Freij-Hollanti, Ragnar; Grezet, Matthias; Hollanti, Camilla; Westerbäck, Thomas

Cyclic flats of binary matroids

Published in:
Advances in Applied Mathematics

DOI:
10.1016/j.aam.2021.102165

Published: 01/06/2021

Document Version
Publisher's PDF, also known as Version of record

Advances in Applied Mathematics 127 (2021) 102165

Contents lists available at ScienceDirect

Advances in Applied Mathematics

www.elsevier.com/locate/yaama

Cyclic flats of binary matroids

Ragnar Freij-Hollanti [a,*], Matthias Grezet [a], Camilla Hollanti [a], Thomas Westerbäck [b]

[a] *Department of Mathematics and Systems Analysis, Aalto University, FI-00076 Aalto, Finland*
[b] *Division of Applied Mathematics, UKK, Mälardalen University, Högskoleplan 1, Box 883, 721 23 Västerås, Sweden*

ARTICLE INFO

Article history:
Received 8 November 2019
Received in revised form 30 December 2020
Accepted 16 January 2021
Available online 28 January 2021

MSC:
05B35

Keywords:
Cyclic flats
Binary matroids
Atomic lattices

ABSTRACT

In this paper, first steps are taken towards characterizing rank-decorated lattices of cyclic flats $\mathcal{Z}(M)$ that belong to matroids M that can be represented over a prescribed finite field $\mathbb{F}_q$. Two natural maps from $\mathcal{Z}(M)$ to the lattice of cyclic flats of a minor of M are given. Binary matroids are characterized via their lattice of cyclic flats. It is shown that the lattice of cyclic flats of a simple binary matroid without isthmuses is atomic.

1. Introduction

In traditional matroid theory, one of the most crucial objects is that of a lattice of flats. This is a geometric lattice, *i.e.*, it is atomic and semimodular, and in fact every geometric lattice is the lattice of flats $\mathcal{F}(M)$ of a simple matroid $M = (E, \rho)$ [2]. This

* Corresponding author.
E-mail addresses: ragnar.freij@aalto.fi (R. Freij-Hollanti), matthias.grezet@aalto.fi (M. Grezet), camilla.hollanti@aalto.fi (C. Hollanti), thomas.westerback@mdh.se (T. Westerbäck).

https://doi.org/10.1016/j.aam.2021.102165

correspondence between lattices and matroids behaves reasonably well with respect to their respective notions of duality, namely, the dual lattice of $\mathcal{F}(M)$ is isomorphic to the lattice of cyclic sets $\mathcal{U}(M^*)$, whose elements are unions of circuits in the dual M^*.

Thus, the Boolean lattice 2^E has two subposets $\mathcal{F}(M)$ and $\mathcal{U}(M)$, both of which are lattices, each of which determine the matroid M uniquely. This has inspired many authors to look at their intersection $\mathcal{Z}(M) = \mathcal{F}(M) \cap \mathcal{U}(M)$ [19,3,14,5]. It was shown independently in [19,3] that $\mathcal{Z}(M)$ together with the restriction of the rank function ρ to $\mathcal{Z}(M)$ is enough to determine M. Moreover, $\mathcal{Z}(M)$ is a lattice, although its lattice structure is neither induced by 2^E, $\mathcal{F}(M)$, or $\mathcal{U}(M)$ [19,3].

As opposed to $\mathcal{F}(M)$ and $\mathcal{U}(M)$, the lattice of cyclic flats has no additional structure apart from being a lattice. Indeed, it is shown in [3] that every finite lattice is isomorphic to the lattice of cyclic flats of some finite matroid. Yet, there are many advantages in describing a matroid in terms of its lattice of cyclic flats. Firstly, the cyclic flats description is rather concise for many naturally occurring matroids. Secondly, it was shown in [23] that many central invariants in coding theory can be naturally described in terms of the lattice of cyclic flats of the associated matroid. Especially, this was shown to be the case for invariants related to applications to distributed data storage [23]. It was earlier shown in [5] that the Tutte polynomial can be computed efficiently for matroids whose lattice of cyclic flats has bounded height. Yet another reason to take interest in the lattices of cyclic flats is that some natural classes of matroids can be defined in terms of the structure of $\mathcal{Z}(M)$. For instance, a matroid M is nested if and only if $\mathcal{Z}(M)$ is a chain. The nested matroids form the first known example of a minor-closed class of matroids that is well-quasi-ordered under the minor relation, but has infinitely many forbidden minors.

