BULLETIN OF THE ICA
Volume **104** (2025), 114–152

On cyclic matroids and their applications

Gianira N. Alfarano, Karan Khathuria, and Simran Tinani

Abstract. A matroid is a combinatorial structure that captures and generalizes the algebraic concept of linear independence under a broader and more abstract framework. Matroid theory is closely related to many other topics in discrete mathematics, such as graphs, matrices, codes, and projective geometries. In this work, we define *cyclic matroids* as matroids over a ground set of size n whose automorphism group contains an n-cycle. We study the properties of such matroids, with special focus on the minimum size of their basis sets. For this, we broadly employ two different approaches: the multiple basis exchange property and an orbit-stabilizer method developed by analyzing the action of the cyclic group of order n on the set of bases. We further present some applications of our theory to algebra and geometry, illustrating connections to cyclic projective planes, cyclic codes, and k-normal elements.

1 Introduction

Matroids are versatile combinatorial structures known to have close ties with other objects in discrete mathematics such as graphs, matrices, codes, and projective geometries. In this paper, we introduce the family of *cyclic matroids* as matroids over a ground set of size n whose automorphism group contains a cyclic subgroup of order n. We show that these matroids are highly pertinent to the study of cyclic projective planes, cyclic codes, and k-normal elements over finite fields.

We describe the properties of cyclic matroids, focusing our attention on the size of their basis sets. Counting the bases of matroids is a common problem in combinatorics and in particular in optimization; see [6, 11, 16, 19, 25] to mention but a few contributions. In full generality, giving an estimate of the number of bases of a matroid is a difficult problem. Indeed, its exact

Key words and phrases: Cyclic matroids, Cyclic codes, k-normal elements, number of basis, cyclic projective planes
Mathematics Subject Classifications: 05B35, 94B15
Coresponding author: Gianira N. Alfarano <gianira.alfarano@gmail.com>

Received: 25 August 2023
Accepted: 12 August 2024

computational complexity is still only partially understood. Depending on the class of matroids in question, the exact counting problem may be polynomial time, #P-complete, or unsolved. For example, it is #P-complete to count the number of bases of transversal matroids and bicircular matroids; see [4, 7].

We show that the defining feature of a cyclic matroid enforces the presence of certain types, and therefore a threshold number, of basis elements. Let $\mathcal{M}$ be a cyclic matroid with ground set $\{0, 1, \ldots, n-1\}$ and rank k. We prove, in particular, that the subset $B_0 = \{0, 1, \ldots, k-1\}$ is always a basis for $\mathcal{M}$. Further, we provide some lower bounds on the number of bases of $\mathcal{M}$. For this purpose, we employ two different approaches. On the one hand, we use the *basis exchange property* on the cyclic shifts of B_0, i.e., $B_i = \{i, i+1, \ldots, i+k-1\}$. On the other hand, we use the fact that the basis set $\mathcal{B}$ is closed under the action of the cyclic group $\mathbb{Z}_n$ of order n and find the minimum number of orbits contained in $\mathcal{B}$. While this group action has been studied for different purposes (see for instance [1,17,21,24]), to the best of our knowledge, its connection to matroids has not been investigated before.

We finally describe the connections of cyclic matroids to well known structures in algebra and geometry. We observe that every cyclic code of length n and dimension k gives rise to a representable cyclic matroid of rank k and ground set $\{0, 1, \ldots, n-1\}$ and that, more generally, the incidence matrix of every cyclic projective plane $\mathrm{PG}(2, q)$ can be represented as a binary cyclic matroid over a ground set of size $q^2 + q + 1$ and rank depending on q. Furthermore, we establish and explain a connection between k-normal elements of $\mathbb{F}_{q^n}$ and cyclic matroids of rank $(n-k)$ and ground set $\{0, 1, \ldots, n-1\}$. However, all these connections leave open a lot of questions; in particular, it is not clear yet if representable cyclic matroids are always represented by cyclic codes or k-normal elements. We leave those problems for further investigation.

The paper is structured as follows. In Section 2, we give some preliminary background on matroids, finite projective geometry, linear codes, and k-normal elements. In Section 3, we introduce cyclic matroids and study the structure and properties of their basis sets. To this end, we use the multiple basis exchange property to provide different lower bounds on the number of bases of cyclic matroids. Then, we study the orbits and the stabilizers of the group action of $\mathbb{Z}_n$ on the set $2^{\mathbb{Z}_n}$ and then apply this analysis to the bases of cyclic matroids to obtain two more lower bounds. Since the formulas for these bounds are obtained using different approaches, they are not directly comparable, and one may exceed the other depending

on the relationship between n and k. Therefore, we provide and compare some concrete values of all of our calculated bounds for different values of n and k. In addition to concrete values, we also compare the asymptotic behavior of all the bounds. In Section 4, we explain the link between cyclic projective planes, cyclic codes, and k-normal elements and cyclic matroids. These links indicate that the class of cyclic matroids deserves to be further studied from different points of view and may hold powerful potential to uncover results on related algebraic, combinatorial, and geometric objects. Finally, in Appendix A we provide some concrete, non-trivial examples of cyclic matroids found by computer search.

Notation

Let E be a finite set. We denote by 2^E the set of all subsets of E. The cardinality of E is denoted by $|E|$. Let $A \subseteq E$ be any subset. We denote by A^C the complement set of A in E. Given a positive integer n, let $\mathbb{Z}_n$ denote the set of integers modulo n. By abuse of notation, we use the same symbols for the integer a and its residue class $a \bmod n$ and perform arithmetic modulo n, unless stated otherwise. As is standard, the elements of $\mathbb{Z}_n$ are represented by integers $0 \leq a \leq n-1$, and so $\mathbb{Z}_n$ inherits the ordering on $\mathbb{Z}$. We denote by $\mathcal{S}_n$ the symmetric group on n symbols, and by the cycle $(0\ 1\ \ldots\ n-1)$ the permutation $0 \mapsto 1,\ 1 \mapsto 2,\ \ldots,\ (n-2) \mapsto (n-1),\ (n-1) \mapsto 0$. Given a prime power q, we denote by $\mathbb{F}_q$ the finite field of order q and by $\mathbb{F}_q^n$ the n-dimensional vector space over $\mathbb{F}_q$.

2 Background

In this section, we provide some useful background for the rest of the paper. We first briefly recall what a matroid is; later we introduce other combinatorial and algebraic structures such as projective planes, linear codes, and k-normal elements, which are closely related to the main object of study of this paper, namely cyclic matroids. These relations are explained in Section 4.

2.1 Matroids

We first recall the basic definitions of matroid theory that are used throughout the paper. For a detailed treatment on matroids we refer the interested reader to [18].

Definition 2.1. A *matroid* $\mathcal{M}$ is a pair $(E, \mathcal{I})$ where E is a finite set and $\mathcal{I}$ is a subset of 2^E satisfying the following properties:

(I1) $\varnothing \in \mathcal{I}$.

(I2) If $I \in \mathcal{I}$ and $J \subseteq I$, then $J \in \mathcal{I}$.

(I3) If $I, J \in \mathcal{I}$ and $|I| < |J|$, then there is an element $e \in J \setminus I$ such that $I \cup \{e\} \in \mathcal{I}$.

The elements of $\mathcal{I}$ are called the *independent sets* of $\mathcal{M}$, and the elements outside $\mathcal{I}$ are called the *dependent sets* of $\mathcal{M}$. A maximal (with respect to inclusion) independent set in $\mathcal{I}$ is called a *basis* of $\mathcal{M}$.

If $\mathcal{B}$ is the set of bases of $\mathcal{M}$, then by (I1) it follows that

(B1) $\mathcal{B} \neq \varnothing$.

By (I3), it is easy to see that all the bases have the same cardinality, which is called the *rank* of $\mathcal{M}$. Moreover, the set of bases $\mathcal{B}$ satisfies the following property, known as the *basis exchange property*:

(B2) If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$, then there exists an element $y \in B_2 \setminus B_1$ such that $\big(B_1 \setminus \{x\}\big) \cup \{y\} \in \mathcal{B}$.

Using (B1) and (B2), we get an equivalent characterization of a matroid in terms of bases. Throughout the paper we define matroids using the bases axioms, and use the notation $\mathcal{M} = (E, \mathcal{B})$ for a matroid with ground set E and basis set $\mathcal{B}$.

Example 2.2 (Uniform Matroid)**.** Let E be a set of cardinality n and, for an integer $k \leq n$, denote by $\mathcal{I}$ the collection of subsets of E with at most k elements and by $\mathcal{B}$ the collection of subsets of E with exactly k elements. It is not difficult to verify that $\mathcal{I}$ satisfies properties (I1)–(I3) and $\mathcal{B}$ satisfies properties (B1)–(B2); hence, the pair $(E, \mathcal{B})$ defines a matroid of rank k, denoted by $U_{n,k}$ and called the *uniform matroid*.

In Lemma 2.3, we state an equivalent formulation of the basis exchange property given in [9], which we use many times in the paper.

Lemma 2.3 (Multiple Exchange Property)**.** *Let $\mathcal{M} = (E, \mathcal{B})$ be a matroid on a ground set E and let $\mathcal{B}$ be its collection of bases. Further, let $B_1, B_2 \in \mathcal{B}$ and let $Q \subset B_1 \setminus B_2$. Then there exists a subset $P \subset B_2 \setminus B_1$ such that $(B_1 \setminus Q) \cup P \in \mathcal{B}$.*

Definition 2.4. Let $\mathcal{M} = (E, \mathcal{B})$ be a matroid. An *automorphism* τ of $\mathcal{M}$ is a permutation of E such that $B \in \mathcal{B}$ if and only if $\tau(B) \in \mathcal{B}$, where $\tau(B) \coloneqq \{\tau(b) \mid b \in B\}$. The *automorphism group* $\mathrm{Aut}(\mathcal{M})$ is the group of automorphisms of $\mathcal{M}$ under composition.

More generally, given a matroid $\mathcal{M} = (E, \mathcal{B})$, another matroid $\mathcal{M}' = (E', \mathcal{B}')$ is said to be *isomorphic* to $\mathcal{M}$ if there exists a bijection $\tau \colon E \to E'$ such that $\tau(B) \in \mathcal{B}'$ if and only if $B \in \mathcal{B}$.

We recall the notion of dual matroid.

Definition 2.5. Let $\mathcal{M} = (E, \mathcal{B})$ be a matroid with ground set E and collection of bases $\mathcal{B}$. Let $\mathcal{B}^* = \left\{B^C \mid B \in \mathcal{B}\right\}$. Then $\mathcal{B}^*$ satisfies the axioms (B1) and (B2); hence, it is the collection of bases of a matroid $\mathcal{M}^* = (E, \mathcal{B}^*)$, called the *dual matroid* of $\mathcal{M}$.

Finally, we provide an example of matroids arising from matrices.

Example 2.6 (Representable Matroid)**.** Let $\mathbb{F}$ be a field and let A be an $m \times n$ matrix over $\mathbb{F}$. We define E to be the index set of the columns of A and $\mathcal{I}$ to be the collection of subsets of E that correspond to linearly independent sets of columns of A. Then, $\mathcal{M}(A) = (E, \mathcal{I})$ is a matroid of rank equal to the rank of A, and it is called a *representable matroid*. A proof can be found in [18, Theorem 1.1.1].

2.2 Projective planes

In this short section, for convenience of the reader, we recall the definition of a (cyclic) projective plane, incidence matrix, and collineation group.

Definition 2.7. A (point-line) *incidence structure* is a triple $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ of sets with $\mathcal{P}$ called a set of *points*, $\mathcal{L}$ called a set of *lines*, and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$ called the set of *incidence relations*. We say that a point P and a line ℓ are *incident* with each other if $(P, \ell) \in \mathcal{I}$, and in this case we write $P \in \ell$. A subset of points is called *collinear* if they are all incident with the same line.

Definition 2.8. Let n be an integer. A *finite projective plane* $\mathrm{PG}(2,n)$ is a (point-line) incidence structure with n^2+n+1 points and n^2+n+1 lines that satisfy the following axioms:

1. Every two points are incident with exactly one line.
2. Every two lines are incident with exactly one point.
3. There are four points such that no three of them are collinear.

When $n=q$, where q is a prime power, and the points and lines of $\mathrm{PG}(2,q)$ are the one- and two-dimensional subspaces of $\mathbb{F}_q^3$, then the projective plane is called *Desarguesian*.

In this paper, we assume that $\mathrm{PG}(2,q)$ is Desarguesian. It is immediate to see that every line in $\mathrm{PG}(2,q)$ is incident with exactly $q+1$ points and that, dually, every point is incident with exactly $q+1$ lines. The incidence relation of $\mathrm{PG}(2,q)$ can be represented via an *incidence matrix* A, whose rows and columns are indexed by points and lines respectively such that

$$A_{i,j} = \begin{cases} 1, & \text{if } P_i \in \ell_j, \\ 0, & \text{otherwise,} \end{cases}$$

where for $i,j \in \{1,\ldots,q^2+q+1\}$ the P_i's are the points and ℓ_j's are the lines of the projective plane.

