi_{[q+1,t-1]}$, we then conclude that $a^{t-q-1} \notin \Phi_{[2t+2,3t-q]}$, that is, $2t+2 \notin \mathrm{Loc}_\Phi(a^{t-q-1})$.

We further observe that $\emptyset = \Phi_{[t+1,2t]} \cap \Phi_{[0,t-1]} = (\Phi_{[t+1,t+q+1]} \cap \Phi_{[0,q]}) \times (\Phi_{[t+q+2,2t]} \cap \Phi_{[q+1,t-1]})$. This together with Eq. (45) says that $\Phi_{[t+q+2,2t]} \cap \Phi_{[q+1,t-1]} = \emptyset$. Using $a^{t-q-1} \in \Phi_{[q+1,t-1]}$ again, we obtain $a^{t-q-1} \notin \Phi_{[t+q+2,2t]}$, resulting in $t+q+2 \notin \mathrm{Loc}_\Phi(a^{t-q-1})$, as wanted.

(d). If $(D_1, D_2, D_3) = (A, B, C)$, then we will infer from Eq. (35) that $(\Phi_0, \Phi_t, \Phi_{2t}) = (C \sqcup B, A \sqcup C, B \sqcup A)$, contradicting Corollary 6.3. □

**Lemma 6.6.** *Let $K$ be a set, let $t \geq 3$ be an integer, and let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $3t$. Then $|\mathrm{Diag}_\Phi| \neq 3$.*

*Proof.* Suppose, for the sake of contradiction, that $|\mathrm{Diag}_\Phi| = 3$. According to Lemma 3.4 (a), we have $\mathrm{Diag}_\Phi = \{\ell, \ell+t, \ell+2t\}$ for some $\ell \in \mathrm{Diag}_\Phi$. There is no loss of generality in assuming $\mathrm{Diag}_\Phi = \{1, t+1, 2t+1\}$. We put $A \doteq \bigcap_{i=1}^{t} \Phi_i$, $B \doteq \bigcap_{i=t+1}^{2t} \Phi_i$, and $C \doteq \bigcap_{i=2t+1}^{3t} \Phi_i$. Clearly, it holds $A \sqcup B \sqcup C = K$ and none of $A$, $B$, and $C$ is empty. By Lemma 5.4, there exists $q \in \mathbb{N}_0$ such that $\mathrm{h}_{\Phi,x} = q$ for all $x \in K$. It follows from Lemma 5.7 (b) that $2q \leq t-1$.



(a) All $(t-1)$-intervals in $\mathbb{Z}/(3t\mathbb{Z})$ that intersect $\{2t, 2t+1\}$. (b) All $t$-intervals in $\mathbb{Z}/(3t\mathbb{Z})$ ending at $\{t, t+1\}$.

Figure 5: Case 1 of the proof of Lemma 6.6.

Case 1. $q = 0$.

Because $\underbrace{A \times \cdots \times A}_{t-1} \times A \subseteq \Phi_{[1,t]}$ and $\underbrace{A \times \cdots \times A}_{t-1} \times B \subseteq \Phi_{[2,t+1]}$, we know that $\underbrace{A \times \cdots \times A}_{t-1} \times (A \sqcup B)$ is disjoint from $\bigsqcup_{i \in [3t] \setminus [2]} \Phi_{[i,i+t-1]}$. This means that

$$\mathrm{Loc}_\Phi(a^{t-1}) \subseteq [t+2, 2t+1] \cup [2] \tag{46}$$

is valid for all $a \in A$. Corollary 3.6 asserts that $\Phi_{2t+1} \cap \Phi_{2t} = \Phi_{t+1} \cap \Phi_t = \emptyset$. Since $\Phi_{2t+1} \cup \Phi_{2t} \supseteq C \cup B = K \setminus A$ and $\Phi_{t+1} \cup \Phi_t \supseteq B \cup A = K \setminus C$, a further application of Lemma 5.2 (f) then demonstrates that we can find $a \in A \setminus (\Phi_{2t} \cup \Phi_{2t+1})$ and $c \in C \setminus (\Phi_t \cup \Phi_{t+1})$. It follows from $a \in A \setminus (\Phi_{2t} \cup \Phi_{2t+1})$ that $\mathrm{Loc}_\Phi(a^{t-1}c) \notin [t+2, 2t+1]$; see Fig. 5(a). On the other hand, it follows from $c \in C \setminus (\Phi_t \cup \Phi_{t+1})$ that $\mathrm{Loc}_\Phi(a^{t-1}c) \notin [2]$; see Fig. 5(b). These two observations show us that $\mathrm{Loc}_\Phi(a^{t-1}c) \notin [t+2, 2t+1] \cup [2]$. But we surely have $\mathrm{Loc}_\Phi(a^{t-1}c) \in \mathrm{Loc}_\Phi(a^{t-1})$, thus yielding a contradiction with Eq. (46).

Case 2. $1 \leq q \leq \frac{t-1}{2}$.

Let $\Psi_i \doteq \Phi_{t+1-i}$ for all $i \in \mathbb{Z}/(3t\mathbb{Z})$. By virtue of Lemmas 5.2 (d) and 5.6, we may, via replacing $\Phi$ with $\Psi$ when necessary, always assume that $\Phi$ satisfies Eq. (21) for all $j \in \mathrm{Diag}_\Phi$; we depict a picture of $\Phi$ in Fig. 4. Especially, we have

$$\Phi_0 \sqcup \Phi_1 = \Phi_t \sqcup \Phi_{t+1} = \Phi_{2t} \sqcup \Phi_{2t+1} = K. \tag{47}$$

By the symmetry among the three elements $1$, $t+1$, and $2t+1$ of $\mathrm{Diag}_\Phi$, Lemma 6.4 (d) indeed demonstrates the following:

(i) It holds either $\Phi_t \cap C \neq \emptyset$ or $\Phi_{t+1} \cap C \neq \emptyset$, but not both;

(ii) It holds either $\Phi_0 \cap B \neq \emptyset$ or $\Phi_1 \cap B \neq \emptyset$, but not both;

(iii) It holds either $\Phi_{2t} \cap A \neq \emptyset$ or $\Phi_{2t+1} \cap A \neq \emptyset$, but not both.

In light of Eq. (47) and (i) to (iii), and that $A \subseteq \Phi_1 \cap \Phi_t$, $B \subseteq \Phi_{t+1} \cap \Phi_{2t}$, and $C \subseteq \Phi_{2t+1} \cap \Phi_{3t}$, we then have $(\Phi_1, \Phi_{t+1}, \Phi_{2t+1}) \in \{A \sqcup B, A\} \times \{B \sqcup C, B\} \times \{C \sqcup A, C\}$. There are four cases to consider, depending on the value of $\mathbb{1}_{B \subseteq \Phi_1} + \mathbb{1}_{C \subseteq \Phi_{t+1}} + \mathbb{1}_{A \subseteq \Phi_{2t+1}}$, which may be 3, 2, 1 or 0. Let $\Psi_i = \Phi_{i+t}$ and $\Xi_i = \Phi_{i+2t}$ for all $i \in \mathbb{Z}/(3t\mathbb{Z})$. By replacing $\Phi$ by $\Psi$ or $\Xi$ if necessary, these four cases are dealt with already in Lemmas 6.5 (a) to 6.5 (d), respectively. Indeed, as we know from Lemma 6.5, they are all impossible, thus completing our proof. □

## 7. Possible periods $\leq 4t-1$ of $t$-hydras

**Definition 7.1** (Three projections of $\mathcal{U}$)**.** For any $(t,p)\in\mathbb{N}\times\mathbb{N}$, designate by $\mathcal{S}(t,p)$ the set of positive integers $k$ such that there is a cyclic decomposition of $([k]^t,[k],t)$ with period $p$, namely $\mathcal{S}(t,p)=\{k\in\mathbb{N}:\ p\in\mathcal{P}(k,t)\}$. For any $(p,k)\in\mathbb{N}\times\mathbb{N}$, designate by $\mathcal{T}(p,k)$ the set of positive integers $t$ such that there is a cyclic decomposition of $([k]^t,[k],t)$ with period $p$, namely $\mathcal{T}(p.k)=\{t\in\mathbb{N}:\ p\in\mathcal{P}(k,t)\}=\{t\in\mathbb{N}:\ k\in\mathcal{S}(t,p)\}$. We may think of $\mathcal{P},\mathcal{S},\mathcal{T}$ as three projections of $\mathcal{U}\cap\mathbb{N}^3$ along its first, second and third axes, namely the period-axis, space-axis and time-axis.

**Lemma 7.2.** $\mathcal{S}(3,9)=\emptyset$.

*Proof.* Assume for a contradiction that there exists a set $K$ and a cyclic decomposition $\Phi$ of $(K^3,K,3)$ with period 9.

Up to translation, we may assume that $1\in\mathrm{Diag}_\Phi$. Combining Lemmas 3.4 and 6.6 yields that $\mathrm{Diag}_\Phi=\{1,x\}$ for some $x\in\{4,5,6,7\}$. Lemma 6.1 excludes the possibility of $x\in\{5,6\}$. As a result, we have $\mathrm{Diag}_\Phi\in\{\{1,4\},\{1,7\}\}$. After making a reflection, if necessary, we may assume that $\mathrm{Diag}_\Phi=\{1,4\}$.

We set $A\doteq\bigcap_{i=1}^3\Phi_i$ and $B\doteq\bigcap_{i=4}^6\Phi_i$. We apply Corollary 3.6 for $i=1$ and $i=4$, respectively, and then find that $\Phi_7\subseteq K\setminus\Phi_6\subseteq A$ and $\Phi_9\subseteq K\setminus\Phi_1\subseteq B$. This means that $\Phi_7\times\Phi_9\subseteq A\times B\subseteq(\Phi_2\times\Phi_4)\cap(\Phi_3\times\Phi_5)$. Since $\Phi_2\times\Phi_3\times\Phi_4,\Phi_3\times\Phi_4\times\Phi_5$ and $\Phi_7\times\Phi_8\times\Phi_9$ are pairwise disjoint, we conclude that $\Phi_8=\Phi_8\cap K=\Phi_8\cap(\Phi_3\cup\Phi_4)=\emptyset$, which is absurd. □

**Lemma 7.3.** $\mathcal{S}(3,10)=\emptyset$.

*Proof.* We assume the opposite, that there is a cyclic decomposition $\Phi$ of $(K^3,K,3)$ with period 10 for some set $K$. In view of Lemma 3.4, we may, up to translation of $\Phi$, consider only the following four cases.