In this work, we are taking first steps towards characterizing lattices of cyclic flats that belong to matroids that can be represented over a prescribed finite field $\mathbb{F}_q$. Our approach is to study the minor relation from the point of view of cyclic flats. In particular, in Theorem 6 we construct two natural maps from $\mathcal{Z}(M)$ to the lattice of cyclic flats of a minor of M.

We take inspiration from Rota's conjecture [15], and its recently announced proof [6], that representability over a prescribed finite field $\mathbb{F}_q$ is equivalent to avoiding a finite set $L(\mathbb{F}_q)$ of minors. However, in this initial work we only actually use the rather weak result that if $n > q+1$, and the uniform matroid U_n^2 is a minor of M, then M is not representable over $\mathbb{F}_q$ [12]. Thus, in Theorem 11, we compute the largest n for which U_n^2 is a minor of M, from $\mathcal{Z}(M)$. This is done via studying a certain antichain of flats associated to every cyclic flat of rank $\rho(1_{\mathcal{Z}(M)}) - 2$. By duality, of course, this can also be used to find the largest n for which U_n^{n-2} is a minor of M.

The representability over $\mathbb{F}_2$, or other small fields of characteristic 2, is particularly interesting from a data storage point of view. For instance, small fields allow an efficient implementation of locally repairable codes [13]. Constructions of optimal locally repairable codes over $\mathbb{F}_2$ were also derived in [18,9]. Therefore, it motivates a deeper understanding of the dependency structures of binary matroids.

Since binary matroids are exactly characterized by not having U_4^2 as a minor, we thus get two equivalent necessary and sufficient conditions for a matroid to be representable over $\mathbb{F}_2$ in Corollary 7. In the second half of the paper, we focus exclusively on binary matroids. In Sections 7 and 8, we study sublattices of $\mathcal{Z}(M)$ of height 2 and 3 respectively, when M is binary. We also prove, in Theorem 13, that the lattice of cyclic flats of a simple matroid with no isthmuses is atomic.

Understanding the sublattices of small height helps us describe constraints on $\mathcal{Z}(M)$ recursively in Section 9, and these recursive constraints are enough to reprove the Griesmer bound for binary codes [10]. On our way to proving the Griesmer bound, we define the class of *blunt* cyclic flats of a binary matroid. These play a special role in our analysis and seem relevant also in a much broader context, although it is not clear how to generalize the definition to non-binary matroids.

Part of this work has previously been presented at the 5th International Castle Meeting on Coding Theory and Applications [7] and at the International Zurich Seminar on Information and Communication [8].

2. Preliminaries

Matroids have many equivalent definitions in the literature. Here, we choose to present matroids via their rank functions.

Definition 1. A *(finite) matroid* $M = (E, \rho)$ is a finite set E together with a *rank function* $\rho : 2^E \to \mathbb{Z}$ such that for all subsets $X, Y \subseteq E$

(R1) $0 \leq \rho(X) \leq |X|$,
(R2) If $X \subseteq Y$ then $\rho(X) \leq \rho(Y)$,
(R3) $\rho(X) + \rho(Y) \geq \rho(X \cup Y) + \rho(X \cap Y)$.

When $M = (E, \rho)$ is a matroid, we also define the *nullity function* $\eta : 2^E \to \mathbb{Z}$ by $\eta(X) = |X| - \rho(X)$.

Any matrix G over a field $\mathbb{F}$ generates a matroid $M_G = (E, \rho)$, where E is the set of columns of G, and $\rho(X)$ is the rank of $G(X)$ over $\mathbb{F}$, where $G(X)$ denotes the submatrix of G formed by the columns indexed by X. Clearly, ρ only depends on the row space of G, so row-equivalent matrices generate the same matroid.