Definition 2.9. A *collineation* of $\mathrm{PG}(2,q)$ is a permutation of the points of $\mathrm{PG}(2,q)$ that preserves their collinearity, i.e., lines are mapped onto lines. The set of collineations forms a group, called a *collineation group*.

Definition 2.10. A projective plane $\mathrm{PG}(2,q)$ is called *cyclic* if its collineation group is transitive on the points of $\mathrm{PG}(2,q)$ and there exists a collineation that generates a cyclic subgroup of order q^2+q+1.

2.3 Linear codes

This section introduces linear codes, with a particular focus on cyclic codes. For a more detailed treatment of the topic we refer the interested reader to [27].

Definition 2.11. Let $1 \leq k \leq n$. An $[n,k]_q$ (*linear*) *code* $\mathcal{C}$ is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$. The vectors in $\mathcal{C}$ are called *codewords*. A matrix $G \in \mathbb{F}_q^{k\times n}$ whose rows form a basis for $\mathcal{C}$ is called a *generator matrix* for $\mathcal{C}$.

In 1976, Greene [10] explored several connections between matroids and linear codes. Ever since, many authors have exploited this link and used matroid theory to prove coding theoretic results. It is straightforward to obtain a representable matroid $\mathcal{M}(G)$ from a generator matrix G of a linear code $\mathcal{C}$; see Example 2.6. Moreover, $\mathcal{M}(G)$ does not depend on the choice of the generator matrix G.

In this work, we are interested in a special class of linear codes, called *cyclic codes*, which are one of the most studied families of codes due to their polynomial representation as ideals of $\mathbb{F}[x]/\langle x^n - 1\rangle$. More precisely, they are defined as follows.

Definition 2.12. A code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is said to be *cyclic* if for every codeword $c = (c_0, c_1, \ldots, c_{n-1})$, the cyclic shift of c, namely

$$\mathrm{sh}(c) = (c_{n-1}, c_0, \ldots, c_{n-2}),$$

is also a codeword.

Consider the following map $\phi\colon \mathbb{F}_q^n \to \mathbb{F}_q[x]/\langle x^n - 1\rangle$ where

$$(c_0, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}.$$

It is easy to see that ϕ is an isomorphism of vector spaces, and it turns out that $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a cyclic code if and only if $\phi(\mathcal{C})$ is an ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, which derives from the fact that $\phi\big(\mathrm{sh}(c)\big) = x\phi(c) \mod (x^n - 1)$. With abuse of notation, we then identify $\mathcal{C}$ with $\phi(\mathcal{C})$, and we say that a cyclic code is an ideal of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.

Since $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is a principal ideal ring, every cyclic code consists of the multiples of a polynomial $g(x)$, which is the monic polynomial of lowest degree in the ideal. Such a polynomial $g(x)$ is called a *generator polynomial*; it divides $x^n - 1$; and if $g(x)$ has degree $n - k$, then the cyclic code that it generates has dimension k.

2.4 k-normal elements

In this last introductory section, we introduce k-normal elements.
We are interested in studying elements in a finite extension $\mathbb{F}_{q^n}$ of degree n over $\mathbb{F}_q$. An element $\alpha \in \mathbb{F}_{q^n}$ is called a *normal element* over $\mathbb{F}_q$ if all its Galois conjugates, i.e., the n elements $\left\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\right\}$, form a basis of $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$. A basis of this form is called a *normal basis*.

As a generalization of normal elements, in [14] k-normal elements were defined.

Definition 2.13. An element $\alpha \in \mathbb{F}_{q^n}$ is called *k-normal* if

$$\dim_{\mathbb{F}_q}\left(\mathrm{span}_{\mathbb{F}_q}\left\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\right\}\right) = n - k.$$

Questions on the existence of k-normal elements have been investigated in [22] and in [26]. In this last work, a general lower bound for the number of k-normal elements was also provided.

3 Cyclic matroids

In this section we introduce cyclic matroids and study the structure of their basis sets.

Definition 3.1. Let n be a positive integer. A matroid $\mathcal{M} = (E, \mathcal{B})$ on the ground set E with $|E| = n$ is called a *cyclic k-matroid* if it has rank k and satisfies one of the following equivalent conditions:

1. The automorphism group $\mathrm{Aut}(\mathcal{M})$ contains an isomorphic copy of the cyclic group $\mathbb{Z}_n$.
2. There exists a cycle σ of length n acting on E such that $\sigma(B) \in \mathcal{B}$ for each $B \in \mathcal{B}$.
3. $\mathcal{M}$ is isomorphic to some matroid $\mathcal{M}_0$ with ground set $\{0, 1, \ldots, n-1\}$ such that $(0\ 1\ \ldots\ n-1) \in \mathrm{Aut}(\mathcal{M}_0)$.

When the rank is clear or not necessary, we simply say that $\mathcal{M}$ is a *cyclic matroid*. Using the definition of an automorphism of $\mathcal{M}$ (see Definition 2.4), it is easy to see that the above three conditions are equivalent.

For simplicity, we fix the ground set $E = \{0, 1, \ldots, n-1\}$, and use $\mathbb{Z}_n$ interchangeably with E. Without loss of generality, we assume that the automorphism group of a cyclic matroid contains the n-cycle $(0\ 1\ \ldots\ n-1)$. We define *cyclic shifts on the subsets* of E as follows: let $s \in \mathbb{Z}_n$ and $A \subseteq E$, then the shifted subset $s + A$ is defined as $\sigma^s(A)$, where σ is the permutation $(0\ 1\ \ldots\ n-1)$. If $A = \{g_0, g_1, \ldots, g_{k-1}\}$, then $s + A = \{s + g_0 \bmod n, s + g_1 \bmod n, \ldots, s + g_{k-1} \bmod n\}$.

Notice that in [28, p. 330], Welsh defines a matroid $\mathcal{M}$ to be cyclic if $\mathrm{Aut}(\mathcal{M}) = \mathbb{Z}_n$. We redefine cyclic matroids because often, in the literature,

cyclic objects are the ones that are closed under cyclic shifts. Definition 3.1 introduces a more general class of matroids, which strictly includes Welsh's cyclic matroids. For instance, the uniform matroid $U_{k,n}$ defined in Example 2.2 has automorphism group equal to the symmetric group $\mathcal{S}_n$; hence, it is not cyclic according to Welsh's definition. Another example is the well known Fano matroid, which is described in Example 4.7.

Remark 3.2. For fixed values of n and k, cyclic matroids are not uniquely determined. For example, in the case of $n = 4$ and $k = 2$, we have two distinct cyclic k-matroids with bases $\mathcal{B} = \big\{\{0,1\}, \{1,2\}, \{2,3\}, \{0,3\}\big\}$ and $\mathcal{B}' = \big\{\{0,1\}, \{1,2\}, \{2,3\}, \{3,0\}, \{0,2\}, \{1,3\}\big\}$. Note that the matroid $\big(\{0,1,2,3\}, \mathcal{B}'\big)$ is the uniform matroid $U_{2,4}$.

Remark 3.3. It is easy to see that the dual matroid $\mathcal{M}^*$ of a cyclic k-matroid with ground set of size n is a cyclic $(n-k)$-matroid. Moreover, for $k \geq 1$, every singleton in a cyclic matroid clearly has rank 1. So a non-trivial cyclic matroid, i.e., with $\mathcal{B} \neq \{\varnothing\}$, does not have loops (i.e, elements that do not belong to any basis), and a proper cyclic matroid, i.e., with $\mathcal{B} \subsetneq 2^E$, does not have coloops (i.e., elements that belong to every basis).

The main problem we address in this paper is counting the minimum number of basis elements, i.e., finding the minimum cardinality $|\mathcal{B}|$ in a cyclic k-matroid. Throughout, we let

$$B_0 \coloneqq \{0, 1, \ldots, k-1\}.$$

Given a cyclic k-matroid $\mathcal{M}$, we show in Proposition 3.7 that B_0 is always a basis of $\mathcal{M}$. As a result, each of its shifts $B_i = i + B_0$ for $1 \leq i \leq n-1$ is also a basis. We refer to these bases $B_0, B_1, \ldots, B_{n-1}$ as *cyclic bases* for the matroid $\mathcal{M}$. To prove this result, we associate to each subset of $\mathbb{Z}_n$ a set partition in the following way.

Definition 3.4. Let $A \subseteq \mathbb{Z}_n$ be any set. The *consecutive block structure* of A is the (ordered) set partition of A given by $\pi(A) = (D_1, D_2, \ldots, D_\ell)$, where each $D_i = \{d_i, d_i+1, \ldots, d_i+|D_i|-1\}$ is a maximal subset of A containing consecutive elements modulo n, ordered according to

$$d_1 < d_2 < \cdots < d_\ell.$$

It is useful also to associate to a k-subset of $\mathbb{Z}_n$ the following tuple.

Definition 3.5. If $|A| = k$, given the consecutive block structure of A, $\pi(A) = (D_1, D_2, \ldots, D_\ell)$, the composition (ordered integer partition) $|D_1| + |D_2| + \cdots + |D_\ell|$ of k is called the *block composition* of A, denoted by $c(A) = \big(|D_1|, |D_2|, \ldots, |D_\ell|\big)$.

Example 3.6. Let $A = \{0, 2, 3, 4, 6, 7, 9\} \subseteq \mathbb{Z}_{10}$, then the consecutive block structure of A is $\pi(A) = (\{2, 3, 4\}, \{6, 7\}, \{9, 0\})$, and the block composition of A is $c(A) = (3, 2, 2)$.

Proposition 3.7. *Let $\mathcal{M} = (E, \mathcal{B})$ be a cyclic k-matroid. Then $B_0 \in \mathcal{B}$.*

Proof. Let $B \in \mathcal{B}$ be a basis of $\mathcal{M}$, and let $\pi(B) = (D_1, D_2, \ldots, D_\ell)$ be its consecutive block structure, i.e., $B = D_1 \cup D_2 \cup \cdots \cup D_\ell$. If $\ell = 1$, then we are done, as one of the shifts of B must be equal to B_0.

Now assume that $\ell > 1$. Using the basis exchange property, we construct a new basis that has $\ell - 1$ blocks in its consecutive block structure. Note that this is enough to prove the result, as we can apply this argument repetitively until we obtain $\ell = 1$.

Let $D_i = \{d_i, d_i + 1, \ldots, d_i + |D_i| - 1\}$ for each $i \in \{1, 2, \ldots, \ell\}$. We apply the basis exchange property (B2) with respect to bases B and $B + 1$. Note that $B \setminus (B + 1) = \{d_1, d_2, \ldots, d_\ell\}$, hence we obtain a new basis element $B' = (B \setminus \{d_\ell\}) \cup \{p\}$, for some $p \in (B+1) \setminus B = \{d_1 + |D_1|, \ldots, d_\ell + |D_\ell|\}$.

Let $B' = D'_1 \cup \cdots \cup D'_{\ell'}$ be the consecutive block structure of B'. Consider the two possibilities $|D_\ell| > 1$ and $|D_\ell| = 1$. If $|D_\ell| > 1$, then $B \setminus \{d_\ell\}$ also has ℓ blocks in its consecutive block structure. Every $p \in \big\{d_1 + |D_1|, \ldots, d_\ell + |D_\ell|\big\}$ gets added to one of these blocks, so $\ell' = \ell$. If $|D_\ell| = 1$, then $B \setminus \{d_\ell\}$ contains $\ell - 1$ blocks. If $p \neq d_\ell + 1$, then p just gets added to one of the blocks in $B \setminus \{d_\ell\}$, and B' has $\ell - 1$ blocks. If $p = d_\ell + 1$, then it forms its own separate block, and $\ell' = \ell$. Thus, $\ell' = \ell$ or $\ell' = \ell - 1$. If $\ell' = \ell - 1$, then we are done. So assume that $\ell' = \ell$. This implies that $D'_\ell = \big\{d_\ell + 1, \ldots, d_\ell + |D_\ell| - 1\big\}$ or $D'_\ell = \big\{d_\ell + 1, \ldots, d_\ell + |D_\ell|\big\}$. In each case, the smallest element in D'_ℓ increases by 1. Hence, by applying this basis exchange process repeatedly, the block D'_ℓ either vanishes or merges with the next block D'_1, and this results in a new basis with $\ell - 1$ consecutive blocks. □

Proposition 3.7 therefore shows that each of the cyclic bases

$$B_0, B_1, \ldots, B_{n-1}$$

is indeed a basis for any cyclic k-matroid.

Example 3.8. Let n and k be integers such that $k \mid n$. Consider a representable matroid $\mathcal{M}(A) = (E, \mathcal{B})$, where A is the $k \times n$ matrix

$$A = \begin{pmatrix} \mathrm{Id}_k & \mathrm{Id}_k & \cdots & \mathrm{Id}_k \end{pmatrix} \in \mathbb{F}^{k \times n}$$

with $\mathbb{F}$ being any field and Id_k denoting the $k \times k$ identity matrix. If $E = \{0, 1, \ldots, n-1\}$ is the index set of the columns of A, then the set of bases $\mathcal{B}$ is given by

$$\mathcal{B} = \big\{\{a_0, a_1, \ldots, a_{k-1}\} \mid a_i \equiv i \pmod{k}\big\}.$$

It is easy to check that $\mathcal{M}$ is a cyclic k-matroid.