Case 1. $\mathrm{Diag}_\Phi=\{1,4\}$.

We set $A\doteq\bigcap_{i=1}^3\Phi_i$ and $B\doteq\bigcap_{i=4}^6\Phi_i$. It follows from Corollary 3.6 that $\Phi_3\cap\Phi_4=\emptyset$, and so we have $\Phi_3\sqcup\Phi_4=A\sqcup B=K$. Applying Lemmas 5.2 (f) and 5.2 (g) for $j=4$ and $j=1$, respectively, we thus find that $\mathrm{h}_{\Phi,B}\geq1$ and $\mathrm{h}_{\Phi,A}\geq1$. This enables us to get $\Phi_7=\Phi_1=A$ and $\Phi_6=\Phi_{10}=B$ from Lemma 5.3 (e). According to Lemma 5.3 (a), $\Phi_{10}\cap B\neq\emptyset$ leads to $\Phi_9\subseteq K\setminus B=A$ and $\Phi_7\cap A\neq\emptyset$ leads to $\Phi_8\subseteq K\setminus A=B$. At this moment, we see that $\Phi_{[6,8]}\cap\Phi_{[8,10]}=(\Phi_6\cap\Phi_8)\times(\Phi_7\cap\Phi_9)\times(\Phi_8\cap\Phi_{10})=\Phi_8\times\Phi_9\times\Phi_8\neq\emptyset$, which is ridiculous.

Case 2. $\mathrm{Diag}_\Phi=\{1,5\}$.

By Lemma 6.1, this case will never occur.

Case 3. $\mathrm{Diag}_\Phi=\{1,6\}$.

We set $A\doteq\bigcap_{i=1}^3\Phi_i$ and $B\doteq\bigcap_{i=6}^8\Phi_i$. Obviously, it holds $A\sqcup B=K$. By symmetry, let us assume that $\mathrm{h}_{\Phi,A}\leq\mathrm{h}_{\Phi,B}$.

If $\mathrm{h}_{\Phi,A}\geq1$, Lemma 5.3 (e) claims that $\Phi_6=\Phi_8=\Phi_{10}=\Phi_4=B$ and $\Phi_5=\Phi_9=\Phi_1=\Phi_3=A$, which means that $\Phi_{[3,5]}=A\times B\times A=\Phi_{[9,11]}$, violating the definition of a cyclic decomposition.

Let us move on to the case of $\mathrm{h}_{\Phi,A}=0$. Corollary 3.6 shows that

$$\Phi_i\cap\Phi_{i+1}=\emptyset\text{ for all }i\in\{3,5,8,10\}.\tag{48}$$

Especially, we have $\Phi_9\subseteq K\setminus\Phi_8\subseteq K\setminus B=A$. Pick $a\in\Phi_9\subseteq A$ arbitrarily. Note that $7\notin\mathrm{Loc}_\Phi(a^2)$ as it would imply $a^3\in\Phi_{[7,9]}\cap\Phi_{[1,3]}$. From Eq. (48) we can read $\Phi_5\cap\Phi_6=\emptyset$ and so $\Phi_5\subseteq K\setminus\Phi_6\subseteq K\setminus B=A$. Therefore, a consequence of $6\in\mathrm{Loc}_\Phi(a^2)$ is that $\Phi_{[5,7]}\cap\Phi_{[1,3]}\supseteq\Phi_5\times a^2\neq\emptyset$, which is impossible. Moreover, a direct consequence of Eq. (48) is that $\mathrm{Loc}_\Phi(a^2)\cap\{3,5,8,10\}=\emptyset$. Due to $\mathrm{h}_{\Phi,A}=0$, Lemma 5.2 (e) asserts that $\mathrm{Loc}_\Phi(a^2)\setminus[2]\neq\emptyset$. Take $\ell\in\mathrm{Loc}_\Phi(a^2)\setminus[2]$. By now, we have seen that $\ell\in\{4,9\}\subseteq\mathbb{Z}/10\mathbb{Z}$. The assumption of $\ell=4$ leads to $a^3\in\Phi_{[3,5]}\cap\Phi_{[1,3]}$ and the assumption of $\ell=9$ leads to $a^3\in\Phi_{[9,1]}\cap\Phi_{[1,3]}$, neither of which is compatible with the definition of a cyclic decomposition.

Case 4. $\mathrm{Diag}_\Phi=\{1,4,7\}$.

We set $A\doteq\bigcap_{i=1}^3\Phi_i$, $B\doteq\bigcap_{i=4}^6\Phi_i$, and $C\doteq\bigcap_{i=7}^9\Phi_i$, which surely form a partition of $K$. Lemma 5.4 shows that $\mathrm{h}_{\Phi,x}$ takes a constant value $q$ for all $x\in K$. We claim that

$$q\geq1.\tag{49}$$

By Corollary 3.6, it holds

$$\Phi_i \cap \Phi_{i+1} = \emptyset \text{ for all } i \in \{3, 6, 9, 10\}. \quad (50)$$

Especially, we have $\Phi_6 \cap \Phi_7 = \emptyset$. Therefore, applying Lemma 5.2 (f) for $j = 7$, (49) is equivalent to $\Phi_6 \cup \Phi_7 = K$.

Assume, on the contrary, that Eq. (49) fails. This means that $\emptyset \neq K \setminus (\Phi_6 \cup \Phi_7) \subseteq K \setminus (B \cup C) = A$ and hence we can find $a \in A \setminus (\Phi_6 \cup \Phi_7)$. By Lemma 5.2 (e) for $j = 1$, it also follows from $q = 1$ the existence of an $\ell \in \mathrm{Loc}_\Phi(a^2) \setminus [2]$. Note that $a \notin \Phi_6 \cup \Phi_7$ ensures that $\ell \notin \{5, 6, 7\}$. In light of Eq. (50), it holds

$$\ell \notin \{3, 6, 9, 10\},$$

$$\emptyset = \Phi_3 \cap \Phi_4 \supseteq A \cap \Phi_4, \quad (51)$$

and

$$\Phi_{10} \subseteq (K \setminus \Phi_1) \cap (K \setminus \Phi_9) \subseteq (K \setminus A) \cap (K \setminus C) = B. \quad (52)$$

It is direct from Eq. (51) that $\ell \neq 4$. We infer from Eq. (52) that $\Phi_4 \supseteq B \supseteq \Phi_{10}$ and hence $\Phi_4 \cap \Phi_{10} = \Phi_{10} \neq \emptyset$. By virtue of $\Phi_{[2,4]} \cap \Phi_{[8,10]} = \emptyset$, we then further derive $(A \times A) \cap \Phi_{[8,9]} \subseteq \Phi_{[2,3]} \cap \Phi_{[8,9]} = \emptyset$, which gives $\ell \neq 8$. To conclude, we have now excluded the possibility of $\ell = x$ for all $x \in \mathbb{Z}/10\mathbb{Z}$, which is a contradiction. This ends the proof of (49), as wanted.

Thanks to Lemma 5.2 (f) for $j = 1$, (49) tells us that $\Phi_{10} \sqcup \Phi_1 = K$. Since $0 \in (\mathbb{Z}/10\mathbb{Z}) \setminus \{4, 5, 6\}$, we see from Eq. (52) and Lemma 5.3 (c) that

$$\Phi_{10} = B. \quad (53)$$

Applying Lemma 5.2 (f) for $j = 1$ and Lemma 5.2 (g) for $j = 7$, respectively, we know from Eq. (49) that

$$\Phi_1 = K \setminus \Phi_{10} = A \cup C \quad \text{and} \quad \Phi_9 = K \setminus \Phi_{10} = A \cup C. \quad (54)$$

Having Eqs. (49) and (54) in hand, it follows from Lemma 5.3 (a) that $\Phi_8 \cap A = \emptyset$. In addition, Eq. (54) also shows that $\Phi_7 \cap \Phi_9 \supseteq C$ and $\Phi_9 \cap \Phi_{11} = A \cup C$, which allows us to conclude from Eq. (53) and $\Phi_{[7,9]} \cap \Phi_{[9,11]} = \emptyset$ that $\emptyset = \Phi_8 \cap \Phi_{10} = \Phi_8 \cap B$. Therefore, it holds that $C \subseteq \Phi_8 \subseteq (K \setminus B) \cap (K \setminus A) = C$, proving that $\Phi_8 = C$. The same conclusion surely applies to the map $\Psi$ with $\Psi_i = \Phi_{-i}$ for all $i \in \mathbb{Z}/10\mathbb{Z}$, giving us $\Phi_2 = \Psi_8 = A$. Accordingly, we arrive at

$$\Phi_8 \cup \Phi_2 = C \cup A. \quad (55)$$

In view of Eq. (50), we have $\Phi_3 \cap \Phi_4 = \Phi_6 \cap \Phi_7 = \emptyset$, and therefore $\Phi_3 \cap B = \emptyset$ and $B \cap \Phi_7 = \emptyset$. Considering that $B \doteq \bigcap_{i=4}^{6} \Phi_i$, this along with Eqs. (53) to (55) shows that $\mathrm{Loc}_\Phi(b) = \{4, 5, 6, 10\}$ for all $b \in B$. By Lemma 2.4, we thus obtain

$$\bigsqcup_{i \in \{5,6,7,10\}} \Phi_{[i,i+1]} = K^2. \quad (56)$$

For all $i \in \mathbb{Z}/10\mathbb{Z}$, let $d_i \doteq \mathrm{DM}(K, K; \Phi_i, \Phi_{i+1})$ and observe that $d_i = 2$. As $\sum_{i \in \{5,6,7,10\}} 2^{-d_i} = 1$, it follows from Theorem 2.8 and Eq. (56) that, for the pairs $(\Phi_7, \Phi_8)$ and $(\Phi_1, \Phi_2)$, we should have either $\Phi_7 = K \setminus \Phi_1$ or $\Phi_8 = K \setminus \Phi_2$. However, Eq. (54) says that $\Phi_7 \cap \Phi_1 = \Phi_7 \cap (A \cup C) \supseteq C \neq \emptyset$, whereas Eq. (55) asserts that $\Phi_8 \cup \Phi_2 = C \cup A \neq K$. This contradiction then completes the proof. □

**Lemma 7.4.** $\mathcal{S}(3, 11) = \emptyset$.

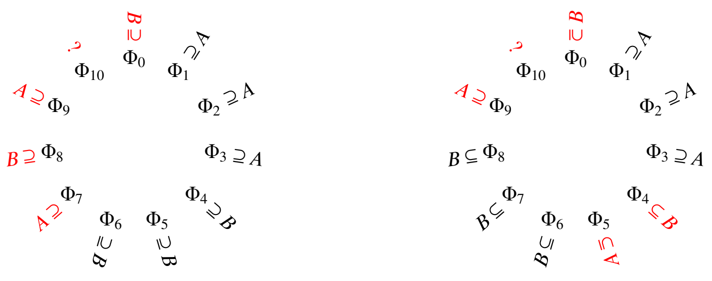
*Proof.* For the sake of contradiction, suppose there is a cyclic decomposition $\Phi$ of $(K^3, K, 3)$ with period 11 for some set $K$. Up to translation of $\Phi$, Lemma 3.4 allows us to restrict our attention to the following five cases.