Two matroids $M_1 = (E_1, \rho_1)$ and $M_2 = (E_2, \rho_2)$ are *isomorphic* if there exists a bijection $\psi : E_1 \to E_2$ such that $\rho_2(\psi(X)) = \rho_1(X)$ for all subsets $X \subseteq E_1$.

Definition 2. A matroid that is isomorphic to M_G for some matrix G over $\mathbb{F}$ is said to be *representable* over $\mathbb{F}$. A *binary* matroid is a matroid that is representable over $\mathbb{F}_2$.

Definition 3. For integers $0 \leq k \leq n$, the *uniform matroid* $U_n^k = ([n], \rho)$ is a matroid with a ground set $[n] = \{1, 2, \ldots, n\}$ and a rank function $\rho(X) = \min\{|X|, k\}$ for $X \subseteq [n]$.

Motivated by coding theory and the relation between linear codes and matroids, we define the minimum distance of a matroid to be the following.

Definition 4. Let $M = (E, \rho)$ be a matroid. The minimum distance of M is

$$d = \min\{|X| : X \subseteq E, \rho(E - X) < \rho(E)\}.$$

A matroid with $|E| = n$, $\rho(E) = k$, and minimum distance d is referred to as an (n, k, d)-matroid.

Therefore, if the matroid $M_{\mathcal{C}}$ comes from a linear code $\mathcal{C}$, then the minimum distance of $M_{\mathcal{C}}$ coincides with the minimum Hamming distance.

Definition 5. Let $M = (E, \rho)$ be a matroid and $X, Y \subseteq E$, and denote by $\bar{X} = E - X$ for any $X \subseteq E$. Then

(i) The *restriction* of M to Y is the matroid $M|Y = (Y, \rho_{|Y})$, where $\rho_{|Y}(A) = \rho(A)$ for $A \subseteq Y$. The restriction operation to Y is also referred to as *deletion* of the set $E - Y$.
(ii) The *contraction* of M by X is the matroid $M/X = (\bar{X}, \rho_{/X})$, where $\rho_{/X}(A) = \rho(A \cup X) - \rho(X)$ for $A \subseteq \bar{X}$.
(iii) For $X \subseteq Y$, a *minor* of M is a matroid isomorphic to $M|Y/X = (Y - X, \rho_{|Y/X})$, obtained from M by restriction to a set $Y \subseteq E$ and contraction by $X \subseteq Y$. Observe that this does not depend on the order in which the restriction and contraction are performed.
(iv) The *dual* of M is the matroid $M^* = (E, \rho^*)$, where

$$\rho^*(A) = |A| + \rho(\bar{A}) - \rho(E) = \eta(E) - \eta(\bar{A}) \text{ for } A \subseteq E.$$

We recall the following standard identity connecting the notions of duality and minors.

Proposition 1. *Let $M = (E, \rho)$ and $X \subseteq Y \subseteq E$. Then $(M|Y/X)^* = M^*|\bar{X}/\bar{Y}$.*

It is well known and not difficult to prove that representability over $\mathbb{F}_q$ is preserved under minors and duals [12]. Given the structure of uniform matroids and the definition of a minor, the minors of uniform matroids are very easily described:

Lemma 1. *Let $U_n^k = ([n], \rho)$ be a uniform matroid, and let $X \subseteq Y \subseteq E$. Then the minor $U_n^k|Y/X$ is isomorphic to $U_{n'}^{k'}$, where $n' = |Y| - |X|$ and*

$$k' = \begin{cases} 0 & \text{if } |X| > k \\ n' & \text{if } |Y| < k \\ k - |X| & \text{otherwise.} \end{cases}$$

In particular, M is a minor of U_n^k if and only if $M \cong U_{n'}^{k'}$, for some $0 \leq k' \leq k$ and $0 \leq n' - k' \leq n - k$.