3.1 Basis exchange approach for the number of bases

In this section, we present some lower bounds on the size of the collection of bases $\mathcal{B}$ of an arbitrary cyclic matroid $\mathcal{M} = (\mathbb{Z}_n, \mathcal{B})$. In particular, we use the basis exchange property on the cyclic bases $B_0, B_1, \ldots, B_{n-1}$ to construct other basis elements.

We first prove some properties of the cyclic bases that we use to count the number of bases in a cyclic matroid. In the following result we compute the size of the difference between the intersection of two cyclic bases and the basis set B_0.

Lemma 3.9. *Let $1 \le j \le i \le n-1$. Then,*

$$\big|(B_i \cap B_j) \setminus B_0\big| = \begin{cases} 0, & \text{if } i - j \ge k, \\ j + k - \max\{k, i\}, & \text{otherwise.} \end{cases}$$

Proof. Write $\ell = i - j$. Assume $k \le n/2$. Then we can observe that

$$B_i \cap B_j = \begin{cases} \{i, i+1, \ldots, j+k-1\}, & \text{if } \ell < k, \\ \{j, j+1, \ldots, i-n+k-1\}, & \text{if } \ell > n-k, \\ \varnothing, & \text{if } k \le \ell \le n-k. \end{cases}$$

Similarly, if $k > n/2$, we have that

$$B_i \cap B_j = \begin{cases} \{i, i+1, \ldots, j+k-1\}, & \text{if } \ell < n-k, \\ \{j, j+1, \ldots, i-n+k-1\}, & \text{if } \ell \geq k, \\ \{j, j+1, \ldots, i-n+k-1\} & \\ \qquad \cup \{i, \ldots, j+k-1\}, & \text{if } n-k \leq \ell \leq k. \end{cases}$$

Therefore, if $\ell \geq k$, then $B_i \cap B_j = \varnothing$ or $B_i \cap B_j \subseteq B_0$. Whereas, if $\ell < k$ then

$$(B_i \cap B_j) \setminus B_0 = \begin{cases} \{k, k+1, \ldots, j+k-1\}, & \text{if } i \leq k, \\ \{i, i+1, \ldots, j+k-1\}, & \text{if } i > k. \end{cases}$$ □

In order to apply the basis exchange property on B_0, we calculate the collection of all cyclic shifts of B_0 that intersect trivially (i.e., empty intersection) with a subset of B_0.

Lemma 3.10. *Let $Q \subseteq B_0$. Let q_1 and q_2 be the smallest and largest elements of Q, respectively. For $i \in \{q_2 - q_1 + 1, \ldots, n-k\}$, the $n-k-q_2+q_1$ bases $B_0 + q_1 + i$ intersect trivially with Q, and any cyclic basis satisfying this property must lie among these.*

Proof. We may rule out cyclic bases of the form $B_0 + j$ with $j < q_2$, since these would always contain q_2. So, we are looking for cyclic bases of the form $B_0 + q_1 + i$ with $i > q_2 - q_1$. For q_1 to lie outside these bases, we would additionally need $k - 1 + q_1 + i < n + q_1$, so $i \leq n - k$. Now let $q \in Q$ and suppose that $q \in B_0 + q_1 + i$ for some $q_2 - q_1 < i \leq n - k$. Thus, $q = b_0 + q_1 + i$ or $q + n = b_0 + q_1 + i$ for some $q_2 - q_1 < i \leq n - k$ and $b_0 \in B_0$. Since $q < q_2$, the first case is impossible. Similarly, $b_0 + q_1 + i < k - 1 + q_1 + i < n + q_1 < n + q$, so the second case is also impossible. Thus, $Q \subseteq B_0 \setminus B_{q_1+i}$ for all $q_2 - q_1 < i \leq n - k$. The number of such bases is clearly given by $n - k - q_2 + q_1$, which is the number of valid indices i. □

Lemma 3.11. *Let $Q \subseteq B_0$ be fixed with $|Q| = r$. Let q_1 and q_2 be the smallest and largest elements of Q, respectively, and assume that $q_2 - q_1 < n - k$. For any $q \in B_0$ and $q_2 - q_1 + 1 \leq j < i \leq n - k$, we have that $\left|(B_{q+i} \setminus B_0) \cap (B_{q+j} \setminus B_0)\right| < r$ if and only if $i - j \geq k - r + 1$.*

Proof. Let $q_2 - q_1 + 1 \leq j < i \leq n - k$ and $i - j \geq k - r + 1$. Note first that $(B_{q+i} \setminus B_0) \cap (B_{q+j} \setminus B_0) = (B_{q+i} \cap B_{q+j}) \setminus B_0$. Thus, by Lemma 3.9, we have

$$\left|(B_{q_1+i} \setminus B_0) \cap (B_{q_1+j} \setminus B_0)\right| = \begin{cases} 0, & \text{if } i - j \geq k, \\ q_1 + j + k - \max\{k, q_1 + i\}, & \text{otherwise.} \end{cases}$$

Now, since $r \leq q_2 - q_1 + 1 \leq j < i$, the smallest values for j and i in the above expressions are, respectively, $q_2 - q_1 + 1$ and $q_2 - q_1 + k - r + 2$. Thus, $q_1 + i \geq (q_2 - r) + k + 2 \geq q_1 + 1 + k > k$, and so for any $q \in B_0$ we have $\max\{k, q + i\} = q_1 + i$ for the relevant values of i. Now, if $i - j \geq k$, we are done. If $i - j < k$, then, $\left|(B_{q+i} \setminus B_0) \cap (B_{q+j} \setminus B_0)\right| < r$, which can happen if and only if $q + j + k - q - i < r$ and equivalently when $i - j > k - r$. This completes the proof. □

For an arbitrary cyclic k-matroid $\mathcal{M} = (\mathbb{Z}_n, \mathcal{B})$, we know from Proposition 3.7 that all the n shifts of B_0 are bases of $\mathcal{M}$. In the rest of the section, we use Lemma 2.3 to show the existence of more bases in $\mathcal{B}$.

Proposition 3.12. *Let $\mathcal{M} = (\mathbb{Z}_n, \mathcal{B})$ be a cyclic k-matroid and let $Q \subseteq B_0 = \{0, 1, \ldots, k-1\}$ with $|Q| = r$. Let q_1 and q_2 denote, respectively, the smallest and largest elements of Q and assume that $q_2 - q_1 < n - k$. Define $m = \left\lfloor \frac{n-k-q_2+q_1-1}{k-r+1} \right\rfloor + 1$. Then, there exist m distinct bases in $\mathcal{B}$ of the form $(B_0 \setminus Q) \cup P_i$, where $P_i \subseteq B_{q_1+i} \setminus B_0$ and $q_2 - q_1 < i \leq n - k$.*

Proof. By Lemma 3.10, we have $Q \cap B_{q_1+i} = \varnothing$ precisely for the $n - k - q_2 + q_1$ values of $i \in I \coloneqq \{q_2 - q_1 + 1, \ldots, n - k\}$. Applying the basis exchange property (B2) to B_0 and B_{q_1+i} for each $i \in I$, we get subsets $P_i \subseteq B_{q_1+i} \setminus B_0$ such that $(B_0 \setminus Q) \cup P_i$ is a basis.

Using Lemma 3.11 for $q = q_1$, we have $\left|(B_{q_1+i} \setminus B_0) \cap (B_{q_1+j} \setminus B_0)\right| < r$ for each pair $i, j \in I$ that satisfies $i - j \geq k - r + 1$. Thus, for each

$$i \in \left\{q_2 - q_1 + 1, q_2 - q_1 + 1 + (k - r + 1), \ldots, q_2 - q_1 + 1 + \tilde{m}(k - r + 1)\right\},$$

where $\tilde{m} = \left\lfloor \frac{n-k-q_2+q_1-1}{k-r+1} \right\rfloor$ is the largest integer such that $q_2 - q_1 + 1 + \tilde{m}(k - r + 1) \leq n - k$, we get distinct bases $(B_0 \setminus Q) \cup P_i$. Thus, there are $m = \tilde{m} + 1$ bases in $\mathcal{B}$ of this form. □

We now apply Proposition 3.12 on each subset Q of B_0 to obtain a lower bound on the size of $\mathcal{B}$. For the next two theorems, we use the following convention for binomial coefficients:

$$\tbinom{a}{-1} \coloneqq \begin{cases} 0, & \text{if } a \geq 0, \\ 1, & \text{if } a = -1. \end{cases}$$

Theorem 3.13. *Let $\mathcal{M} = (\mathbb{Z}_n, \mathcal{B})$ be a cyclic k-matroid. Then, there are at least $m_1(n,k)$ distinct bases in $\mathcal{B}$ of the form $(B_0 \setminus Q) \cup P$, where $Q \subseteq B_0$, $P \subseteq B_i$ for some $1 \leq i \leq n-1$, and*

$$m_1(n,k) \;=\; 1 \;+ \sum_{\Delta=0}^{\min\{k-1,n-k-1\}} \sum_{r=1}^{\Delta+1} (k-\Delta)\tbinom{\Delta-1}{r-2}\Big(\Big\lfloor \tfrac{n-k-\Delta-1}{k-r+1} \Big\rfloor + 1\Big).$$

Proof. First note that for distinct subsets Q and Q' of B_0, bases of the form $(B_0 \setminus Q) \cup P$ and $(B_0 \setminus Q') \cup P'$ are distinct, where P and P' are some subsets outside B_0. So, we may simply add up the number of bases resulting from the individual subsets Q.

Now for a subset Q of B_0 with smallest and largest terms q_1 and q_2, respectively, and size $r \geq 1$, write $\Delta = q_2 - q_1$ as the value corresponding to Q.

In the case of $\Delta = 0$, we get $r = 1$ and the number of bases of the form $\big(B_0 \setminus \{q\}\big) \cup \{p\}$ is given by $k\big(\lfloor \frac{n-k-1}{k} \rfloor + 1\big)$. This directly follows from Proposition 3.12 by taking $q_1 = q_2 = q$ and $r = 1$.

For a fixed value of $\Delta \in \big\{1, 2, \ldots, \min\{k-1, n-k-1\}\big\}$, we may calculate the number of subsets Q corresponding to Δ and with a fixed size r as follows. There are $(k-\Delta)$ subsets of B_0 of the form $\{q_1, q_1+1, \ldots, q_1+\Delta\}$, each with size $\Delta+1$. Any Q must contain q_1 and $q_1+\Delta$ and may then contain any $(r-2)$-subset of the remaining $\Delta+1-2 = \Delta-1$ elements of this set. Thus, this gives us a total of $(k-\Delta)\binom{\Delta-1}{r-2}$ options for Q corresponding to r.

We may further sum over the relevant values of r for a given value of Δ, i.e., from 2 to $\Delta+1$. For each of these subsets Q, there are at least $\lfloor \frac{n-k-\Delta-1}{k-r+1} \rfloor + 1$ distinct bases in $\mathcal{B}$, by Proposition 3.12. Finally, we add 1 to include the case $Q = \varnothing$. This completes the proof. □

Lemma 3.14. *For $\ell = \lfloor n/k \rfloor - 1$, we have $\left|B_{(\ell+1)k} \setminus B_0\right| = n - (\ell+1)k = \left|B_0 \setminus B_{(\ell+1)k}\right|$.*

Proof. There exists some i with $0 \leq i \leq k-1$, such that $(\ell+1)k + i = n$. Clearly, $i = n-(\ell+1)k$. The number of terms in $B_0 \cap B_{(\ell+1)k}$ is the number of terms starting at $(\ell+1)k+i$ and ending at $(\ell+1)k+(k-1)$, i.e. $k-i$ terms, i.e. $k-n+(\ell+1)k = (\ell+2)k-n$. Therefore, $\left|B_{(\ell+1)k} \setminus B_0\right| = |B_{(\ell+1)k}| - \left|B_0 \cap B_{(\ell+1)k}\right| = k-(\ell+2)k+n = n-(\ell+1)k$. Also, we have $\left|B_0 \setminus B_{(\ell+1)k}\right| = |B_0| - \left|B_0 \cap B_{(\ell+1)k}\right| = |B_{(\ell+1)k}| - \left|B_0 \cap B_{(\ell+1)k}\right| = \left|B_{(\ell+1)k} \setminus B_0\right|$. □

The next result provides a different bound on the number of bases of a cyclic matroid.