Case 1. $\mathrm{Diag}_\Phi = \{1, 5\}$.

This is impossible by Lemma 6.1.

Case 2. $\mathrm{Diag}_\Phi = \{1, 4\}$.

We set $A \doteq \bigcap_{i=1}^{3} \Phi_i$ and $B \doteq \bigcap_{i=4}^{6} \Phi_i$, which together form a partition of $K$. From Corollary 3.6 we deduce that $\Phi_0 \subseteq B$ and $\Phi_7 \subseteq A$. We next see from $\Phi_{[6,8]} \cap \Phi_{[0,2]} = \emptyset$ that $\Phi_8 \subseteq B$. We further examine the fact that $\Phi_{[7,9]} \cap \Phi_{[3,5]} = \emptyset$ and can tell from it that $\Phi_9 \subseteq A$. Finally, for the value of $\Phi_{10}$, $\Phi_{[5,7]} \cap \Phi_{[10,12]} = \emptyset$ requires $\Phi_{10} \subseteq A$, while $\Phi_{[9,11]} \cap \Phi_{[2,4]} = \emptyset$ forces $\Phi_0 \subseteq B$; see Fig. 6(a). This is the desired contradiction.



(a) $\mathrm{Diag}_\Phi = \{1,4\}$.
(b) $\mathrm{Diag}_\Phi = \{1,6\}$.

Figure 6: Case 2 and Case 3 in the proof of Lemma 7.4.

Case 3. $\mathrm{Diag}_\Phi = \{1,6\}$.

Let $A \doteq \bigcap_{i=1}^{3} \Phi_i$ and $B \doteq \bigcap_{i=6}^{8} \Phi_i$, which together form a partition of $K$. Corollary 3.6 shows $\Phi_0 \subseteq B, \Phi_4 \subseteq B$, $\Phi_5 \subseteq A$ and $\Phi_9 \subseteq A$. Therefore, from $\Phi_{[7,9]} \cap \Phi_{[10,12]} = \emptyset$ we derive $\Phi_{10} \subseteq A$, while from $\Phi_{[0,2]} \cap \Phi_{[8,10]} = \emptyset$ we get $\Phi_{10} \subseteq B$; see Fig. 6(b). This implies $\Phi_{10} = \emptyset$, in conflict with the definition of a cyclic decomposition.

Case 4. $\mathrm{Diag}_\Phi = \{1,4,7\}$.

By Lemma 5.4, $\mathrm{h}_{\Phi,x}$ takes a constant value for all $x \in K$, say $q$. Let us partition $K$ into three nonempty sets,

$$A \doteq \bigcap_{i=1}^{3} \Phi_i,\ B \doteq \bigcap_{i=4}^{6} \Phi_i,\ \text{and}\ C \doteq \bigcap_{i=7}^{9} \Phi_i \tag{57}$$

It follows from Corollary 3.6 that

$$\Phi_0 \cap \Phi_1 = \Phi_3 \cap \Phi_4 = \Phi_6 \cap \Phi_7 = \Phi_9 \cap \Phi_{10} = \emptyset. \tag{58}$$

Case 4.1. $q = 0$.

Recall from Eq. (58) that $\Phi_6 \cap \Phi_7 = \emptyset$. Hence, in view of Definition 5.1, $q = 0$ along with $7 \in \mathrm{Diag}_\Phi$ means that $B \cup C \subseteq \Phi_6 \cup \Phi_7 \subsetneq K$. This allows us to take $a \in A \setminus (\Phi_6 \cup \Phi_7)$. From $a \notin \Phi_6 \cup \Phi_7$ we obtain $5,6,7 \notin \mathrm{Loc}_\Phi(a^2)$. From Eq. (58) we derive $\{3,6,9,11\} \cap \mathrm{Loc}_\Phi(a^2) = \emptyset$. Taking into account $\emptyset = \Phi_{[1,3]} \cap \Phi_{[10,12]} = \Phi_{[1,3]} \cap \Phi_{[3,5]}$, we see that $10, 4 \notin \mathrm{Loc}_\Phi(a^2)$. By virtue of $A \subseteq \Phi_3, B \subseteq \Phi_4, C \subseteq \Phi_9$, it holds $\Phi_{10} = \Phi_{10} \cap K = \Phi_{10} \cap (\Phi_3 \cup \Phi_4 \cup \Phi_9)$. Observe from Eq. (58) that $\Phi_9 \cap \Phi_{10} = \emptyset$, which shows that either $\Phi_{10} \cap \Phi_3 \neq \emptyset$ or $\Phi_{10} \cap \Phi_4 \neq \emptyset$. Considering that $\Phi_{[8,10]} \cap \Phi_{[1,3]} = \Phi_{[8,10]} \cap \Phi_{[2,4]} = \emptyset$, we now conclude that either $\Phi_{[8,9]} \cap \Phi_{[1,2]} = \emptyset$ or $\Phi_{[8,9]} \cap \Phi_{[2,3]} = \emptyset$. Since $a^2 \in \Phi_{[1,2]} \cap \Phi_{[2,3]}$, we thus find that $8 \notin \mathrm{Loc}_\Phi(a^2)$. The above analysis shows that $\mathrm{Loc}_\Phi(a^2) \setminus [2] = \emptyset$. But, by Lemma 5.2 (b) for $j = 1$, we have $\mathrm{Loc}_\Phi(a^2) \setminus [2] \neq \emptyset$. This is a desired contradiction.

Case 4.2. $q \geq 1$.

Since $q \geq 1$, it follows from Lemmas 5.2 (f) and 5.2 (g) that

$$\Phi_0 \sqcup \Phi_1 = \Phi_3 \sqcup \Phi_4 = \Phi_6 \sqcup \Phi_7 = \Phi_9 \sqcup \Phi_{10} = K; \tag{59}$$

applying Lemma 5.3 (b) for $\ell = 10$ and $j \in \{1,4,7\}$ gives $\Phi_{10} \cap \Phi_{11} \cap A = \Phi_{10} \cap \Phi_{11} \cap B = \Phi_{10} \cap \Phi_{11} \cap C = \emptyset$, namely

$$\Phi_{10} \cap \Phi_{11} = \emptyset; \tag{60}$$

while applying Lemma 5.3 (b) for $\ell = 8$ and $j \in \{1,4\}$ gives

$$C \subseteq \Phi_7 \cap \Phi_8 \subseteq K \setminus (A \cup B) = C \text{ and } C \subseteq \Phi_8 \cap \Phi_9 \subseteq K \setminus (A \cup B) = C; \tag{61}$$

and applying Lemma 5.3 (b) for $\ell = 2$ and $j \in \{4,7\}$ gives

$$A \subseteq \Phi_1 \cap \Phi_2 \subseteq K \setminus (B \cup C) = A \text{ and } A \subseteq \Phi_2 \cap \Phi_3 \subseteq K \setminus (B \cup C) = A. \tag{62}$$

An application of Lemma 5.3 (c) and Eqs. (57) and (59) leads to

$$\begin{cases}\Phi_1 \in \{A, A \sqcup B, A \sqcup C\}, \Phi_0 \in \{B \sqcup C, C, B\}, \Phi_3 \in \{A, A \sqcup C\}, \Phi_4 \in \{B \sqcup C, B\}, \\ \Phi_6 \in \{B, B \sqcup A\}, \Phi_7 \in \{C \sqcup A, C\}, \Phi_9 \in \{C, C \sqcup A, C \sqcup B\}, \Phi_{10} \in \{A \sqcup B, B, A\}.\end{cases} \tag{63}$$

Eqs. (59) and (60) implies that $\Phi_{11} \subseteq K \setminus \Phi_{10} = \Phi_9$ and $\Phi_{10} \subseteq K \setminus \Phi_{11} = \Phi_1$. Thanks to $\Phi_{[9,11]} \cap \Phi_{[0,2]} = \emptyset$ and $\Phi_{[8,10]} \cap \Phi_{[10,12]} = \emptyset$, this allows us to get

$$\Phi_0 \cap \Phi_2 = \emptyset \text{ and } \Phi_8 \cap \Phi_{10} = \emptyset, \tag{64}$$

respectively. It follows from Eqs. (59), (61), (62) and (64) that

$$\begin{cases}\Phi_2 = \Phi_2 \cap (\Phi_0 \sqcup \Phi_1) = (\Phi_2 \cap \Phi_0) \sqcup (\Phi_2 \cap \Phi_1) = \Phi_2 \cap \Phi_1 = A, \\ \Phi_8 = \Phi_8 \cap (\Phi_9 \sqcup \Phi_{10}) = (\Phi_8 \cap \Phi_9) \sqcup (\Phi_8 \cap \Phi_{10}) = \Phi_8 \cap \Phi_9 = C.\end{cases} \tag{65}$$

Comparing Eqs. (60) and (63), we see that either $\Phi_{10} = A$ or $\Phi_0 = C$. Up to replacing $\Phi$ by its reflection $\Psi$ with $\Psi_i = \Phi_{10-i}$ for all $i \in \mathbb{Z}/11\mathbb{Z}$, we may assume that $\Phi_0 = C$ happens. In view of Eqs. (59), (63) and (65), we can depict the current situation in Fig. 7, from which we can see that $\mathrm{Loc}_\Phi(aba) \in \{3, 5\}$ for any $a \in A$ and $b \in B$. For any $a \in A$ and $b \in B$, from $\mathrm{Loc}_\Phi(aba) = 5$ we will easily deduce $aba \in \Phi_{[3,5]} \cap \Phi_{[5,7]}$, which is absurd. Therefore, $\mathrm{Loc}_\Phi(aba) = 3$ for all $(a, b) \in A \times B$. This then tells us that $A \subseteq \Phi_5$ and then $\Phi_7 = C$. By Eq. (59), $\Phi_7 = C$ gives $\Phi_6 = B \sqcup A$, and so $\Phi_5 \cap \Phi_6 \cap A \supseteq A \cap (B \sqcup A) \cap A = A$. Finally, by Lemma 5.3 (b), it should happen $\Phi_5 \cap \Phi_6 \cap A = \emptyset$, which is the required contradiction.