In general there is no simple criterion to determine if a matroid is representable [22,11]. However, there is a simple criterion for when a matroid is binary.

Theorem 1 *([21]). Let $M = (E, \rho)$ be a matroid. The following two conditions are equivalent.*

1. *M is representable over $\mathbb{F}_2$.*
2. *There are no sets $X \subseteq Y \subseteq E$ such that $M|Y/X$ is isomorphic to the uniform matroid U_4^2.*

If M is representable over a fixed finite field $\mathbb{F}_q$, then so are all its minors. The class of matroids representable over $\mathbb{F}_q$ is therefore closed under minors. The following result, which extend the previous theorem, was first conjectured by Gian-Carlo Rota in 1970 [15]. A proof of this conjecture was announced by Geelen, Gerards, and Whittle in 2014, but the details of the proof remain to be written up [6].

Theorem 2 *([6]). For any finite field $\mathbb{F}_q$, there is a finite set $L(\mathbb{F}_q)$ of matroids such that any matroid M is representable over $\mathbb{F}_q$ if and only if it contains no element from $L(\mathbb{F}_q)$ as a minor.*

Since the 1970's, it has been known that a matroid is representable over $\mathbb{F}_3$ if and only if it avoids the uniform matroids U_5^2, U_5^3, the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$, and its dual $\mathbb{P}^2(\mathbb{F}_2)^*$ as minors. The list $L(\mathbb{F}_4)$ was given explicitly in 2000 and contains seven elements. For larger fields, the explicit list is not known, and there is little hope to even find useful bounds on its size. Assuming the MDS conjecture [16], a matroid M that is linearly representable over $\mathbb{F}_q$ must avoid U_{q+2}^k as a minor, for $k = 2$, $4 \leq k \leq q-2$, and $k = q$. If q is odd, M must also avoid U_{q+2}^3 and U_{q+2}^{q-1} minors. The MDS conjecture is widely believed to be true, and is proven when q is prime [1].

The following theorem by Higgs is known as the *Scum Theorem*, and will be of importance later in this paper. It significantly restricts the sets $A \subseteq B \subseteq E$ that one must consider in order to find all minors of M as $M|B/A$.

Theorem 3 *(Proposition 3.3.7 in [4]). Let $N = (E_N, \rho_N)$ be a minor of a matroid $M(E_M, \rho_M)$. Then there is a pair of sets $A \subseteq B \subseteq E_M$ with $\rho_M(A) = \rho_M(E_M) - \rho_N(E_N)$ and $\rho_M(B) = \rho_M(E_M)$, such that $M|B/A \cong N$. Further, if N has no loops, then A can be chosen to be a flat of M.*

2.1. Fundamentals on cyclic flats

Before we define and give the properties of the cyclic flats, we need a minimal background on posets and lattices. We refer the reader to [20] for further information about these objects.

A *partially ordered set* P (or *poset*, for short) is a set together with a partial order $\leq$. For $x, y \in P$, we say that y *covers* x or x is *covered* by y, denoted by $x \lessdot y$, if $x \leq y$, $x \neq y$, and there is no $z \in P$ different from x and y such that $x \leq z \leq y$. An *upper bound* of x and y is an element $u \in P$ satisfying $x \leq u$ and $y \leq u$. The *join* of x and y, denoted by $x \vee y$ if it exists, is the least upper bound. Dually, the *meet* $x \wedge y$ is the greatest lower bound. If P has an element 0_P such that $0_P \leq x$ for all $x \in P$, then 0_P is called the *bottom element* of P. Similarly, if P has an element 1_P such that $x \leq 1_P$ for all $x \in P$, then 1_P is called the *top element* of P.

A *lattice* is a poset L for which every pair of elements has a meet and join. It is not difficult to see that every finite lattice has a bottom element and top element. If L is a lattice and $x \in L$, then x is an *atom* of L if x covers 0_L. A lattice L is said to be *atomic* if every element of L is the join of atoms. Dually, $x \in L$ is a *coatom* if $x \lessdot 1_L$ and L is *coatomic* if every element of L is the meet of coatoms.