Theorem 3.15. *Let $\mathcal{M} = (\mathbb{Z}_n, \mathcal{B})$ be a cyclic k-matroid. Then, there are at least $m_2(n,k)$ distinct bases in $\mathcal{B}$ of the form $(B_0 \setminus Q) \cup P_k \cup P_{2k} \cup \cdots \cup P_{\ell k} \cup P_{(\ell+1)k}$, where $\ell = \left\lfloor \frac{n}{k} \right\rfloor - 1$, $\varnothing \subseteq P_{(i+1)k} \subseteq B_{(i+1)k}$ for $0 \leq i \leq \ell$, and*

$$m_2(n,k) \;=\; \sum_{|Q|=0}^{k} \sum_{j=0}^{\min\{n-(\ell+1)k,\,|Q|\}} \tbinom{n-(\ell+1)k}{j} \tbinom{k-j}{|Q|-j} \tbinom{|Q|-j+\ell-1}{\ell-1}.$$

Proof. Note that $\ell = \left\lfloor \frac{n}{k} \right\rfloor - 1$ gives the number of cyclic bases of the form B_{ik}, $1 \leq i \leq \ell$, which are disjoint pairwise as well from B_0 and for which basis exchange is possible for any subset $Q \subseteq B_0$. If $k \nmid n$, then we have an additional basis $B_{(\ell+1)k}$ with $\left|B_{(\ell+1)k} \setminus B_0\right| = n-(\ell+1)k$. Clearly, on performing multiple basis exchanges, for every $Q \subseteq B_0$ we obtain that there must be at least one basis element of the form

$$\big(B_0 \setminus Q\big) \cup P_k \cup P_{2k} \cup \cdots \cup P_{\ell k} \cup P_{(\ell+1)k}, \tag{1}$$

where $\varnothing \subseteq P_{(i+1)k} \subseteq B_{(i+1)k}$ for $0 \leq i \leq \ell$. Note that any such basis element can be uniquely written as in (1), hence it is counted at most once.

We count all sets of this form as follows. For a given subset Q, let j denote the number of elements $P_{(\ell+1)k}$ picked from the last basis element $B_{(\ell+1)k}$. This leaves $|Q|-j$ elements to be picked from the remaining bases, which is possible in any way since they are all disjoint from B_0. For fixed Q, the number of possibilities for doing basis exchange with the sets $B_k, \ldots, B_{\ell k}$ is given by the number of ways to split the number $|Q|-j$ into ℓ summands—allowing each summand to be equal to zero—i.e., to the number of length-ℓ weak compositions of $|Q|-j$. This is given by the number $\binom{|Q|-j+\ell-1}{\ell-1}$.

Note that in the case $k > n/2$, i.e., $\ell = 0$, the above number is 1 if and only if $|Q| = j$, i.e., if all elements are picked from B_k, and 0 otherwise. The latter value represents the fact that, if $\ell = 0$, there are no bases of the form B_{ik} disjoint from B_0, and the basis exchange must necessarily take place with B_k.

Now, for fixed values of $|Q|$ and j, we can choose Q in the following way: first pick j elements from $B_0 \setminus B_{(\ell+1)k}$ and then $|Q| - j$ elements from the remaining $k - j$ elements in B_0. Thus, the total number of bases obtained by this process for a fixed cardinality $|Q|$ and fixed $j \geq 0$ is $\binom{n-(\ell+1)k}{j}\binom{k-j}{|Q|-j}\binom{|Q|-j+\ell-1}{\ell-1}$.

Finally, note that $\left|B_{(\ell+1)k} \setminus B_0\right| = n - (\ell+1)k = \left|B_0 \setminus B_{(\ell+1)k}\right|$. So, we must have $j \leq \min\left\{|Q|, n-(\ell+1)k\right\}$. Because Q is allowed to vary across all subsets of B_0, we take a sum over $0 \leq |Q| \leq k$. This completes the proof. □

3.2 Group action approach for the number of bases

In order to further investigate cyclic matroids, we define the following group action $\varphi\colon \mathbb{Z}_n \times 2^{\mathbb{Z}_n} \to 2^{\mathbb{Z}_n}$ where

$$(s, A) \mapsto A + s. \tag{2}$$

It follows from the definition that the basis set $\mathcal{B}$ of a cyclic matroid is closed under the action φ. In other words, $\mathcal{B}$ is a union of orbits of $2^{\mathbb{Z}_n}$ under φ. Therefore, in order to study some properties of a cyclic matroid, we analyze here the orbits and stabilizers of φ.

For any $A \subseteq \mathbb{Z}_n$, the orbit of A is denoted by $\mathrm{Orb}(A) = \{A + s : s \in \mathbb{Z}_n\}$, and the stabilizer of A is denoted by $\mathrm{Stab}(A) = \{s \in \mathbb{Z}_n : A+s = A\}$.

Remark 3.16. Let $A \subseteq \mathbb{Z}_n$. Then $\mathrm{Stab}(A) = \mathrm{Stab}(A^C)$, and hence $|\mathrm{Orb}(A)| = \left|\mathrm{Orb}\left(A^C\right)\right|$, where A^C denotes the complement of A in $\mathbb{Z}_n$.

3.2.1 Size of a stabilizer

We know that for any $A \subseteq \mathbb{Z}_n$, $\mathrm{Stab}(A)$ is a subgroup of $\mathbb{Z}_n$, and so $|\mathrm{Stab}(A)|$ divides n. Moreover, $\mathrm{Stab}(A) = \langle s_0 \rangle$ for some s_0 that divides n.

Proposition 3.17. *Let $A \subseteq \mathbb{Z}_n$ and $s \in \{1, \ldots, n-1\}$. Then $s \in \mathrm{Stab}(A)$ if and only if A is a union of arithmetic progressions with common difference s, each with length $\frac{n}{\gcd(n,s)}$.*

Proof. First assume that $A = A_1 \cup A_2 \cup \cdots \cup A_r$, where each A_i is an arithmetic progression with common difference s and having length $\frac{n}{\gcd(n,s)}$. Pick a "first term" in each A_i and denote it by a_i (this choice is arbitrary since we are working modulo n). Note that the additive order of s mod n is equal to the cardinality of A_i, i.e., $\frac{n}{\gcd(n,s)}$, and so $a_i + j \cdot s \bmod n \in A_i$ for all $j \geq 0$. In other words, we must have $A_i + s = A_i$, for every index $i \in \{1, \ldots, r\}$. Therefore, $A + s = A$.

Conversely, assume that $A + s = A$ and pick $a_1 \in A$. Again, since the additive order of s mod n is equal to $\frac{n}{\gcd(n,s)}$, we must have $a_1 + \frac{n}{\gcd(n,s)} \cdot s = a_1$, and $A_1 \coloneqq \{a_1, a_1 + s, \ldots, a_1 + (\frac{n}{\gcd(n,s)} - 1) \cdot s\} \subseteq A$. If $A = A_1$, then the proof is complete. If not, we have some $a_2 \in A \setminus A_1$, so $A_2 \coloneqq \{a_2, a_2 + s, \ldots, a_2 + (\frac{n}{\gcd(n,s)} - 1) \cdot s\} \subseteq A$, and $A_2 \cap A_1 = \varnothing$. Continuing in this manner, we obtain, in a finite number of steps, $A = A_1 \cup A_2 \cup \cdots \cup A_r$, where each A_i is an arithmetic progression with common difference s and having length $\frac{n}{\gcd(n,s)}$. This completes the proof. □

The above proposition shows that for any $s \in \mathrm{Stab}(A)$, $\frac{n}{\gcd(n,s)}$ divides $|A|$. In particular, the result also holds for a generator of the stabilizer group.

Corollary 3.18. *Let $A \subseteq \mathbb{Z}_n$, $|A| = k$, and $\mathrm{Stab}(A) = \langle s_0 \rangle$. Then for $r = \frac{k \gcd(n, s_0)}{n} \in \mathbb{Z}$ we have*

$$A = \bigcup_{i=1}^{r} (a_i + \mathrm{Stab}(A)),$$

for some $a_1, \ldots, a_r \in \mathbb{Z}_n$. Consequently, $|\mathrm{Stab}(A)|$ divides k, and thus also $\gcd(k, n)$.

Proof. Proposition 3.17 implies that $s \in \mathrm{Stab}(A)$ if and only if A is a union of $\frac{k \gcd(n,s)}{n}$ many full-length arithmetic progressions, each with common difference s. Thus, $r \in \mathbb{Z}$, and we obtain

$$A = \bigcup_{i=1}^{r} (a_i + \mathrm{Stab}(A)),$$

for some $a_1, \ldots, a_r \in \mathbb{Z}_n$. We may assume that $a_1, \ldots, a_r \in \{0, \ldots, s-1\}$. □

As a consequence of the above result, we note that whenever n and k are co-prime, $\mathrm{Stab}(A)$ is trivial for all subsets $A \subseteq \mathbb{Z}_n$ of size k.

In the following, we relate the size of the stabilizer of A with the number of parts in the consecutive block structure $\pi(A)$ of A; see Definition 3.4.

Proposition 3.19. *Let $A \subseteq \mathbb{Z}_n$ with $\pi(A) = (D_1, D_2, \ldots, D_\ell)$. Then $|\mathrm{Stab}(A)|$ divides ℓ.*

Proof. Let $\mathrm{Stab}(A) = \langle s \rangle$. If $s = 0$, then the statement follows immediately.

Assume $s \neq 0$ and let $r = n/s = |\mathrm{Stab}(A)|$. We define the following relation on the set $\{D_1, \ldots, D_\ell\}$:

$$D_i \sim D_j \iff D_i = D_j + ts \quad \text{for some } t \in \{0, \ldots, r-1\}.$$

It is easy to check that $\sim$ is an equivalence relation. We show that each equivalence class contains exactly r elements. For any $i \in \{1, \ldots, \ell\}$ and $t \in \{0, \ldots, r-1\}$, we have that $D_i + ts \in \{D_1, \ldots, D_\ell\}$ because $A + ts = A$. Moreover, if $D_i + t_1 s = D_i + t_2 s$ for some $t_1, t_2 \in \{0, \ldots, r-1\}$, then $t_1 = t_2$. This implies that each equivalence class contains r elements. Hence, r divides ℓ. □

We know from Proposition 3.7 that a cyclic k-matroid over $\mathbb{Z}_n$ contains bases of the form $B_i = \{i, i+1, \ldots, i+k-1\}$ for all $i \in \{0, \ldots, n-1\}$. Clearly, all these bases belong to the same orbit, as $B_i = B_0 + i$ for each i. Moreover, using Lemma 2.3 we get that, for each subset $Q \subset B_0$, there exists a basis of the form $(B_0 \setminus Q) \cup P$ for some $P \subset B_0^C$. As an application of Proposition 3.19, we obtain the following bound on the size of the stabilizer of such sets.

Corollary 3.20. *Let $A = (B_0 \setminus Q) \cup P \subseteq \mathbb{Z}_n$, where $Q \subset B_0$ and $P \subset B_0^C$ with $|Q| = |P|$. Then $|\mathrm{Stab}(A)| \leq 2|Q| + 1$.*

Proof. Let r and s be the number of blocks in the consecutive block structure of Q and P, respectively. Observe that the number of blocks in the consecutive block structure of A takes one of the values in the set $\{r+s-1, r+s, r+s+1\}$. By Proposition 3.19, $|\mathrm{Stab}(A)|$ divides this value, and is thus bounded from above by the value $2|Q| + 1$, as required. □

Example 3.21. Let $A = \big(\{0, 1, \ldots, k-1\} \setminus \{q\}\big) \cup \{p\}$ for some

$$q \in \{0, 1, \ldots, k-1\}$$

and

$$p \in \{k, k+1, \ldots, n-1\}.$$

Using Corollary 3.20, we get that $|\mathrm{Stab}(A)| \in \{1, 2, 3\}$. Note that if n is not a multiple of 2 or 3, then $\mathrm{Stab}(A)$ is trivial. We examine the case $|\mathrm{Stab}(A)| > 1$. We may assume that $2 \leq k \leq n/2$, as $\mathrm{Stab}(A) = \mathrm{Stab}(A^C)$.

1. $|\mathrm{Stab}(A)| = 3$ if and only if $n = 6,\ k = 3$, and $A = \{0, 2, 4\}$.

   In this case, the consecutive block structure of A is

   $$\pi(A) = \big(\{0, 1, \ldots, q-1\},\ \{q+1, \ldots, k-1\},\ \{p\}\big).$$

   Thus, $\mathrm{Stab}(A) = \langle n/3 \rangle$ if and only if the sizes of each block are equal and the shift by $n/3$ permutes them. This is possible only if $q = 1$, $k = 3$, $p = 4$, and $n = 6$.

2. $|\mathrm{Stab}(A)| = 2$ if and only if n is even and $A = \{0, n/2\}$ or $A = \{1, n/2 + 1\}$.

   In this case,

   $$\big|A \cap \{0, 1, \ldots, n/2 - 1\}\big| = \big|A \cap \{n/2, n/2 + 1, \ldots, n-1\}\big|.$$

   Since $k \leq n/2$, we have that $\big|A \cap \{0, 1, \ldots, n/2 - 1\}\big| \geq k - 1$ and $\big|A \cap \{n/2, n/2 + 1, \ldots, n-1\}\big| \leq 1$. Therefore, $k = 2$ and hence $A = \{0, n/2\}$ or $A = \{1, n/2 + 1\}$.

3.2.2 Number of bases

Let $n \geq 3$, $k \in \{2, \ldots, n-1\}$, and $\mathcal{M} = (\mathbb{Z}_n, \mathcal{B})$ be a cyclic k-matroid. Then $\mathcal{B}$ is closed under the action (2) of $\mathbb{Z}_n$, and hence it is a union of some orbits of subsets of size k. The following two results are based on the observation that the block composition $c(s + A)$ is simply a cyclic shift of the block composition $c(A)$; hence, they are equal as unordered sets. This leads to a bound on the number of distinct orbits of bases of the form $(B_0 \setminus Q) \cup P$, where $B_0 = \{0, 1, \ldots, k-1\}$, $Q \subseteq B_0$, and $P \subseteq B_0^C$, which are contained in $\mathcal{B}$.