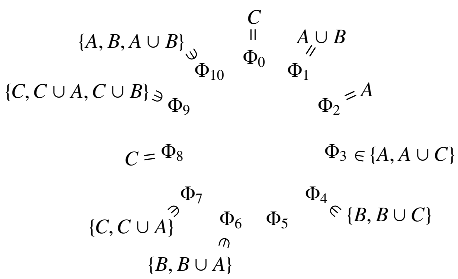



Figure 7: Case 4.2 in the proof of Lemma 7.4.

Case 5. $\mathrm{Diag}_\Phi = \{1, 4, 8\}$.

We set $A \doteq \bigcap_{i=1}^{3} \Phi_i$, $B \doteq \bigcap_{i=4}^{6} \Phi_i$ and $C \doteq \bigcap_{i=8}^{10} \Phi_i$. Corollary 3.6 implies

$$\Phi_i \cap \Phi_{i+1} = \emptyset \text{ for all } i \in \{3, 6, 7, 10, 11\}. \tag{66}$$

As a consequence of Eq. (66), we have

$$\Phi_7 \subseteq (K \setminus \Phi_6) \cap (K \setminus \Phi_8) \subseteq A \tag{67}$$

and

$$\Phi_0 \subseteq (K \setminus \Phi_1) \cap (K \setminus \Phi_{10}) \subseteq B. \tag{68}$$

Case 5.1. $\mathrm{h}_{\Phi,A} \geq 1$.

It follows from Lemma 5.4 that $\mathrm{h}_{\Phi,B} = \mathrm{h}_{\Phi,A} \geq 1$. This enables us utilize Lemmas 5.2 (f) and 5.2 (g) and find that

$$\Phi_6 \sqcup \Phi_7 = K, \Phi_0 \sqcup \Phi_1 = K, \text{ and } \Phi_3 \sqcup \Phi_4 = K. \tag{69}$$

Having in mind Eqs. (67) and (68) additionally, the first two equalities in Eq. (69) yield

$$\Phi_6 \cap \Phi_1 = K \setminus (\Phi_7 \cup \Phi_0) \supseteq K \setminus (A \cup B) = C. \tag{70}$$

We also read from Eq. (68) that $\Phi_5 \cap \Phi_0 \supseteq B \cap \Phi_0 = \Phi_0 \neq \emptyset$. Since $\Phi_{[4,6]} \cap \Phi_{[10,12]} = \emptyset$, this along with Eq. (70) shows that $\emptyset = \Phi_4 \cap \Phi_{10} \supseteq \Phi_4 \cap C$, and thus $\Phi_4 \cap C = \emptyset$. The third equality in Eq. (69), combined with $\Phi_4 \cap C = \emptyset$, then gives

$$\Phi_8 \cap \Phi_3 = \Phi_8 \cap (K \setminus \Phi_4) \supseteq C. \tag{71}$$

Recall from Eq. (67) that

$$\Phi_7 \cap \Phi_2 \supseteq \Phi_7 \cap A = \Phi_7. \tag{72}$$

At last, we conclude from Eqs. (70) to (72) that $\Phi_{[6,8]} \cap \Phi_{[1,3]} \supseteq C \times \Phi_7 \times C \neq \emptyset$, which is a contradiction.

Case 5.2. $\mathrm{h}_{\Phi,A} = 0$.

Pick $a \in A$. As we have $\mathrm{h}_{\Phi,A} = 0$, Lemma 5.2 (e) guarantees the existence of $\ell \in \mathrm{Loc}_\Phi(a^2) \setminus [2]$. It follows from Eq. (66) that $\ell \notin \{3, 6, 7, 10, 11\}$, and that $\emptyset = \Phi_3 \cap \Phi_4 \supseteq A \cap \Phi_4$, which gives $\ell \neq 4$. By Eq. (67), we tell from $\Phi_{[1,3]} \cap \Phi_{[5,7]} = \emptyset$ and $\Phi_{[1,3]} \cap \Phi_{[7,9]} = \emptyset$ that $\ell \neq 5$ and $\ell \neq 8$, respectively. To sum up, it only remains the possibility of $\ell = 9$. For any $b \in \Phi_0$, $\ell = 9$ together with Eq. (68) would imply $a^2 b \in \Phi_{[2,4]} \cap \Phi_{[9,11]}$. This contradiction ends the proof. □

**Lemma 7.5.** $\mathcal{S}(4, 12) = \emptyset$.

*Proof.* Let $K$ be a set and let $\Phi$ be a cyclic decomposition of $(K^4, K, 4)$ with period 12. Let us work towards a contradiction.

By Lemma 3.5 (b) and Theorem 2.11, we have $\Phi^\#_< \geq 3$ and $\Phi^\#_< \leq \lfloor \log_2(12) \rfloor = 3$, respectively. Hence, the deflation number of $\Phi$ is exactly three. In view of Lemma 2.5, we may thus assume that $\Phi_i = K$ if and only if $i \in \{3, 7, 11\}$. By Corollary 3.6, we then obtain $\mathrm{Diag}_\Phi \cap \{3, 7, 11\} = \mathrm{Diag}_\Phi \cap \{0, 4, 8\} = \emptyset$. Up to equivalence, there is thus no loss of generality in assuming that $1 \in \mathrm{Diag}_\Phi$. Furthermore, we can apply Lemmas 3.4 and 6.6 and find that $|\mathrm{Diag}_\Phi| = 2$ and that $1 \in \mathrm{Diag}_\Phi \subseteq \{1, 5, 6, 9\}$. Since $1 \in \mathrm{Diag}_\Phi$, it then follows from Lemma 6.1 that $\mathrm{Diag}_\Phi \in \{\{1, 5\}, \{1, 9\}\}$. Let $\Psi$ be the reflection of $\Phi$ such that $\Psi_i = \Phi_{2-i}$ for all $i \in \mathbb{Z}/12\mathbb{Z}$. Replacing $\Phi$ by $\Psi$ if necessary, we can always assume that $\mathrm{Diag}_\Phi = \{1, 5\}$.

Set $B \doteq \bigcap_{i=5}^{8} \Phi_i$ and $C \doteq \bigcap_{i=1}^{4} \Phi_i$. Utilizing Lemma 3.5 (a) for $i \doteq 5$ and $j \doteq 2$ yields $j_1 \in \Phi^5_< = \{0, 1, 3\}$ such that $\Phi_{7+j_1} \cap B = \emptyset$. Since $B \subseteq \Phi_7 \cap \Phi_8$, we must have $j_1 = 3$ and thus $\Phi_{10} \cap B = \emptyset$ follows. We continue to apply Lemma 3.5 (a) for $i \doteq 1$ and $j \doteq 3$ and then get the existence of $j_2 \in \Phi^1_< = \{0, 1, 3\}$ such that $\Phi_{1-3+j_2} \cap C = \emptyset$. Since $\Phi_{-2+1} = \Phi_{11} = K \supseteq C$ and $\Phi_{-2+3} = \Phi_1 \supseteq C$, we must have $j_2 = 0$ and thus $\Phi_{10} \cap C = \emptyset$. We have seen now $\Phi_{10} \cap B = \Phi_{10} \cap C = \emptyset$. But $B \sqcup C = K$, and so $\Phi_{10} = \emptyset$ follows, which is a contradiction. □

**Lemma 7.6.** $\mathcal{S}(6, 18) = \emptyset$.

*Proof.* Let us assume that the statement is false, namely there is a cyclic decomposition $\Phi$ of $(K^6, K, 6)$ with period 18 for some set $K$.

By Lemmas 3.4 (b), 3.4 (c) and 6.6, we have $|\mathrm{Diag}_\Phi| = 2$. Up to a possible translation of $\Phi$, we may assume that $\mathrm{Diag}_\Phi = \{1, \ell\}$ for some $\ell \in [2, 10]$. From Lemmas 3.4 (a) and 6.1 we then conclude that

$$\mathrm{Diag}_\Phi \in \{\{1, 7\}, \{1, 9\}, \{1, 10\}\}. \tag{73}$$

By Lemma 3.5 (a) for $(i, j) \doteq (1, 1)$, there is a $j_1 \in \Phi^1_< \subseteq \langle 5 \rangle$ such that $j_1 - 5 = j + j_1 - t \in \Phi^1_< \subseteq \langle 5 \rangle$. This forces $j_1 = 5$. Note that Corollary 3.6 has ensured that $0 \in \Phi^1_<$. Thus, we indeed have

$$\{0, 5\} \subseteq \Phi^1_<. \tag{74}$$

By applying Lemma 3.5 (a) for $(i, j) \doteq (1, 2)$, we find the existence of a $j_1 \in \Phi^1_< \subseteq \langle 5 \rangle$ satisfying $j_1 - 4 = j + j_1 - t \in \Phi^1_< \subseteq \langle 5 \rangle$. Therefore, it holds $j_1 \in \{4, 5\}$. As $\{4, 1\} = \{4, 5 - 4\}$, we see that

$$\{4, 1\} \cap \Phi^1_< \neq \emptyset. \tag{75}$$

Applying Lemma 3.5 (a) for $(i, j) \doteq (1, 4)$ yields some $j_1 \in \Phi^1_< \subseteq \langle 5 \rangle$ such that $j_1 - 2 = j + j_1 - t \in \Phi^1_< \subseteq \langle 5 \rangle$. It follows that $(j_1 - 2, j_1) \in \{(0, 2), (1, 3), (2, 4), (3, 5)\}$, and hence

$$\{2, 3\} \cap \Phi^1_< \neq \emptyset. \tag{76}$$

Theorem 2.11 asserts $\Phi^{\#}_{<} \le \lfloor \log_2(18) \rfloor = 4$. This combined with Eqs. (74) to (76) shows that $\Phi^{\#}_{<} = 4$ and $\langle 5\rangle \setminus \Phi^1_{<} \in \{\{4,2\},\{1,2\},\{4,3\},\{1,3\}\}$. By Definition 2.1 and Lemma 2.5, we have

$$\{i \in \mathbb{Z}/18\mathbb{Z} :\ \Phi_i = K\} = \begin{cases} \{3,5,9,11,15,17\}, & \text{if } \langle 5\rangle \setminus \Phi^1_{<} = \{4,2\},\\ \{2,3,8,9,14,15\}, & \text{if } \langle 5\rangle \setminus \Phi^1_{<} = \{1,2\},\\ \{4,5,10,11,16,17\}, & \text{if } \langle 5\rangle \setminus \Phi^1_{<} = \{4,3\},\\ \{2,4,8,10,14,16\}, & \text{if } \langle 5\rangle \setminus \Phi^1_{<} = \{1,3\}. \end{cases} \tag{77}$$

Moreover, Corollary 3.6 and Eqs. (73) and (77) demonstrate that

$$\mathrm{Diag}_{\Phi} = \begin{cases} \{1,7\}, & \text{if } \langle 5\rangle \setminus \Phi^1_{<} = \{4,2\},\\ \{1,7\}, & \text{if } \langle 5\rangle \setminus \Phi^1_{<} = \{1,2\},\\ \{1,7\} \text{ or } \{1,9\}, & \text{if } \langle 5\rangle \setminus \Phi^1_{<} = \{4,3\},\\ \{1,7\}, & \text{if } \langle 5\rangle \setminus \Phi^1_{<} = \{1,3\}. \end{cases} \tag{78}$$

Eqs. (77) and (78) allow us to divide our further analysis into the following five cases.

Case 1. $\Phi^1_{<} = \{0,1,3,5\}$ and $\mathrm{Diag}_{\Phi} = \{1,7\}$.

We set $A \doteq \bigcap_{i=1}^{6} \Phi_i$ and $B \doteq \bigcap_{i=7}^{12} \Phi_i$. By applying Lemma 3.5 (a) with $(i,j) \doteq (7,2)$, we find the existence of a $j_1 \in \Phi^7_{<} = \{0,1,3,5\}$ such that $j_1 - 4 = j_1 + j - t \in \Phi^7_{<} = \{0,1,3,5\}$ and that $\Phi_{i+j_1+j} \cap B = \emptyset$. This forces $j_1 = 5$, and hence $\Phi_{14} = \Phi_{7+5+2} \subseteq K \setminus B = A$. By putting $(i,j) \doteq (1,5)$ in Lemma 3.5 (a), we obtain the existence of a $j_2 \in \Phi^1_{<} = \{0,1,3,5\}$ such that $j_2 + 1 = j_2 - j + t \in \Phi^1_{<} = \{0,1,3,5\}$ and that $\Phi_{i+j_2-j} \cap A = \emptyset$. This forces $j_2 = 0$, and hence $\Phi_{14} = \Phi_{1+0-5} \subseteq K \setminus A = B$. As a result, it holds $\Phi_{14} = \emptyset$, yielding a contradiction!

Case 2. $\Phi^1_{<} = \{0,3,4,5\}$ and $\mathrm{Diag}_{\Phi} = \{1,7\}$.

We set $A \doteq \bigcap_{i=1}^{6} \Phi_i$ and $B \doteq \bigcap_{i=7}^{12} \Phi_i$. Applying Lemma 3.5 (a) for $(i,j) \doteq (7,4)$, we conclude that there exists a $j_1 \in \Phi^7_{<} = \{0,3,4,5\}$ such that $j_1 - 2 = j_1 + j - t \in \Phi^7_{<} = \{0,3,4,5\}$ and that $\Phi_{i+j_1+j} \cap B = \emptyset$. It is obvious that we must have $j_1 = 5$, and hence $\Phi_{16} = \Phi_{7+5+4} \subseteq K \setminus B = A$. Putting $(i,j) \doteq (1,3)$ in Lemma 3.5 (a) yields the existence of a $j_2 \in \Phi^1_{<} = \{0,3,4,5\}$ such that $j_2 + 3 = j_2 - j + t \in \Phi^1_{<} = \{0,3,4,5\}$ and that $\Phi_{i+j_2-j} \cap A = \emptyset$. Note that the only possibility is $j_2 = 0$, and hence $\Phi_{16} = \Phi_{1+0-3} \subseteq K \setminus A = B$. At this moment, we find that $\Phi_{16} = \emptyset$, violating the fact that $\Phi$ is a cyclic decomposition.

Case 3. $\Phi^1_{<} = \{0,1,2,5\}$ and $\mathrm{Diag}_{\Phi} = \{1,7\}$.

Let $\Psi$ be a reflection of $\Phi$ satisfying $\Phi_i = \Psi_{13-i}$ for all $i \in \mathbb{Z}/18\mathbb{Z}$. Applying the conclusion in Case 2 on the cyclic decomposition $\Psi$, we see that the assumption in this case will cause a contradiction.

Case 4. $\Phi^1_{<} = \{0,1,2,5\}$ and $\mathrm{Diag}_{\Phi} = \{1,9\}$.

We set $A \doteq \bigcap_{i=1}^{6} \Phi_i$ and $B \doteq \bigcap_{i=9}^{14} \Phi_i$. By substituting $(i,j) \doteq (1,2)$ in Lemma 3.5 (a), we find the existence of $j_1 \in \Phi^1_{<} = \{0,1,2,5\}$ such that $j_1 - 4 = j_1 + j - t \in \Phi^1_{<} = \{0,1,2,5\}$ and that $\Phi_{i+j_1+j} \cap A = \emptyset$. This forces $j_1 = 5$, and hence $\Phi_8 = \Phi_{1+5+2} \subseteq B$. Consequently, for any $b \in B$ it holds $b^6 \in \Phi_{[8,13]} \cap \Phi_{[9,14]} = \emptyset$, which is absurd.

Case 5. $\Phi^1_{<} = \{0,2,4,5\}$ and $\mathrm{Diag}_{\Phi} = \{1,7\}$.

Let $\Psi$ be a reflection of $\Phi$ satisfying $\Phi_i = \Psi_{13-i}$. We can reach a contradiction by utilizing the analysis in Case 1 on the cyclic decomposition $\Psi$, and thus we are done. □

**Lemma 7.7.** $\mathcal{S}(7,21) = \emptyset$.

*Proof.* To the contrary, suppose that we have a cyclic decomposition $\Phi$ of $(K^7, K, 7)$ with period 21 for some set $K$. Without loss of generality, we may assume that $1 \in \mathrm{Diag}_{\Phi}$.

Theorem 2.11 implies that $\Phi^{\#}_{<} \le \lfloor \log_2(21) \rfloor = 4$. According to Lemma 3.5 (a), the possible value of $\Phi^1_{<}$ has many additional constraints; a computer enumeration based on Lemma 3.5 (a) now shows that $\Phi^1_{<} \in \{\{0,1,4,6\},\{0,2,5,6\}\}$. Up to reflection, let us suppose that $\Phi^1_{<} = \{0,1,4,6\}$.

Take $a \in \bigcap_{i\in[7]} \Phi_i$. By applying Lemma 3.5 (a) with $i \doteq 1$ and $j = 1, 2, 5$, respectively, we find the existence of $j_1 \in \Phi^1_< = \{0, 1, 4, 6\}$ such that $j_1 + j - t \in \Phi^1_< = \{0, 1, 4, 6\}$ and that $a \notin \Phi_{i+j_1+j}$. In all cases, we have $j_1 = 5$, and hence

$$a \notin \Phi_8 \cup \Phi_9 \cup \Phi_{12}. \tag{79}$$

In addition, by applying Lemma 3.5 (a) with $i \doteq 1$ and $j \in \{1, 3, 6\}$, we find the existence of $j_2 \in \Phi^1_< = \{0, 1, 4, 6\}$ such that $j_2 - j + t \in \Phi^1_< = \{0, 1, 4, 6\}$ and that $a \notin \Phi_{i+j_2-j}$. In all cases, we conclude that $j_2 = 0$, and hence

$$a \notin \Phi_{16} \cup \Phi_{19} \cup \Phi_{21}. \tag{80}$$

Taking Eqs. (79) and (80) into account, we find that $\mathrm{Loc}_\Phi(a^4) \subseteq [4]$. By Lemma 5.2 (b), this implies that

$$\mathrm{h}_{\Phi,a} \geq 3. \tag{81}$$

On the other hand, let $d_i \doteq \mathrm{DM}(K, K, K; \Phi_i, \Phi_{i+1}, \Phi_{i+2})$ for all $i \in \mathbb{Z}/(21\mathbb{Z})$. It follows from $\Phi^1_< = \{0, 1, 4, 6\}$ and Lemma 2.5 that $d_5 = d_6 = d_8 = 2$ and $d_7 = 3$, and hence $\sum_{i\in\{5,6,7,8\}} 2^{-d_i} < 1$. Thereby, we derive from Theorem 2.8 that $\bigsqcup_{j\in\langle 3\rangle}(\Phi_{j+5} \times \Phi_{j+6} \times \Phi_{j+7}) \neq K^3$. By Lemma 5.2 (g), this means that $\mathrm{h}_{\Phi,a} \leq 2$. This violates Eq. (81) and so the proof is completed. □

**Lemma 7.8.** $\mathcal{S}(11, 33) = \emptyset$.

*Proof.* Let $\Phi$ be a cyclic decomposition of $(K^{11}, K, 11)$ with period 33. According to Lemma 3.5 (b) and Theorem 2.11, it holds $\Upsilon(11) \leq \Phi^\#_< \leq \lfloor \log_2(33) \rfloor = 5$. However, Lemma 3.2 (d) asserts that $\Upsilon(11) = 6$, yielding a contradiction. □

| $r$ | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|
| $2r$ | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 |
| $3r$ | 12 | 15 | 18 | 21 | 24 | 27 | 30 | 33 |
| $\rho_r$ | 8 | 16 | 16 | 16 | 32 | 32 | 32 | 32 |

Table 1: $\rho_r \doteq 2^{\left\lceil \sqrt{2r-\frac{7}{4}}+\frac{1}{2} \right\rceil}$.