Theorem 3.22. *There are at least $\lfloor k/4 \rfloor + 1$ orbits of bases of the form $A = \big(B_0 \setminus \{q\}\big) \cup \{p\}$, where $p \in B_0^C$. Consequently, there are at least $\frac{n}{\gcd(n,k)}\big(\lfloor \frac{k}{4} \rfloor + 1\big)$ bases in $\mathcal{B}$.*

Proof. We first note that the block composition associated to

$$A = \big(B_0 \setminus \{q\}\big) \cup \{p\}$$

has the following possibilities:

$$c(A) = \begin{cases} (q, k-q-1, 1), & \text{if } q \notin \{0, k-1\},\ p \notin \{k, n-1\}, \\ (k-q-1, q+1), & \text{if } q \notin \{0, k-1\},\ p = n-1, \\ (q, k-q), & \text{if } q \notin \{0, k-1\},\ p = k, \\ (k-1, 1), & \text{if } q = 0,\ p \neq k \text{ or } q = k-1,\ p \neq n-1, \\ (k), & \text{if } q = 0,\ p = k \text{ or } q = k-1,\ p = n-1. \end{cases}$$

Now suppose that $A = \big(B_0 \setminus \{q\}\big) \cup \{p\}$ and $A' = \big(B_0 \setminus \{q'\}\big) \cup \{p'\}$ are in the same orbit, i.e., $s + A = A'$ for some s. Clearly, the block composition of A' is then a shift of $c(A)$. Thus, we have one of the following cases:

1. $\{q, k-q-1, 1\} = \{q', k-q'-1, 1\}$, i.e., $q = q'$ or $q + q' = k-1$.
2. $\{q+1, k-q-1\} = \{q'+1, k-q'-1\}$, i.e., $q = q'$ or $q + q' = k$.
3. $\{q, k-q\} = \{q', k-q'\}$, i.e., $q = q'$ or $q + q' = k+1$.
4. $\{q, k-q\} = \{q'+1, k-q'-1\}$ or $\{q+1, k-q-1\} = \{q', k-q'\}$, i.e., $q = q' \pm 1$ or $q + q' = k-1$.
5. $q, q' \in \{0, k-1\}$.

Lemma 3.10 shows that there exist $(n-k)$ bases not containing q. Thus, if we fix q and pick q' so that $|q - q'| > 1$ and $q + q' < k-1$, then all the resulting bases give rise to distinct orbits. In particular, there is a distinct orbit corresponding to each of the $m+1$ values $q \in \{0, 2, 4, \ldots, 2m\}$, where $2m + 2(m-1) < k-1 \leq 2(m+1) + 2m$ or $m = \left\lceil \frac{k-3}{4} \right\rceil = \left\lfloor \frac{k}{4} \right\rfloor$. The final result on the number of bases follows using Corollary 3.18, which implies that the size of an orbit is at least $\frac{n}{\gcd(n,k)}$. □

We further improve the lower bound on the number of orbits by considering the bases of the form $(B_0 \setminus Q) \cup P$, where $|Q| > 1$ and $P \subseteq B_0^C$.

Theorem 3.23. *The total number of orbits in $\mathcal{B}$ is bounded from below by $M + \left\lfloor \frac{k}{4} \right\rfloor + 1$, where*

$$M = \left\lfloor \log_2 \left(\frac{\left\lfloor \frac{k}{2} \right\rfloor + 2}{3} \right) \right\rfloor.$$

In particular, we have the following lower bound on the number of bases in $\mathcal{B}$:

$$m_3(n,k) = \big(M + \left\lfloor \tfrac{k}{4} \right\rfloor + 1\big) \tfrac{n}{\gcd(n,k)}.$$

Proof. Let r and s denote, respectively, the number of blocks in the consecutive block structure of Q and P. It is easy to see that the number of blocks in the block structure of the basis element $A = (B_0 \setminus Q) \cup P$ is at least $r + s - 1$ and at most $r + s + 1$. Now, if $|Q| \leq \lfloor k/2 \rfloor$, we can choose Q so that $r = |Q|$. Then A has at least r and at most $2r + 1$ blocks in its decomposition.

Consider the finite sequence $S = (x_1 = 1, x_2 = 4, \ldots, x_i, \ldots, x_\ell)$, where $x_i = 2x_{i-1} + 2$ for $2 \leq i \leq \ell$ and where ℓ is such that $x_\ell \leq \lfloor k/2 \rfloor$ and $2x_\ell + 2 \geq k/2$. Then for each pair of distinct $r, r' \in S$, there are sets Q_r and $Q_{r'}$ with $|Q_r| = r$ and $|Q_{r'}| = r'$ that have r and r' blocks, respectively, and give rise to distinct orbits. Thus, the size ℓ of the sequence S gives a lower bound for the number of orbits.

We have

$$x_i = 2x_{i-1} + 2 = 2 + 2^2 + 2^3 + \cdots + 2^{i-2} + 2^i = 3 \cdot 2^{i-1} - 2.$$

Moreover, for each index i,

$$3 \cdot 2^{i-1} - 2 = x_i \leq \lfloor k/2 \rfloor$$

or $i \leq \log_2\left(\frac{\lfloor k/2 \rfloor + 2}{3}\right) + 1$. Therefore, we have

$$\ell = \left\lfloor \log_2\left(\frac{\lfloor k/2 \rfloor + 2}{3}\right) \right\rfloor + 1.$$

From the discussion above, it is clear that the number of orbits arising from the case $|Q| > 1$ is at least $\ell - 1$. From Theorem 3.22, we also have the lower bound $\lfloor k/4 \rfloor + 1$ for the number of orbits for $|Q| = 1$. Plugging in this value then gives the result. □

Proposition 3.24. *In any orbit under the action $\mathbb{Z}_n \times \mathcal{B} \to \mathcal{B}$, where $(c, B) \mapsto c + B$, there exists a representative of the form*

$$\{0, a_1, \ldots, a_{k-1}\}$$

such that $a_i \leq ni/k$, for all $1 \leq i \leq (k-1)$. Moreover, if $a_i < in/k$ for all i, then such a representative is unique. In particular, if $\gcd(n, k) = 1$, then this representation is always unique.

Proof. (Existence) Consider an orbit $\mathrm{Orb}(A)$ of an arbitrary set A. We may assume that A has a form $\{0, a_1, \ldots, a_{k-1}\}$ with a_i's in increasing order. If

$a_i \leq in/k$ for each i, then we are done. Therefore, we assume that this is not the case.

Let $1 \leq i \leq k-1$ be such that $a_i - in/k$ is largest. We define $B \coloneqq A - a_i$ and write B as $\{0, b_1, \ldots, b_{k-1}\}$. We claim that $b_j \leq jn/k$ for each j.

For all $1 \leq j \leq k-i-1$, we note that

$$\begin{aligned} b_j = a_{i+j} - a_i &= a_{i+j} - in/k - (a_i - in/k) \\ &\leq a_{i+j} - in/k - \big(a_{j+i} - (j+i)n/k\big) \\ &= jn/k. \end{aligned}$$

The inequality above follows because i is such that $a_i - in/k$ is largest. Similarly, for all $k-i \leq j \leq k-1$, we note that

$$\begin{aligned} b_j = n - a_i + a_{k-i-j} &= (n - in/k) + a_{k-i-j} - (a_i - in/k) \\ &\leq (k-i)n/k + a_{k-i-j} - \big(a_{k-i-j} - (k-i-j)n/k\big) \\ &= jn/k. \end{aligned}$$

(Uniqueness) Let us assume that

$$A = \{0, a_1, \ldots, a_{k-1}\} \qquad \text{and} \qquad B = \{0, b_1, \ldots, b_{k-1}\}$$

are two distinct sets in the same orbit satisfying $a_i, b_i < in/k$ for each i. Since A and B are in the same orbit, $B = A - a_i$ for some i. This implies $b_{k-i} = n - a_i \geq n - in/k = (k-i)n/k$. This is a contradiction as by assumption $b_{k-i} < (k-i)n/k$. □

Corollary 3.25. *Let n, k be positive integers with $\gcd(n,k) \neq 1$ and let $A = \{0, a_1, \ldots, a_{k-1}\}$ be an orbit representative with $a_i < in/k$ for each $i \in \{1, \ldots, k-1\}$. Then, $|\mathrm{Orb}(A)| = n$.*

Proof. Suppose $|\mathrm{Orb}(A)| = s < n$, then by Corollary 3.18 we have that s is a multiple of $n/\gcd(n,k)$. Let $s = in/k$ for some $1 \leq i \leq k-1$.

Since $A + s = A$, there exists j such that $a_j + s = n \equiv 0 \pmod{n}$. This implies $a_j = (k-i)n/k$. Now, since $a_j \leq jn/k$, we have that $k - i \leq j$.

As $0 < a_1 < \cdots < a_{k-1}$, we note that by adding s we are shifting the indices by $k - j$. In particular, $0 + s = a_{k-j}$. Again, since $a_{k-j} \leq (k-j)n/k$, we have that $i \leq k - j$, i.e., $j \leq k - i$. This implies that $j = k - i$, and hence $a_i = a_{k-j} = s = in/k$. This is a contradiction because we assumed that $a_i < in/k$ for all i. □

Corollary 3.26. *Let n and k be positive integers such that $\gcd(n,k) \neq 1$. Then, the number of orbits with size strictly less than n is at most $\mathcal{O}(n^{k-2})$.*

Proof. Let $A = \{0, a_1, a_2, \ldots, a_{k-1}\}$ be an orbit representative satisfying $\mathrm{Orb}(A) < n$, then from previous corollary it follows that $a_i = in/k$ for some $i \in \{1, \ldots, k-1\}$.

Let T_i be the set of orbit representatives A satisfying $|\mathrm{Orb}(A)| < n$ and $a_i = in/k$. Then, the set of all orbit representatives satisfying $\mathrm{Orb}(A) < n$ is equal to $\bigcup_{i=1}^{k-1} T_i$. Note that $|T_i| \leq n^{k-2}$, as $a_i = in/k$ is fixed and a_j has at most jn/k choices for each $j \neq i$. Therefore, $\left|\bigcup_{i=1}^{k-1} T_i\right| \leq (k-1)n^{k-2}$. □

Using the above results, we derive another bound on the minimum number of bases in a cyclic k-matroid. The main idea here is to count the number of orbit representatives that can be constructed using the multiple basis exchange property.

In the following series of results we focus on the disjoint bases

$$B_0, B_k, B_{2k}, \ldots, B_{\ell k},$$

where $\ell = \lfloor n/k \rfloor - 1$. To ease the notations, we define $\beta\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq -1}$ given by

$$\beta(t) = \max\big\{s \mid (s+1)k - 1 \leq t\big\} = \big\lfloor (t+1)/k \big\rfloor - 1.$$

In other words, the value $\beta(t)$ is the maximum index s such that

$$B_{sk} \subseteq \{0, \ldots, t\}.$$

If no such index exists, then $\beta(t)$ is -1 by convention.

Theorem 3.27. *Let $\mathcal{M} = (\mathbb{Z}_n, \mathcal{B})$ be a cyclic k-matroid. Assume that $k \leq n/2$, so that $\beta\big(\lfloor in/k \rfloor\big) \geq 0$ for $i \geq 1$. Further, let*

$$S \coloneqq \Big\{(s_1, \ldots, s_{k-1}) \in \mathbb{Z}^{k-1} \mid 0 \leq s_1 \leq \beta\big(\lfloor n/k \rfloor\big) \text{ and } s_{i-1} \leq s_i \leq \beta\big(\lfloor in/k \rfloor\big) \text{ for each } i \in \{2, \ldots, k-1\}\Big\}.$$

Then, if $\gcd(n,k) = 1$, then the total number of orbits in $\mathcal{B}$ is at least $|S|$. If $\gcd(n,k) \neq 1$, then there exists a lower bound $n_s = |S| - \mathcal{O}(n^{k-2})$ for the total number of orbits in $\mathcal{B}$.

Proof. To bound the number of orbits, we first show that for each $(s_1, \ldots, s_{k-1}) \in S$ there exists a unique set $A = \{0, \alpha_1, \ldots, a_{k-1}\} \in \mathcal{B}$ satisfying $a_i \leq in/k$.

We may assume that $s_1, \ldots, s_{k-1}$ are as follows:

$$\begin{aligned} s_1 = s_2 = \cdots = s_{j_0} &= 0, \\ s_{j_0+1} = \cdots = s_{j_1} &= i_1, \\ &\vdots \\ s_{j_{t-1}+1} = \cdots = s_{j_t} &= i_t, \end{aligned}$$

for some $t \geq 0$, $0 \leq j_0 < j_1 < \cdots < j_t = k-1$, and $0 < i_1 < i_2 < \cdots < i_t$. Here, $j_0 = 0$ indicates that the first value s_1 is also greater than 0.

Now, let Q be any subset of $B_0 \setminus \{0\}$ having size $|Q| = k - j_0 - 1$. Then, we apply multiple basis exchange property to obtain a basis

$$(B_0 \setminus Q) \cup P_{i_1 k} \cup \cdots \cup P_{i_t k},$$

where $P_{i_w} \subseteq B_{i_w k}$ of size $|P_w| = j_w - j_{w-1}$ for each $w \in \{1, \ldots, t\}$. We can write the obtained basis as $\{0, a_1, \ldots, a_{k-1}\}$ with $a_1, \ldots, a_{j_0} \in B_0$ and $a_{j_{w-1}+1}, \ldots, a_{j_w} \in B_{i_w k}$ for each $w \in \{1, \ldots, t\}$. In particular, $a_i \in B_{s_i k}$ for each $i \in \{1, \ldots, k-1\}$. Since each $s_i \leq \beta\big(\lfloor in/k \rfloor\big)$, we get that $a_i \leq in/k$ for each $i \in \{1, \ldots, k-1\}$. Finally, we note that each $(s_1, \ldots, s_{k-1}) \in S$ gives a distinct basis $\{0, a_1, \ldots, a_{k-1}\}$ of the above form because each $a_i \in B_{s_i k}$ and $B_k, B_{2k}, \ldots, B_{\ell k}$ are pairwise disjoint.

Using Proposition 3.24, we know that each set $A = \{0, a_1, \ldots, a_{k-1}\}$ of the above form corresponds to an orbit. If $\gcd(n, k) = 1$, then this correspondence is one-to-one because $a_i < in/k$ for each i, and such sets are unique in each orbit.

Now assume that $\gcd(n, k) \neq 1$. In this case, the corresponding orbits may not be unique. However, from Proposition 3.24 we observe that the non-unique orbits correspond to sets A satisfying $a_i = in/k$ for some i. The number of all such sets A is at most $\mathcal{O}(n^{k-2})$. Thus, there exists a lower bound $n_s = |S| - \mathcal{O}(n^{k-2})$ for the number of unique orbits obtained by this process. □

We observe that S is a set of integer vectors of a convex polytope. Using Ehrhart's theory for counting lattice points in certain polytopes, we can approximate the size of S.

Theorem 3.28. *Let $\mathcal{M} = (\mathbb{Z}_n, \mathcal{B})$ be a cyclic k-matroid for $k \leq n/2$ and let S be as defined in Theorem 3.27. Then,*

$$|S| = \frac{n^{k-1}}{k^{2k-2}} + \mathcal{O}(n^{k-2}).$$

Consequently, a lower bound on the number of bases in $\mathcal{B}$ is

$$m_4(n,k) = \frac{n^k}{k^{2k-2}} + \mathcal{O}(n^{k-1}).$$

Proof. We define a convex polytope P_n that is inspired by the constraints of the set S, i.e.,

$$P_n \coloneqq \Big\{(s_1, \ldots, s_{k-1}) \in \mathbb{R}^{k-1} \mid 0 \leq s_1 \leq n/k^2 \text{ and } s_{i-1} \leq s_i \leq in/k^2 \text{ for each } i \in \{2, \ldots, k-1\}\Big\}.$$

Let $T = P_n \cap \mathbb{Z}^{k-1}$. Then, it is easy to see that $S \subseteq T$ because $\beta(e) \leq e/k$ for any integer e. Moreover, $T \setminus S$ contains vectors that have at least one coordinate s_i satisfying $\beta\big(\lfloor in/k \rfloor\big) < s_i \leq in/k^2$. Thus we can write $T \setminus S = \bigcup_{i=1}^{k-1} U_i$, where

$$U_i = \Big\{(s_1, \ldots, s_{k-1}) \in P_n \cap \mathbb{Z}^{k-1} \mid \beta\big(\lfloor in/k \rfloor\big) < s_i \leq in/k^2\Big\}.$$

Note that there is at most one integer in the interval $\Big(\beta\big(\lfloor in/k \rfloor\big), in/k^2\Big]$. Thus, $|U_i| \leq \mathcal{O}(n^{k-2})$ because s_i has at most one choice and $0 \leq s_j \leq \lfloor in/k^2 \rfloor$ for $j \neq i$. This implies

$$|T \setminus S| = \mathcal{O}(n^{k-2}). \tag{3}$$

Now, to calculate $|T|$, we define another convex polytope

$$P \coloneqq \Big\{(t_1, \ldots, t_{k-1}) \in \mathbb{R}^{k-1} \mid 0 \leq t_1 \leq 1/k^2 \text{ and } t_{i-1} \leq t_i \leq i/k^2 \text{ for each } i \in \{2, \ldots, k-1\}\Big\}.$$

We further note that $P_n = nP = \big\{n(t_1, \ldots, t_{k-1}) \mid (t_1, \ldots, t_{k-1}) \in P\big\}$. To calculate $\big|nP \cap \mathbb{Z}^{k-1}\big|$ we use Ehrhart's theorem [5], which states that $\big|nP \cap \mathbb{Z}^{k-1}\big|$ is a quasi-polynomial[1] on n of degree $k-1$. Moreover, we have that

$$|T| = \big|nP \cap \mathbb{Z}^{k-1}\big| = \text{Volume(P)} \cdot n^{k-1} + \mathcal{O}(n^{k-2}). \tag{4}$$

[1]A function $f\colon \mathbb{Z} \to \mathbb{Z}$ is quasi-polynomial of degree d if there exist periodic functions $f_i\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}$ such that $f(n) = \sum_{i=0}^{d} f_i(n) n^d$.

Finally, we observe that P is a parallelotope in $\mathbb{R}^{k-1}$ of rank $k-1$ defined by the vectors $v_1 = (1/k^2, 1/k^2, \ldots, 1/k^2)$, $v_2 = (0, 1/k^2, \ldots, 1/k^2)$, $\ldots$, $v_{k-1} = (0, \ldots, 0, 1/k^2)$, i.e., $P = \left\{ \sum_{i=1}^{k-1} \lambda_i v_i \mid 0 \leq \lambda_i \leq 1 \right\}$. The volume of P is given by

$$\text{Volume}(P) = \left| \det\left([v_1 \quad \ldots \quad v_{k-1}] \right) \right| = \left(\tfrac{1}{k^2} \right)^{k-1}. \tag{5}$$

Combining (3), (4), and (5), we get

$$|S| = |T| - |T \setminus S| = \frac{n^{k-1}}{k^{2k-2}} + \mathcal{O}(n^{k-2}).$$

If $\gcd(n,k) = 1$, then we know that the size of each orbit is n. Hence, in this case,

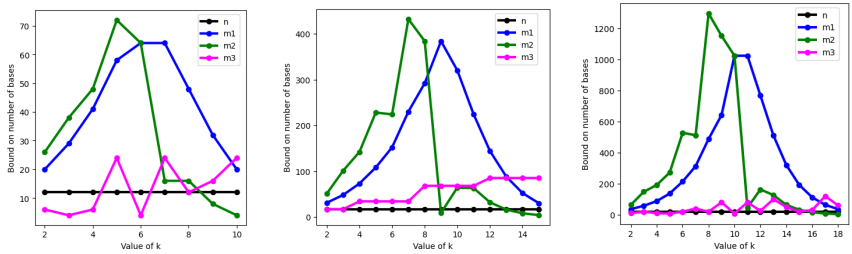
$$m_4(n,k) = n|S| = \frac{n^k}{k^{2k-2}} + \mathcal{O}(n^{k-1}).$$

If $\gcd(n,k) \neq 1$, then from Corollary 3.26 we know that the number of orbits with size strictly less than n is at most $\mathcal{O}(n^{k-2})$. Therefore, there are at least $|S| - \mathcal{O}(n^{k-2})$ orbits having maximum size n. This implies,

$$m_4(n,k) = \frac{n^k}{k^{2k-2}} + \mathcal{O}(n^{k-1}). \qquad \square$$

Remark 3.29. Combining the results from Theorems 3.13, 3.15, 3.23, and 3.27, we get four distinct lower bounds on the number of basis elements: $m_1(n,k)$, $m_2(n,k)$, $m_3(n,k)$, and $m_4(n,k)$. We can further improve these bounds using the following observations:

1. The dual of a cyclic k-matroid is a cyclic $(n-k)$-matroid. Thus, $m_1(n, n-k)$, $m_2(n, n-k)$, and $m_3(n,k)$ are also lower bounds on the number of bases in a cyclic k-matroid. This is not true for $m_4(n,k)$, since it explicitly assumes that $k \leq n/2$. However, it does imply that the bound $m_4(n,k)$ also applies without making this assumption on k.
2. When $\gcd(n,k) = 1$, each orbit under the action (2) has n elements. Since the set of bases $\mathcal{B}$ is a collection of orbits, the number of bases in $\mathcal{B}$ in this case must be a multiple of n. So, the lower bound $m_i(n,k)$ can be improved to $\left\lceil \frac{m_i}{n} \right\rceil n$ for $i = 1, 2, 3$.
3. Using Corollary 3.18, it follows that the size of each orbit under the action (2) is a multiple of $n/\gcd(n,k)$. Since the set of bases $\mathcal{B}$ is a collection of orbits, the number of bases in $\mathcal{B}$ must be a multiple of $n/\gcd(n,k)$.



(a) $n = 12$ (b) $n = 17$ (c) $n = 20$

Figure 3.1: Comparison of the bounds for fixed values of n and varying k.

From the above remark, we obtain the best possible lower bound m_B from m_1, m_2, and m_3:

$$m_B(n,k) = \max\left\{ \left\lceil \frac{m_i(n,t)}{(n/\gcd(n,t))} \right\rceil \frac{n}{\gcd(n,t)} \mid i \in \{1,2,3\},\, t \in \{k, n-k\} \right\}.$$

3.3 Experimental results

In the following discussion, we compare explicit values of the different bounds for some values of n and k. In Table 3.1, for each bound we provide some values of the number of bases for different n and k. Note that in the case of $n = 6$ and $k = 3$, the bound 8 is achieved exactly in the cyclic matroid $\mathcal{M}_1$ of Example 4.9. We graphically show in Figures 3.1 and 3.2 the variation of the bounds m_1, m_2, and m_3 with different values of, and relationships between, n and k.

Observe that the bounds m_1 and m_2 by far exceed m_3 for the "middle" values of k, whereas m_3 becomes significant when k is large enough, particularly when k attains its maximum value $k = n-2$. (We disregard the case $k = n-1$ since this only gives the uniform matroid.) It is also observed that the difference between m_2 and the other two bounds increases rapidly as n is increased. This is to be expected since m_2 counts more types of bases than m_1 and m_3, and the possibilities for these types grow rapidly with n.

In Appendix A we provide some explicit examples of cyclic matroids generated through a randomized computer search.

Table 3.1: Comparison of the lower bounds on the number of bases in an arbitrary cyclic k-matroid over a ground set of size n.

k	$m_1(n,k)$	$m_1(n,n-k)$	$m_2(n,k)$	$m_2(n,n-k)$	$m_3(n,k)$	$m_3(n,n-k)$	m_B
2	8	8	8	4	3	6	9
3	8	8	8	8	2	2	8

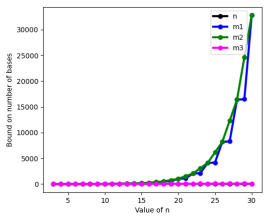
(a) $n = 6$

k	$m_1(n,k)$	$m_1(n,n-k)$	$m_2(n,k)$	$m_2(n,n-k)$	$m_3(n,k)$	$m_3(n,n-k)$	m_B
2	19	18	24	4	11	44	44
3	27	28	36	8	11	44	44
4	35	40	40	15	22	22	44
5	47	48	48	6	22	22	55

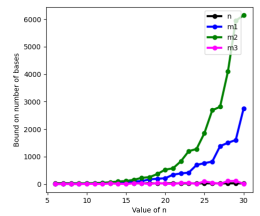
(b) $n = 11$

k	$m_1(n,k)$	$m_1(n,n-k)$	$m_2(n,k)$	$m_2(n,n-k)$	$m_3(n,k)$	$m_3(n,n-k)$	m_B
2	27	26	41	4	15	75	75
3	40	44	63	8	5	25	65
4	60	72	108	16	30	60	120
5	85	112	112	32	6	12	114
6	124	160	216	42	10	20	220
7	156	192	192	8	30	60	195

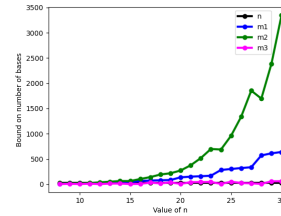
(c) $n = 15$



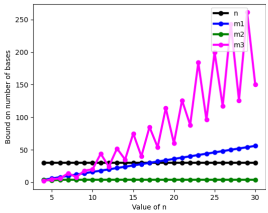
(a) $n \leq 30$, $k = \lfloor \frac{n}{2} \rfloor$



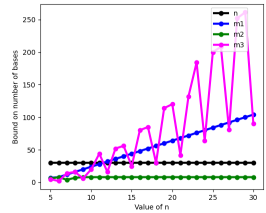
(b) $n \leq 30$, $k = \lfloor \frac{n}{3} \rfloor$



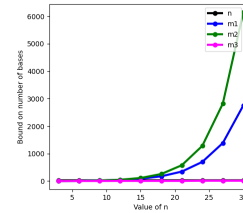
(c) $n \leq 30$, $k = \lfloor \frac{n}{4} \rfloor$



(d) $n \leq 30$, $k = n - 2$



(e) $n \leq 30$, $= n - 3$



(f) $n \leq 30$, $3 \mid n$, $k = n/3$

Figure 3.2: Comparison of the bounds for fixed values of k and varying n.