*Proof of Theorem 1.9.* The case of $t = 1$ is trivial. Theorem 1.4 (c) shows that $\mathcal{PS}(2) \cap [7] = \{1, 4\}$. We deduce from Theorem 1.6 (a) that $\mathcal{PS}(3) \cap [2, 7] = \emptyset$. Lemma 4.2 (a) shows that $\mathcal{S}(3, 8) \neq \emptyset$. Recall from Lemmas 7.2 to 7.4 that $\mathcal{S}(3, 9) = \mathcal{S}(3, 10) = \mathcal{S}(3, 11) = \emptyset$. Therefore, we have $\mathcal{PS}(3) \cap [11] = \{1, 8\}$.

Let us assume that $t \geq 4$ and pick $p \in (\mathcal{PS}(t) \cap [4t - 1]) \setminus \{1\}$. Our task is to show that the only possibility is $(t, p) = (4, 8)$.

Simple calculus shows that $2^x \geq x^2$ for all real numbers $x \geq 4$. Thereby, $2^{\lceil 2\sqrt{t}\rceil} - 4t \geq 2^{2\sqrt{t}} - 4t \geq 0$ follows. In view of Theorem 1.6 (b), we now know that $t \mid p$. Due to $p \in [4t - 1]$, $t > 1$ and $t \mid p$, it happens $p \in \{2t, 3t\}$.

Note that $2^{\sqrt{25\times 2\times 16}} = 2^{\sqrt{800}} > 2^{\sqrt{786}} = 2^{28} = 268435456 > 254803968 = 48^5$, that is, $2^{\sqrt{2r}} > 3r$ for $r = 16$. Calculating the derivative of the function $2^{\sqrt{2r}} - 3r$ with respect to $r$ then shows that $2^{\sqrt{2r}} > 3r$ holds for all $r \geq 16$. It thus comes from Theorem 1.6 (a) that $t \leq 15$.

For those integers $r$ satisfying $12 \leq r \leq 15$, we can check that $2^{\left\lceil \sqrt{2r-\frac{7}{4}}+\frac{1}{2} \right\rceil} = 2^6 > 3 \times 16 > 3r$. Henceforth, Lemma 3.8 excludes the possibility of $12 \leq t \leq 15$.

For those integers $r$ with $4 \leq r \leq 11$, we list $2r$, $3r$ and $\rho_r \doteq 2^{\left\lceil \sqrt{2r-\frac{7}{4}}+\frac{1}{2} \right\rceil}$ in Table 1. We read from Table 1 that $2r \geq \rho_r$ only if $r = 4$, while $3r \geq \rho_r$ only if $r \in \{4, 6, 7, 11\}$. According to Lemma 3.8, this means that $(t, p) \in \{(4, 8), (4, 12), (6, 18), (7, 21), (11, 33)\}$. By Lemmas 7.5 to 7.8, we have $\mathcal{S}(4, 12) = \mathcal{S}(6, 18) = \mathcal{S}(7, 21) = \mathcal{S}(11, 33) = \emptyset$. Note that Example 1.3 claims that $\mathcal{S}(4, 8) \neq \emptyset$. This then proves that $(t, p) = (4, 8)$, as was to be shown. □

## 8. Further questions and remarks

A good understanding of cyclic decomposition should mean a good knowledge about $\mathcal{U}$ as given in Definition 1.1 as well as its three projections as described in Definition 7.1. Our paper has chosen to investigate more about $\mathcal{PS}(t)$ and a study of $\mathcal{U}$ from many other perspectives is still left open. What is the relationship between $\mathcal{PS}(t)$ and $\mathcal{PT}(k)$? Is there any symmetry relationship or any principle of uncertainty between them?

A **numerical semigroup** is a set of nonnegative integers that is closed under addition, contains 0, and whose complement in $\mathbb{N}_0$ is a finite set [ADGS20, BCDF20, RGS09]. Let $t \in \mathbb{N}$. Note that $1 \in \{0\} \cup \mathcal{PS}(t)$ and that $\{0\} \cup \mathcal{PS}(t) = \mathbb{N}_0$ if and only if $t = 1$. Therefore, $\{0\} \cup \mathcal{PS}(t)$ is a numerical semigroup if and only if $t = 1$. Recall the definition of $\mathcal{PS}^*(t)$ and $\mathcal{QS}^*(t)$ from Definition 4.1 and Eq. (9), respectively. Let us put $\mathcal{PS}^\star(t) \doteq \mathcal{PS}^*(t) \cup \{0\}$ and $\mathcal{QS}^\star(t) \doteq \mathcal{QS}^*(t) \cup \{0\}$.

**Lemma 8.1.** *For every $t \in \mathbb{N}$, $\mathcal{QS}^\star(t)$ is a numerical semigroup.*

*Proof.* Lemmas 4.5 (b) and 4.5 (c) claim that $\mathcal{QS}^\star(t)$ is closed under addition, and Lemma 4.11 shows that $\mathbb{N}_0 \setminus \mathcal{QS}^\star(t)$ is a finite set. This completes the proof. □

**Question 8.2.** *Let t be a positive integer. Is $\mathcal{PS}^\star(t)$ a numerical semigroup? Note that Lemma 4.11 says that $\mathbb{N}_0 \setminus \mathcal{PS}^\star(t)$ is finite.*

Take $t, p \in \mathbb{N}$. Let $K$ and $L$ be two sets and let $\Phi$ and $\Psi$ be two cyclic decompositions of $(K^t, K, t)$ and $(L^t, L, t)$ with period $p$, respectively. We say that $\Phi$ **represents** $\Psi$ if there is a map $\beta : K \to 2^L \setminus \emptyset$ such that $\{\beta(a) : a \in K\}$ is a partition of $L$ and for every $i \in [p]$, it holds $\bigcup_{x\in\Phi_i} \beta(x) = \Psi_i$. We also say that $\Psi$ is a **blow-up** of $\Phi$. For every $(t, p) \in \mathbb{N}^2$, let $\kappa_{t,p}$ be the minimum nonnegative integer such that every cyclic decomposition of $(K^t, K, t)$ with period $p$ can be represented by a cyclic decomposition of $([\kappa_{t,p}]^t, [\kappa_{t,p}], t)$ with period $p$. If there does not exist any cyclic decomposition of $(K^t, K, t)$ with period $p$ for some set $K$, we adopt the convention that $\kappa_{t,p} \doteq 0$.

*Remark* 8.3. Let $\Phi$ be a cyclic decomposition of $(K, K^t, t)$ with period $p$.

(a) Assume $t = 1$. It is clear that $\bigsqcup_{i\in[p]} \Phi_i = K$, and hence $\Phi$ can be represented by a cyclic decomposition of $([p], [p], 1)$ with period $p$. Therefore, we have $\kappa_{1,p} = p$.

(b) In general, we can assume, without loss of generality that, for every $J \subseteq \mathbb{Z}/p\mathbb{Z}$, $(\bigcap_{i\in J} \Phi_i) \setminus (\bigcup_{i\in[p]\setminus J} \Phi_i)$ contains at most one element. With this assumption, we are reduced to the case of $|K| \le 2^p$. It thus follows that $\kappa_{t,p} \le 2^p$. Note that we have used this argument in the proof of Lemma 3.4.

It is not too hard to prove that $\liminf_{p\to\infty} \frac{t}{p}\kappa(t, p) \ge 1$ for every $t \in \mathbb{N}$. However, we still have no clue about how to tackle the following conjecture. Anyhow, with the help of Lemma 6.2, a positive solution to Question 8.5 might be useful in tackling Conjecture 8.4.

**Conjecture 8.4.** $\limsup_{t,p\to\infty} \frac{t}{p}\kappa_{t,p}$ *is finite.*

**Question 8.5.** *Let t, k and p be positive integers with $p > tk$. Let M be a matroid and let $\phi_i, i \in \mathbb{Z}/p\mathbb{Z}$, be a circular sequence of elements of M. Let $\Xi \doteq \{\Lambda \subseteq \mathbb{Z}/p\mathbb{Z} : \Lambda \cap (j + \langle t-1\rangle) \neq \emptyset$ for every $j \in \mathbb{Z}/p\mathbb{Z}\}$. Assume that the rank of the set $\{\phi_i : i \in \Lambda\}$ in M is at most k for all $\Lambda \in \Xi$. Is it true that the rank of $\{\phi_i : i \in \mathbb{Z}/p\mathbb{Z}\}$ in M has an $O(k)$ upper bound?*

We call two cyclic decompositions $\Phi'$ and $\Psi'$ **quasiequivalent** provided there are two equivalent cyclic decompositions $\Phi$ and $\Psi$ such that $\Phi'$ and $\Psi'$ are blow-ups of $\Phi$ and $\Psi$, respectively. For any $t, p \in \mathbb{N}$, we write $\pi_{t,p}$ for the maximum of those positive integers $m$ such that we can find $m$ cyclic decompositions of order $t$ and period $p$ which are pairwise non-quasiequivalent. It follows from Remark 8.3 (b) that $\pi_{t,p} < \infty$. It may be of special interest to determine those $(t, p) \in \mathbb{N}^2$ with $\pi_{t,p} = 1$ or those with $\pi_{t,p} = 0$. In Example 8.6, we shall show that the function $\Phi$ listed in Example 1.3 is essentially the only cyclic decomposition of order 4 and period 8, namely $\pi_{4,8} = 1$.

*Example* 8.6. Let $K$ be a set. Let $\Phi$ be a cyclic decomposition of $(K^4, K, 4)$ with period 8. Then Lemma 3.4 shows that $\mathrm{Diag}_\Phi = \{i, i+4\}$ for some $i \in \mathbb{Z}/8\mathbb{Z}$. Up to translation, we can assume that $\mathrm{Diag}_\Phi = \{1, 5\}$. It follows from Lemma 2.5 that $\Phi^1_< = \Phi^5_<$. Let $M \doteq \langle 3\rangle \setminus \Phi^1_< = \langle 3\rangle \setminus \Phi^5_<$. Theorem 2.11 shows that $|M| \ge 1$. Corollary 3.6 shows that $0, 3 \notin M$.

If it holds $\{1,2\} \subseteq M$, then one can check that $\Phi_{[2,5]} \cap \Phi_{[0,3]} \neq \emptyset$, violating the fact that $\Phi$ is a cyclic decomposition. Accordingly, $M = \{1\}$ or $\{2\}$. Let $\Psi$ be the reflection of $\Phi$ with $\Phi_i = \Psi_{5-i}$ for all $i \in \mathbb{Z}/10\mathbb{Z}$. Considering $\Psi$ instead if necessary, We can assume that $\{2\} = M$. Let $A \doteq \bigcap_{i\in[4]} \Phi_i$ and $B \doteq \bigcap_{i\in[4]} \Phi_{i+4}$. For every $x, y \in \mathbb{Z}/8\mathbb{Z}$, there exists $z \in \{x, x+4\}$ such that $z - y \in \langle 3 \rangle$. Consequently, Lemma 6.2 shows that $(\Phi_x, \Phi_{x+4}) \in \{(A, B), (B, A), (K, K)\}$ for every $x \in \mathbb{Z}/8\mathbb{Z}$. It further follows that

$$\Phi_x = \begin{cases} A, & \text{if } x \in \{1,2,4\}; \\ B, & \text{if } x \in \{5,6,8\}; \\ A \sqcup B = K, & \text{if } x \in \{3,7\}. \end{cases} \tag{82}$$

Eq. (82) tells us that $\pi_{4,8} = 1$ and $\kappa_{4,8} = 2$. Due to the symmetry between $A$ and $B$, we may say that $\Phi_{[i,i+3]}$ and $\Phi_{[i+4,i+7]}$ form an "antipodal pair" for all $i \in \mathbb{Z}/8\mathbb{Z}$. Using the 'joker' symbol as adopted in [CKMS17b], we can write $(\Phi_{[1,4]}, \Phi_{[5,8]}) = (AA \diamond A, BB \diamond B)$, $(\Phi_{[2,5]}, \Phi_{[6,9]}) = (A \diamond AB, B \diamond BA)$, $(\Phi_{[3,6]}, \Phi_{[6,9]}) = (\diamond ABB, \diamond BAA)$, $(\Phi_{[4,7]}, \Phi_{[7,10]}) = (ABB\diamond, BAA\diamond)$.

At the end of [CKMS17b, § 2.3], Chen et al. mentioned that Example 1.3 is essentially the only binary cyclic universal partial word which they were aware of. Fillmore et al. [FGK+23, Theorem 3.1] recently found seven inequivalent binary cyclic universal partial words of order 8 and period 128. We mention that the 8-intervals of the 3rd and 4th examples constructed in the proof of [FGK+23, Theorem 3.1] both consist of 64 antipodal pairs. The work of Fillmore et al. [FGK+23] makes use of astute graphs and their Euler tours, namely perfect necklaces. Note that astute graphs are nothing but generalized wrapped butterflies [DW05, Pra89, WL02]. Can we find more binary cyclic universal partial words? Especially, any more such words which provide us antipodal pairs as we see in Example 8.6?

Let $K$ be a set with at least three elements. Let $\Phi_1, \ldots, \Phi_{p+t-1}$ be a sequence of elements from $\{K\} \cup \binom{K}{1}$ such that $K^t = \bigsqcup_{i=1}^{p} (\Phi_i \times \Phi_{i+1} \times \cdots \times \Phi_{i+t-1})$. Goeckner et al. [GGH+18, Theorem 4.8] proved that we must have $\Phi_i = \Phi_{i+p}$ for all $i \in [t-1]$, that is, $\Phi_1, \ldots, \Phi_p$ provide a cyclic decomposition of $(K^t, K, t)$. Can we strengthen this result by relaxing the condition of $\Phi_i \in \{K\} \cup \binom{K}{1}$?

Let $\Phi$ be a cyclic decomposition of $(K^t, K, t)$ with period $p \geq 2$. In case that $\Phi$ is a cyclic universal partial word as introduced in Remark 1.10, Goeckner et al. [GGH+18, Definition 4.2] defined the diamondicity of $\Phi$ to be $t - \Phi^\#_<$. Lemma 3.5 (b) shows that $\Phi^\#_< \geq \sqrt{2t}$, which can be viewed as an extension of [GGH+18, Proposition 4.7] for cyclic universal partial words. We should mention that Goeckner et al. [GGH+18, Question 6.3] asked if any $\Omega(t)$ lower bound for $\Phi^\#_<$ can be established, where they required $\Phi$ to be a cyclic universal partial word and stated the problem in terms of diamondicity. To which extent can we improve Lemma 3.5 (b) for general cyclic decompositions?

Kiefer and Ryzhikov [KR24] studied the complexity of computing the period and exponent of a digraph. We think that various corresponding complexity problems about the hydras should be studied as well.

Let $t$ be a positive integer. Theorem 1.9 determines $\mathcal{PS}(t) \cap [4t-1]$. By virtue of Lemma 3.8, $4t \in \mathcal{PS}(t)$ will imply that $t \in [11] \cup \{16\}$. For $t = 1$, it is clear that $4 \in \mathcal{PS}(1)$. For $t = 2$, Theorem 1.4 (c) gives $8 \in \mathcal{PS}(2)$. For $t = 4$, Lemma 4.2 (a) confirms that $16 \in \mathcal{PS}(4)$. Analogous to Lemma 7.8, we can verify that $4t \notin \mathcal{PS}(t)$ for any $t \in \{11, 16\}$. When $t \in \{3,5,6,7,8,9,10\}$, we have not checked whether or not $4t \in \mathcal{PS}(t)$.

The characterization of the extremal family of subboxes as discussed in Theorem 2.8 is useful in our study of periods; see Lemmas 5.5 and 7.3. Is there any alternative equality characterization? There have been quite some further extensions or variants of the work in [ABHK02], say [AP24, BLLW19, GKP04, GRV15, Hol19, KP08]. In addition to Remark 2.12, we like to mention that [GKP04, Theorem 3] and [Hol19, Theorem 2] are both about the structure of extremal subbox families. The difference between our hydra period problem and the widely studied problem of partitioning a box into subboxes [ABHK02] is that we impose some consecutive constraint on the subboxes. Analogous to the minimum partition problem, a natural problem is to determine $\min \mathcal{PS}(t) \setminus \{1\}$. Note that Theorem 1.9 gives some very rough information on this parameter.

Many combinatorial objects of a flavor similar to cyclic decompositions have been studied in the literature [BMMT23, BSSSW10, GHS22, KNP24, MEY21, MEY23, QWX22]. To conclude the paper, let us suggest the following definition, which somehow unifies our cyclic decomposition as stated in Definition 1.1 and the definition of universal partial cycles for permutations [CDG92, CFH+14, KLSS23, KPV19].

**Definition 8.7.** Let $t$ be a positive integer and let $K$ be a set. Let $\sim$ be an equivalence relation on $K^t$, and let $X$ be a subset of $K^t$. For every $x \in K^t$, we use $[x]_\sim$ for the equivalence class of $\sim$ containing $x$. A **cyclic decomposition** of

$(X, \sim, K, t)$ with **period** $p \in \mathbb{N}$ is a map $\Phi : \mathbb{Z}/p\mathbb{Z} \to 2^K \setminus \emptyset$ together with a map $\mathrm{Loc}_\Phi : X \to \mathbb{Z}/p\mathbb{Z}$ such that, for every $x \in X$, $[x]_\sim \cap \prod_{i=j}^{j+t-1} \Phi_i \neq \emptyset$ holds if and only if $j = \mathrm{Loc}_\Phi(x)$.

**Acknowledgement** We thank Sergey Kitaev for drawing our attention to the large body of research work on universal partial words and related combinatorial objects, and we thank Ron Holzman for providing us relevant literature on partitioning a box into subboxes.

Yao Ting Zhang (22 November 1933 – 29 June 2007) wrote many articles about his teacher, Pao-Lu Hsü (1 September 1910 – 18 December 1970). We know from his articles that Hsü organized seminars on Markov chains, combinatorial designs, and experimental designs during different periods in last fifties and sixties. It is said that Hsü focused on combinatorics in his last few years and made a research plan, which unfortunately could not be finished due to his poor health in those difficult days. Under the instruction of Hsü, Zhang prepared a report on partially balanced incomplete block design, which was published in Chinese in 1964 under the pseudonym Cheng Ban. This pseudonym refers to all participants of Hsü's combinatorics seminar. In 2005, we did plan to find an opportunity to meet Zhang and learn more from him about Hsü's research project. Sadly, we were notified that he was already not in good physical condition and so an academic meeting was not suitable. With the desire to understand some combinatorial aspects of Markov chains, this paper continues our journey in 2017 and carries some classical design theoretic flavor. We dedicate this work to the memory of Pao-Lu Hsü and Yao Ting Zhang, although we will never know what Zhang may have shareed with us if we had the luck of meeting him before 2004.

## References

[ABHK02] Noga Alon, Tom Bohman, Ron Holzman, and Daniel J. Kleitman. On partitions of discrete boxes. *Discrete Math.*, 257(2-3):255–258, 2002. Kleitman and combinatorics: a celebration (Cambridge, MA, 1999). doi:10.1016/S0012-365X(02)00428-4.

[ADGS20] Abdallah Assi, Marco D'Anna, and Pedro A. García-Sánchez. *Numerical Semigroups and Applications*, volume 3 of *RSME Springer Series*. Springer, Cham, 2020. Second edition. doi:10.1007/978-3-030-54943-5.