3.4 Asymptotic analysis of the bounds

Finite values of these bounds do not provide any intuition towards the tightness of the bounds. Therefore, we analyze their asymptotic behavior. In order to do so, we fix the value of k to be a constant and let n go to infinity.

Let $M(n,k)$ be the minimum number of bases in a cyclic k-matroid on n elements. Then, in this section, we are interested in computing the following limit

$$\liminf_{n\to\infty} \frac{1}{n^k} M(n,k)$$

where k is a fixed constant.

It is easy to see that the first and third lower bound, i.e., $m_1(n,k)$ and $m_3(n,k)$, are $\mathcal{O}(n)$, assuming k is a constant. Therefore, it follows that, for any $k \geq 2$,

$$\lim_{n\to\infty} \frac{1}{n^k} m_1(n,k) = \lim_{n\to\infty} \frac{1}{n^k} m_3(n,k) = 0.$$

However, the asymptotic behavior of lower bounds $m_2(n,k)$ and $m_4(n,k)$ are more interesting.

Proposition 3.30. *Let k be a fixed integer. Then,*

$$\lim_{n\to\infty} \frac{1}{n^k} m_2(n,k) \geq \frac{1}{k! \cdot k^k}.$$

Proof. Recall from Theorem 3.15 that

$$m_2(n,k) \;=\; \sum_{|Q|=0}^{k} \sum_{j=0}^{\min\{n-(\ell+1)k,|Q|\}} \tbinom{n-(\ell+1)k}{j} \tbinom{k-j}{|Q|-j} \tbinom{|Q|-j+\ell-1}{\ell-1}.$$

As $\ell = \left\lfloor \frac{n}{k} \right\rfloor - 1$, the value of ℓ goes to infinity when n goes to infinity. Therefore, the most dominant factor in the above expression is $\binom{|Q|-j+\ell-1}{\ell-1}$, because all the other factors are polynomial in k. It is easy to see that $\binom{|Q|-j+\ell-1}{\ell-1}$ maximizes when $|Q| = k$ and $j = 0$. Hence, we get the following

$$m_2(n,k) \geq \tbinom{k+\ell-1}{\ell-1} = \tbinom{k+\ell-1}{k}$$

This implies,

$$\begin{aligned}\lim_{n\to\infty}\frac{1}{n^k}m_2(n,k) &\geq \lim_{n\to\infty}\frac{1}{n^k}\binom{k+\ell-1}{k}\\ &= \lim_{n\to\infty}\frac{(\ell+k-1)(\ell+k-2)\cdots(\ell)}{n^k k!}\\ &= \frac{1}{k!(k)^k}.\end{aligned}$$

□

Proposition 3.31. *Let k be a fixed integer. Then,*

$$\lim_{n\to\infty}\frac{1}{n^k}m_4(n,k) = \frac{1}{k^{2k-2}}.$$

Proof. This follows directly from Theorem 3.28. □

With respect to the above analysis, we observe that $m_4(n,k)$ is asymptotically the largest lower bound on the number of basis elements. In particular, for $k=2$ the $m_4(n,k)$ bound is asymptotically tight.

Corollary 3.32. *Let $k=2$. Then, $m_4(n,k)$ is asymptotically tight.*

Proof. For each even $n \geq 2$, we consider the matroid $\mathcal{M}_n = (E_n, \mathcal{B}_n)$ as defined in Example 3.8, i.e., the basis set is given by

$$\mathcal{B}_n = \big\{\{a_0, a_i\} \mid a_i \equiv i \pmod{n}\big\}.$$

Then, the number of basis elements in $\mathcal{M}_n$ is equal to $(n/2)^2$. Therefore,

$$\lim_{n\to\infty}\frac{1}{n^2}|\mathcal{B}_n| = \frac{1}{4} = \lim_{n\to\infty}\frac{1}{n^k}m_4(n,2).$$

□

4 Algebraic and geometric connections

In this section, we provide examples of algebraic, geometric, and combinatorial objects that may be linked to cyclic matroids. The main objects of interest are the ones introduced in Sections 2.2, 2.3, and 2.4.

4.1 Cyclic projective planes and cyclic codes

There are many works on the existence and non-existence of cyclic projective planes and their collineation groups. We refer the interested reader to [2, 12, 23]. Moreover, cyclic projective codes have been studied in relation with designs, difference sets, and cyclic codes; see [15, Section 8.7].

Let q be a prime power and consider a Desarguesian projective plane $\mathrm{PG}(2, q)$ and its incidence matrix A. Then, it is known that A is necessarily a circulant matrix; see for instance [13, Theorem 4.2.2 and its corollary]. Since the entries of A are only 0's and 1's, we can consider A as a matrix over a finite field $\mathbb{F}_p$ for p prime. In this case, the rank of A has been completely determined by Graham and MacWilliams [8]. Here we state their result only for $p = 2$.

Theorem 4.1. *The rank over $\mathbb{F}_2$ of the incidence matrix A of a Desarguesian projective plane $\mathrm{PG}(2, q)$ is*

$$k = \begin{cases} q^2 + q, & \text{if } q \text{ is odd,} \\ 3^t + 1, & \text{if } q = 2^t. \end{cases}$$

Corollary 4.2. *Let $\mathcal{M}(A)$ be the representable matroid constructed from the incidence matrix A of a cyclic projective plane. Then, $\mathcal{M}(A)$ is a cyclic k-matroid, representable over $\mathbb{F}_2$, with k equal to the rank of A.*

Proof. It is easy to see that, by rearranging the columns, the incidence matrix A is a circulant matrix. We know that the bases in the matroid $\mathcal{M}(A)$ correspond to the sets of indices of k linearly independent columns—see Example 2.6 for the definition of $\mathcal{M}(A)$. Hence, the cyclic shift of a basis in $\mathcal{M}(A)$ is again a basis. □

Moreover, Pless [20] showed also that the incidence matrix of a Desarguesian cyclic projective plane generates a binary cyclic code. Hence, this class of cyclic matroids is a subclass of the one deriving from cyclic codes. Let $\mathcal{C}$ be a k-dimensional linear code in $\mathbb{F}_q^n$. Then, using a generator matrix G of $\mathcal{C}$, we can associate a representable matroid $\mathcal{M}_\mathcal{C} = \mathcal{M}(G)$.

Proposition 4.3. *Let $\mathcal{C}$ be an $[n, k]_q$ cyclic code with generator matrix G. Then $\mathcal{M}(G)$ is a cyclic k-matroid.*

Proof. The proof is similar to the proof of the above corollary. Observe that, since $\mathcal{C}$ is cyclic, then the matrix $\mathrm{sh}(G)$ obtained by shifting to the right every row of G is still a generator matrix for $\mathcal{C}$. In particular, the cyclic shift of each basis is still a basis. □

Remark 4.4. It is immediate to see that the cyclic property is not invariant under permutation of the coordinates. Hence, in general, it is necessary to find an appropriate relabelling of the points of the matroid, in order to obtain a cyclic one. The same property is not invariant for cyclic codes, i.e., cyclicity is not preserved under permutation of columns.

Remark 4.5. Note that in general the cyclic matroid arising from cyclic codes does not satisfy the cyclicity property defined by Welsh. Indeed, for a binary cyclic code $\mathcal{C}$ of odd length n with $n \geq 3$, it is not difficult to see that the automorphism group of $\mathcal{C}$ strictly contains $\mathbb{Z}_n$; see [3].

Example 4.6. The cyclic matroid defined in Example 3.8 is a matroid arising from the $[n, k]$ cyclic code over a field $\mathbb{F}$ with generator polynomial $1 + x^k + x^{2k} + \cdots + x^{n-k} \in \mathbb{F}[x]/\langle x^n - 1\rangle$.

Example 4.7. Consider the simplex code $[7, 3]_2$ with generator matrix

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

G is clearly the generator matrix of a cyclic code. Moreover, the matroid $\mathcal{M}(G)$ associated to it is the well known *Fano matroid*, whose name derives from the Fano plane $\mathrm{PG}(2, 2)$. This is denoted by F_7, the ground set is $E = \{0, 1, \ldots, 6\}$, the set of bases is

$$\begin{aligned} \mathcal{B} = \{&\{0,3,6\}, \{0,2,5\}, \{0,2,4\}, \{3,4,5\}, \{0,2,3\}, \{0,1,5\}, \{1,2,5\}, \\ &\{2,3,6\}, \{0,1,4\}, \{0,4,6\}, \{1,3,5\}, \{2,5,6\}, \{1,3,6\}, \{0,3,5\}, \\ &\{2,4,5\}, \{1,2,3\}, \{3,5,6\}, \{0,1,2\}, \{0,1,6\}, \{2,3,4\}, \{0,5,6\}, \\ &\{0,3,4\}, \{1,2,6\}, \{1,3,4\}, \{1,4,5\}, \{4,5,6\}, \{2,4,6\}, \{1,4,6\}\}, \end{aligned}$$

and it is not difficult to see that it satisfies the property of cyclic 3-matroids. It can be graphically represented as in Figure 4.1, where each basis is made of three points that are not collinear.

We do not know if in general the converse of Proposition 4.3 is true or not. We state this as an open problem.

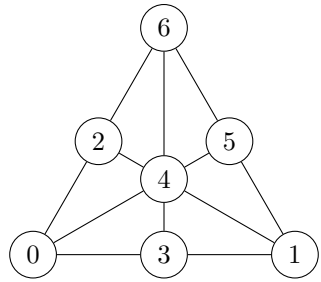


Figure 4.1: Cyclic Fano matroid F_7.

Problem 4.8. Verify the converse of Proposition 4.3: given a representable cyclic k-matroid $\mathcal{M}$ on n elements, determine if there exists a field $\mathbb{F}_q$ and an $[n,k]_q$ cyclic code $\mathcal{C}$ with $\mathcal{M}_\mathcal{C} = \mathcal{M}$.

In some cases, experimental results show that the answer to the previous open problem should be positive, as the next example illustrates.

Example 4.9. Let $n = 6$ and $k = 3$. An exhaustive computer search shows that there are exactly three cyclic matroids on the ground set $E = \{0,1,2,3,4,5\}$ having rank 3. Each of the three matroids corresponds to a cyclic code.

1. $\mathcal{M}_1$ has 8 basis elements, comprising 6 bases from the orbit of $\{0,1,2\}$ and 2 bases from the orbit of $\{0,2,4\}$.

   For $\mathcal{C}_1 = \langle x^3+1\rangle \subseteq \mathbb{F}_2[x]/\langle x^6-1\rangle$, we get $\mathcal{M}_1 = \mathcal{M}_{\mathcal{C}_1}$.

2. $\mathcal{M}_2$ has 18 basis elements, comprising 6 bases from the orbit of $\{0,1,2\}$, 6 bases from the orbit of $\{0,1,3\}$, and 6 bases from the orbit of $\{0,1,4\}$.

   For $\mathcal{C}_2 = \langle x^3+2x^2+2x+1\rangle \subseteq \mathbb{F}_3[x]/\langle x^6-1\rangle$, we get $\mathcal{M}_2 = \mathcal{M}_{\mathcal{C}_2}$.

3. $\mathcal{M}_3$ with 20 basis elements, comprising all the 20 subsets of size 3.

   For $\mathcal{C}_3 = \langle x^3+2x^2+2x+1\rangle \subseteq \mathbb{F}_5[x]/\langle x^6-1\rangle$, we get $\mathcal{M}_3 = \mathcal{M}_{\mathcal{C}_3}$.

4.2 k-normal elements

In this section we establish a connection between $(n-k)$-normal elements and cyclic k-matroids. The connection between matroids and k-normal elements has never been observed before, to the best of our knowledge.

Given an $(n-k)$-normal element $\alpha \in \mathbb{F}_{q^n}$, let

$$V \coloneqq \operatorname{span}_{\mathbb{F}_q} \left\{ \alpha, \alpha^q, \ldots, \alpha^{q^{n-1}} \right\}$$

be the k-dimensional span over $\mathbb{F}_q$ of the conjugates of α. We may associate a matroid $\mathcal{M} = (\mathbb{Z}_n, \mathcal{B})$ on n symbols to α as follows. Let $\mathcal{I}$ be a collection of subsets of $\mathbb{Z}_n$ such that $S \in \mathcal{I}$ if and only if the set of powers $\left\{ \alpha^{q^i} \mid i \in S \right\}$ is linearly independent over $\mathbb{F}_q$. Then $\mathcal{I}$ clearly satisfy axioms (I1)–(I3); hence, it is the collection of independent sets of a matroid. In particular, the collection of bases of such a matroid is defined as

$$\mathcal{B} = \Big\{ \{i_1, \ldots, i_k\} \subseteq \mathbb{Z}_n \mid \{\alpha^{q^{i_1}}, \alpha^{q^{i_2}}, \ldots, \alpha^{q^{i_k}}\} \text{ is a linear basis of } V \text{ as a vector space over } \mathbb{F}_q \Big\}.$$

Proposition 4.10. *The matroid $\mathcal{M} = (\mathbb{Z}_n, \mathcal{B})$ associated to an $(n-k)$-normal element $\alpha \in \mathbb{F}_q^n$ is a cyclic k-matroid.*

Proof. Since the first k powers of α must be linearly independent in order for all of them to span a k-dimensional vector space, we must have $\{0, 1, \ldots, k-1\} \in \mathcal{B}$. Further, for any $s \in \mathbb{Z}_n$, $\left\{ \alpha^{q^{i_1}}, \alpha^{q^{i_2}}, \ldots, \alpha^{q^{i_k}} \right\}$ is linearly independent if and only if $\left\{ \alpha^{q^{i_1+s}}, \alpha^{q^{i_2+s}}, \ldots, \alpha^{q^{i_k+s}} \right\}$ is linearly independent, by the properties of the Frobenius automorphism. Thus, $\mathcal{M}$ is a cyclic k-matroid. □

In [26], it was left as an open problem to determine which subsets of

$$\left\{ \alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}} \right\}$$

of size k or smaller, apart from $\left\{ \alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{k-1}} \right\}$, are linearly independent, for an $(n-k)$-normal element α of $\mathbb{F}_{q^n}$. Clearly, the results of Section 3.1 give lower bounds on the number of k-subsets of $\left\{ \alpha, \alpha^q, \ldots, \alpha^{q^{n-1}} \right\}$ (where α is $(n-k)$-normal), which form bases over $\mathbb{F}_q$, or equivalently upper bounds on the number of dependent k-subsets.

We assert that our association of k-normal elements with matroids strongly suggests that a complete and general solution to the mentioned problem may be very difficult to arrive at.

We further state the following open problem, whose solution we conjecture is positive based on multiple computer experiments and observations.

Problem 4.11. Given a representable cyclic k-matroid $\mathcal{M} = (\mathbb{Z}_n, \mathcal{B})$, determine if there exists a prime power q and an $(n-k)$-normal element $\alpha \in \mathbb{F}_{q^n}$ such that all the bases of the $\mathbb{F}_q$-span of α, a^q, ..., $\alpha^{q^{n-1}}$ are given by the sets $\{\alpha^{q^{i_1}}, \alpha^{q^{i_2}}, \ldots, \alpha^{q^{i_k}}\}$ where $\{i_1, i_2, \ldots, i_k\} \in \mathcal{B}$.

Acknowledgments

The work of Gianira N. Alfarano was supported by the Swiss National Science Foundation under grant no. 188430 and 210966 and by the FWO (Research Foundation Flanders) grant no. 1273624N. The work of Simran Tinani was supported by armasuisse Science and Technology. The work of Karan Khathuria was supported by the Estonian Research Council grant PRG49.

References

[1] N. Alon, Y. Caro, I. Krasikov, and Y. Roditty, Combinatorial reconstruction problems, *J. Combin. Theory Ser. B* **47**(2) (1989), 153–161.

[2] G. Berman, Finite projective plane geometries and difference sets, *Trans. Amer. Math. Soc.* **74**(3) (1953), 492–499.

[3] R. Bienert and B. Klopsch, Automorphism groups of cyclic codes, *J. Algebraic Combin.* **31**(1) (2010), 33–52.

[4] C. J. Colbourn, J. S. Provan, and D. Vertigan, The complexity of computing the Tutte polynomial on transversal matroids, *Combinatorica* **15**(1) (1995), 1–10.

[5] E. Ehrhart, Sur les polyèdres rationnels homothétiques à n dimensions, *CR Acad. Sci. Paris* **254** (1962), 616 pp.

[6] O. Giménez, A. De Mier, and M. Noy, On the number of bases of bicircular matroids, *Ann. Comb.* **9**(1) (2005), 35–45.

[7] O. Giménez and M. Noy, On the complexity of computing the Tutte polynomial of bicircular matroids, *Combin. Probab. Comput.* **15**(3) (2006), 385–395.

[8] R. Graham and J. MacWilliams, On the number of information symbols in difference-set cyclic codes, *Bell System Tech. J.* **45**(7) (1966), 1057–1070.

[9] C. Greene, A multiple exchange property for bases, *Proc. Amer. Math. Soc.* **39**(1) (1973), 45–50.

[10] C. Greene, Weight enumeration and the geometry of linear codes, *Studies in Appl. Math.* **55**(2) (1976), 119–128.

[11] H. Guo and M. Jerrum, Approximately counting bases of bicircular matroids, *Combin. Probab. Comput.* **30**(1) (2021), 124–135.

[12] M. Hall, Jr., Cyclic projective planes, *Duke Math. J.* **14**(4) (1947), 1079–1090.

[13] J. Hirschfeld, *Projective geometries over finite fields. Oxford mathematical monographs*, Oxford University Press New York, 1998.

[14] S. Huczynska, G. L. Mullen, D. Panario, and D. Thomson, Existence and properties of k-normal elements over finite fields, *Finite Fields Appl.* **24** (2013), 170–183.

[15] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2010.

[16] L. C. Lomelí and D. Welsh, Randomized approximation of the number of bases, *Contemp. Math.* **197** (1996), 371–376.

[17] V. B. Mnukhin, The k-orbit reconstruction and the orbit algebra, *Acta Appl. Math.* **29(1-2)** (1992), 83–117.

[18] J. G. Oxley, *Matroid theory*, Oxford University Press, USA, 2006.

[19] R. Pendavingh and J. Van Der Pol, On the number of bases of almost all matroids, *Combinatorica* **38**(4) (2018), 955–985.

[20] V. Pless, Cyclic projective planes and binary, extended cyclic self-dual codes, *J. Combin. Theory Ser. B* **43**(2) (1986), 331–333.

[21] A. J. Radcliffe and A. D. Scott, Reconstructing under group actions, *Graphs Combin.* **22**(3) (2006), 399–419.

[22] L. Reis, Existence results on k-normal elements over finite fields, *Rev. Mat. Iberoamericana* **35**(3) (2019), 805–822.

[23] L. A. Rosati, Piani proiettivi desarguesiani non ciclici., *Boll. Unione Mat. Ital.* **12**(2) (1957), 230–240.

[24] J. Simon, The combinatorial k-deck, *Graphs Combin.* **34**(6) (2018), 1597–1618.

[25] M. Snook, Counting bases of representable matroids, *Electron. J. Combin.* (2012), p. 41.

[26] S. Tinani and J. Rosenthal, Existence and cardinality of k-normal elements in finite fields, in *Arithmetic of Finite Fields. 8th International Workshop, WAIFI 2020, Rennes, France*, Theoretical Computer Science and General Issues, Springer International Publishing, (2021), `https://doi.org/10.1007/978-3-030-68869-1`.

[27] J. H. Van Lint, *Introduction to coding theory*, Graduate Texts in Mathematics, Springer, Berlin, Heidelberg, 1999.

[28] D. J. Welsh, *Matroid theory*, Dover books on mathematics, Dover Publications Inc., 2010.

Gianira N. Alfarano
University College Dublin, Ireland
Vrije Universiteit Brussel, Belgium
gianira.alfarano@gmail.com

Karan Khathuria
University of Tartu, Estonia
Quantinuum, Partnership House,
Carlisle place, London, SW1P 1BX, United Kingdom
khathuria.karan@gmail.com

Simran Tinani
University of Zurich, Switzerland and
cnlab security AG, Switzerland
simran.tinani@gmail.com

A Explicit cyclic k-matroids

Computer search was used to find examples of cyclic k-matroids different from the uniform matroid. Due to the randomized nature of the algorithm used when $\gcd(n,k) = 1$, the matroids obtained were all quite close to the uniform matroid, usually missing one or two cyclic orbits. We list the orbit representatives of the basis set for a few select cases. Thus, the bases sets of matroids represented by the below examples are obtained by taking all the cyclic shifts of these orbit representatives. Using the orbits, we also formally compute the exact number of bases when $\gcd(n,k) = 1$ and a lower bound when $\gcd(n,k) \neq 1$, exploiting the fact that the size of each orbit is at least $n/\gcd(n,k)$. We compare this number to the number of bases in the uniform matroid, i.e., $\binom{n}{k}$. Note that, for given n and k, the listed matroid need not be the only non-uniform cyclic matroid. The working code for the generation algorithm, as well as for the bound calculations in Section 3.3, can be found at `https://github.com/simran-tinani/Cyclic-matroids`.

n	k	Basis Orbit Representatives	Bases	Bases (UM)
6	3	$\{0,1,2\}$, $\{0,2,4\}$	8	20
6	4	$\{0,1,2,4\}$, $\{0,1,2,3\}$	12	15
7	3	$\{0,1,4\}$, $\{0,1,2\}$, $\{1,3,6\}$, $\{1,5,6\}$	28	35
9	3	$\{2,5,7\}$, $\{0,1,2\}$, $\{0,3,8\}$, $\{1,7,8\}$, $\{1,4,5\}$, $\{0,6,8\}$, $\{0,5,7\}$, $\{2,4,7\}$, $\{1,5,6\}$	$\geq$27	84
9	4	$\{3,4,6,8\}$, $\{1,3,4,5\}$, $\{0,3,5,6\}$, $\{0,5,6,8\}$, $\{1,2,3,6\}$, $\{0,1,2,6\}$ $\{0,2,5,8\}$, $\{0,1,2,3\}$, $\{2,3,6,7\}$, $\{2,4,6,7\}$, $\{0,3,5,7\}$, $\{3,4,5,7\}$, $\{1,5,7,8\}$	117	126
10	6	$\{0,1,2,4,7,9\}$, $\{2,3,6,7,8,9\}$, $\{1,2,3,5,6,7\}$, $\{0,1,2,4,8,9\}$, $\{1,3,4,5,6,9\}$, $\{0,1,3,4,6,8\}$, $\{2,3,4,7,8,9\}$, $\{2,3,4,6,7,9\}$, $\{1,2,3,4,5,8\}$, $\{0,2,3,6,7,8\}$, $\{0,2,5,6,8,9\}$, $\{1,2,4,5,6,7\}$, $\{2,3,4,5,7,8\}$, $\{0,1,2,3,4,5\}$, $\{0,1,3,5,8,9\}$, $\{0,1,2,3,7,9\}$, $\{1,3,4,6,8,9\}$, $\{0,1,3,5,6,7\}$, $\{1,2,3,6,8,9\}$, $\{1,2,3,5,6,9\}$, $\{0,2,3,6,7,9\}$, $\{0,1,2,4,6,8\}$	$\geq$110	210

n	k	Basis Orbit Representatives	Bases	Bases (UM)
11	4	$\{0,3,5,10\}$, $\{3,5,7,8\}$, $\{0,1,5,9\}$, $\{1,4,6,9\}$, $\{2,6,9,10\}$, $\{1,6,7,9\}$, $\{0,5,8,9\}$, $\{0,5,7,10\}$, $\{0,3,4,8\}$, $\{0,2,8,9\}$, $\{5,6,7,10\}$, $\{3,5,7,10\}$, $\{0,4,5,9\}$, $\{2,6,7,9\}$, $\{0,1,2,9\}$, $\{1,3,8,10\}$, $\{0,4,5,6\}$, $\{2,3,8,9\}$, $\{0,1,2,6\}$, $\{1,2,7,10\}$, $\{0,1,2,3\}$, $\{2,3,6,9\}$, $\{2,3,6,7\}$, $\{0,2,3,10\}$, $\{2,4,5,8\}$, $\{0,1,3,9\}$, $\{1,2,3,9\}$, $\{0,1,2,4\}$, $\{2,4,8,10\}$	319	330
13	3	$\{3,4,7\}$, $\{0,1,2\}$, $\{4,11,12\}$, $\{0,4,12\}$, $\{7,10,12\}$, $\{0,6,12\}$ $\{3,7,9\}$, $\{4,8,11\}$, $\{2,3,10\}$, $\{5,7,8\}$, $\{0,7,9\}$, $\{6,8,11\}$ $\{0,6,8\}$, $\{3,7,12\}$, $\{2,5,6\}$, $\{4,6,12\}$, $\{7,8,10\}$, $\{7,9,11\}$ $\{1,6,11\}$, $\{1,5,6\}$, $\{1,8,11\}$	273	286
15	3	$\{0,1,2\}$, $\{3,12,13\}$, $\{0,4,12\}$, $\{5,13,14\}$, $\{9,10,13\}$, $\{7,10,13\}$, $\{3,7,9\}$, $\{4,8,11\}$, $\{6,11,14\}$, $\{1,5,12\}$, $\{4,9,10\}$, $\{3,5,13\}$, $\{0,2,7\}$, $\{5,6,14\}$, $\{2,3,10\}$, $\{5,7,8\}$, $\{0,7,9\}$, $\{6,8,11\}$, $\{0,1,12\}$, $\{2,6,12\}$, $\{0,6,8\}$ $\{3,9,12\}$, $\{7,9,11\}$, $\{3,13,14\}$, $\{7,8,10\}$, $\{2,11,13\}$, $\{2,4,14\}$, $\{1,6,11\}$, $\{1,5,6\}$, $\{1,8,11\}$	$\geq$150	455