[AP24] Eyal Ackerman and Rom Pinchasi. On partitions of two-dimensional discrete boxes. *Discrete Math.*, 347(4):Paper No. 113848, 8, 2024. doi:10.1016/j.disc.2023.113848.

[BB99] Jean Berstel and Luc Boasson. Partial words and a theorem of Fine and Wilf. *Theoret. Comput. Sci.*, 218(1):135–141, 1999. WORDS (Rouen, 1997). doi:10.1016/S0304-3975(98)00255-2.

[BCDF20] Valentina Barucci, Scott Chapman, Marco D'Anna, and Ralf Fröberg, editors. *Numerical Semigroups*, volume 40 of *Springer INdAM Series*. Springer, Cham, 2020. IMNS 2018. doi:10.1007/978-3-030-40822-0.

[BLLW19] Matija Bucic, Bernard Lidický, Jason Long, and Adam Zsolt Wagner. Partition problems in high dimensional boxes. *J. Combin. Theory Ser. A*, 166:315–336, 2019. doi:10.1016/j.jcta.2019.02.011.

[BMMT23] Matthew Baker, Bhumika Mittal, Haran Mouli, and Eric Tang. On the existence of balanced generalized de Bruijn sequences. *Discrete Math.*, 346(9):Paper No. 113487, 5, 2023. doi:10.1016/j.disc.2023.113487.

[BR91] Richard A. Brualdi and Herbert J. Ryser. *Combinatorial Matrix Theory*, volume 39 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1991. doi:10.1017/CBO9781107325708.

[Bra42] Alfred Brauer. On a problem of partitions. *Amer. J. Math.*, 64:299–312, 1942. doi:10.2307/2371684.

[BSSSW10] Francine Blanchet-Sadri, Jarett Schwartz, Slater Stich, and Benjamin J. Wyatt. Binary de Bruijn partial words with one hole. In *Theory and applications of models of computation*, volume 6108 of *Lecture Notes in Comput. Sci.*, pages 128–138. Springer, Berlin, 2010. doi:10.1007/978-3-642-13562-0_13.

[CDG92] Fan Chung, Persi Diaconis, and Ron Graham. Universal cycles for combinatorial structures. *Discrete Math.*, 110(1):43–59, 1992. doi:10.1016/0012-365X(92)90699-G.

[CFH+14] Arturo Carpi, Gabriele Fici, Štěpán Holub, Jakub Opršal, and Marinella Sciortino. Universal Lyndon words. In *Mathematical Foundations of Computer Science 2014. 39th International Symposium, MFCS 2014, Budapest, Hungary, August 25–29, 2014. Proceedings, Part I*, pages 135–146. Berlin: Springer, 2014. doi:10.1007/978-3-662-44522-8_12.

[CK20] Herman Z.Q. Chen and Sergey Kitaev. On universal partial words for word-patterns and set partitions. *RAIRO-Theor. Inf. Appl.*, 54:5, 2020. doi:10.1051/ita/2020004.

[CKMS17a] Herman Z. Q. Chen, Sergey Kitaev, Torsten Mütze, and Brian Y. Sun. On universal partial words. *Discrete Math. Theor. Comput. Sci.*, 19(1):Paper No. 16, 19, 2017. doi:10.23638/DMTCS-19-1-16.

[CKMS17b] Herman Z.Q. Chen, Sergey Kitaev, Torsten Mütze, and Brian Y. Sun. On universal partial words. *Electronic Notes in Discrete Mathematics*, 61:231–237, 2017. The European Conference on Combinatorics, Graph Theory and Applications (EUROCOMB'17). doi:10.1016/j.endm.2017.06.043.

[DW05] Aiping Deng and Yaokun Wu. De Bruijn digraphs and affine transformations. *European J. Combin.*, 26(8):1191–1206, 2005. doi:10.1016/j.ejc.2004.06.018.

[FGK+23] Dylan Fillmore, Bennet Goeckner, Rachel Kirsch, Kirin Martin, and Daniel McGinnis. The existence and structure of universal partial cycles, 2023. arXiv:2310.13067.

[GGH+18] Bennet Goeckner, Corbin Groothuis, Cyrus Hettle, Brian Kell, Pamela Kirkpatrick, Rachel Kirsch, and Ryan Solava. Universal partial words over non-binary alphabets. *Theoret. Comput. Sci.*, 713:56–65, 2018. doi:10.1016/j.tcs.2017.12.022.

[GHS22] Daniel Gabric, Štěpán Holub, and Jeffrey Shallit. Maximal state complexity and generalized de Bruijn words. *Inform. and Comput.*, 284:Paper No. 104689, 10, 2022. doi:10.1016/j.ic.2021.104689.

[GKP04] Jaroslaw Grytczuk, Andrzej P. Kisielewicz, and Krzysztof Przeslawski. Minimal partitions of a box into boxes. *Combinatorica*, 24(4):605–614, 2004. doi:10.1007/s00493-004-0037-4.

[Gra24] Andrew Granville. It is not "Bézout's identity", 2024. arXiv:2406.15642.

[GRV15] Navin Goyal, Luis Rademacher, and Santosh Vempala. Query complexity of sampling and small geometric partitions. *Comb. Probab. Comput.*, 24(5):733–753, 2015. doi:10.1017/S0963548314000704.

[GS18] Daniil Gasnikov and Arseny M. Shur. Square-free partial words with many wildcards. *Int. J. Found. Comput. Sci.*, 29(5):845–860, 2018. doi:10.1142/S0129054118420078.

[Haw13] Thomas Hawkins. *The Mathematics of Frobenius in Context: A Journey Through 18th to 20th Century Mathematics*. Sources and Studies in the History of Mathematics and Physical Sciences. Springer, New York, 2013. doi:10.1007/978-1-4614-6333-7.

[Hol19] Ron Holzman. On 2-colored graphs and partitions of boxes. *Eur. J. Comb.*, 79:214–221, 2019. doi:10.1016/j.ejc.2019.03.003.

[KK99] Keith A. Kearnes and Emil W. Kiss. Finite algebras of finite complexity. *Discrete Math.*, 207(1-3):89–135, 1999. doi:10.1016/S0012-365X(99)00042-4.

[KLSS23] Rachel Kirsch, Bernard Lidický, Clare Sibley, and Elizabeth Sprangel. Shortened universal cycles for permutations. *Discrete Appl. Math.*, 324:219–228, 2023. doi:10.1016/j.dam.2022.09.026.

[KNP24] Matthew Kreitzer, Mihai Nica, and Rajesh Pereira. Using alternating de Bruijn sequences to construct de Bruijn tori. *Des. Codes Cryptogr.*, 92(5):1439–1454, 2024. doi:10.1007/s10623-023-01351-0.

[KP08] Andrzej P. Kisielewicz and Krzysztof Przesławski. Polyboxes, cube tilings and rigidity. *Discrete Comput. Geom.*, 40(1):1–30, 2008. doi:10.1007/s00454-007-9005-2.

[KPV19] Sergey Kitaev, Vladimir N. Potapov, and Vincent Vajnovszki. On shortening u-cycles and u-words for permutations. *Discrete Appl. Math.*, 260:203–213, 2019. doi:10.1016/j.dam.2019.01.025.

[KR24] Stefan Kiefer and Andrew Ryzhikov. The complexity of computing the period and the exponent of a digraph, 2024. arXiv:2408.05762.

[KZ01] Maxim Kontsevich and Don Zagier. Periods. In *Mathematics Unlimited—2001 and Beyond*, pages 771–808. Springer, Berlin, 2001. URL: https://www.ihes.fr/~maxim/TEXTS/Periods.pdf.

[MEY21] Sagi Marcovich, Tuvi Etzion, and Eitan Yaakobi. Balanced de Bruijn sequences. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 1528–1533. IEEE Press, 2021. doi:10.1109/ISIT45174.2021.9517873.

[MEY23] Sagi Marcovich, Tuvi Etzion, and Eitan Yaakobi. On hierarchies of balanced sequences. *IEEE Trans. Inf. Theory*, 69(5):2923–2939, 2023. doi:10.1109/TIT.2022.3227467.

[Pra89] Cheryl E. Praeger. Highly arc transitive digraphs. *European J. Combin.*, 10(3):281–292, 1989. doi:10.1016/S0195-6698(89)80064-2.

[QWX22] Chengyang Qian, Yaokun Wu, and Yanzhen Xiong. Cyclic arrangements with minimum modulo $m$ winding numbers. *Graphs Combin.*, 38(3):Paper No. 53, 37, 2022. doi:10.1007/s00373-021-02443-1.

[RGS09] José Carlos Rosales and Pedro A. García-Sánchez. *Numerical Semigroups*, volume 20 of *Developments in Mathematics*. Springer, New York, 2009. doi:10.1007/978-1-4419-0160-6.

[Sak02] Michael Saks. Kleitman and combinatorics. *Discrete Math.*, 257(2-3):225–247, 2002. Kleitman and combinatorics: a celebration (Cambridge, MA, 1999). doi:10.1016/S0012-365X(02)00596-4.

[SK01] Arseny M. Shur and Yulia V. Konovalova. On the periods of partial words. In *Mathematical Foundations of Computer Science 2001. 26th International Symposium, MFCS 2001, Mariánské Lázně, Czech Republic, August 27–31, 2001. Proceedings*, pages 657–665. Berlin: Springer, 2001. doi:10.1007/3-540-44683-4_57.

[WL02] Yaokun Wu and Qiao Li. Some characterizations for the wrapped butterfly. In *Analysis, Combinatorics and Computing*, pages 419–433. Nova Sci. Publ., Hauppauge, NY, 2002. URL: https://math.sjtu.edu.cn/faculty/ykwu/data/Paper/wrapped.pdf.

[WXZ16] Yaokun Wu, Zeying Xu, and Yinfeng Zhu. An expansion property of Boolean linear maps. *Electron. J. Linear Algebra*, 31:381–407, 2016. doi:10.13001/1081-3810.3088.

[WXZ17] Yaokun Wu, Zeying Xu, and Yinfeng Zhu. Strongly connected multivariate digraphs. *Electron. J. Combin.*, 24(1):Paper 1.47, 44, 2017. doi:10.37236/6539.