The main tools from matroid theory in this paper are the cyclic flats. We will define them using the closure and cyclic operator.

Let $M = (E, \rho)$ be a matroid. The *closure* operator $\mathrm{cl} : 2^E \to 2^E$ and *cyclic* operator $\mathrm{cyc} : 2^E \to 2^E$ are defined by

$$\mathrm{cl}(X) = \{e \in E : \rho(X \cup e) = \rho(X)\},$$
$$\mathrm{cyc}(X) = \{e \in X : \rho(X - e) = \rho(X)\}.$$

A subset $X \subseteq E$ is a *flat* if $\mathrm{cl}(X) = X$ and a *cyclic set* if $\mathrm{cyc}(X) = X$. Therefore, X is a *cyclic flat* if

$$\rho(X \cup y) > \rho(X) \quad \text{and} \quad \rho(X - x) = \rho(X)$$

for all $y \in E - X$ and $x \in X$. The collection of flats, cyclic sets, and cyclic flats of M are denoted by $\mathcal{F}(M)$, $\mathcal{U}(M)$, and $\mathcal{Z}(M)$, respectively. If the matroid is clear from context, we may suppress it from the notation and write $\mathcal{F}$, $\mathcal{U}$, and $\mathcal{Z}$, respectively.

It is easy to verify, as in [3], that the closure operator induces flatness and preserves cyclicity, and that the cyclic operator induces cyclicity and preserves flatness. Thus we can write

$$\mathrm{cl} : \begin{cases} 2^E \to \mathcal{F}(M) \\ \mathcal{U}(M) \to \mathcal{Z}(M), \end{cases} \quad \text{and} \quad \mathrm{cyc} : \begin{cases} 2^E \to \mathcal{U}(M) \\ \mathcal{F}(M) \to \mathcal{Z}(M). \end{cases} \tag{1}$$

In particular, for any set $X \subseteq E$, we have $\mathrm{cyc}(\mathrm{cl}(X)) \in \mathcal{Z}(M)$ and $\mathrm{cl}(\mathrm{cyc}(X)) \in \mathcal{Z}(M)$. Moreover, the closure and cyclic operators are order preserving in that $X \subseteq Y$ implies

$\mathrm{cyc}(X) \subseteq \mathrm{cyc}(Y)$ and $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$, so the maps in (1) can be considered as order-preserving poset maps. The following duality properties of flats, cyclic sets, and cyclic flats are easy to verify.

Proposition 2. *Let $M = (E, \rho)$ be a matroid and $X, Y \subseteq E$.*

(i) $\mathcal{F}(M) = \{E - X : X \in \mathcal{U}(M^*)\}$.
(ii) $\mathcal{U}(M) = \{E - X : X \in \mathcal{F}(M^*)\}$.
(iii) $\mathcal{Z}(M) = \{E - X : X \in \mathcal{Z}(M^*)\}$.

Three basic properties of cyclic flats of a matroid are given in the following proposition.

Proposition 3 *([3]). Let $M = (E, \rho)$ be a matroid and $\mathcal{Z}$ the collection of cyclic flats of M. Then,*

(i) $\rho(X) = \min\{\rho(F) + |X \setminus F| : F \in \mathcal{Z}\}$, *for* $X \subseteq E$,
(ii) $(\mathcal{Z}, \subseteq)$ *is a lattice with* $X \vee Y = \mathrm{cl}(X \cup Y)$ *and* $X \wedge Y = \mathrm{cyc}(X \cap Y)$ *for* $X, Y \in \mathcal{Z}$,
(iii) $1_{\mathcal{Z}} = \mathrm{cyc}(E)$ *and* $0_{\mathcal{Z}} = \mathrm{cl}(\emptyset)$.

That E together with the cyclic flats and their ranks together defines the matroid $M = (E, \rho)$ uniquely can be concluded from (i) in the proposition above. It is thus natural to cryptomorphically define matroids via an axiom scheme for their cyclic flats, as was done independently in [3] and [19]. This gives a compact way to represent and construct matroids.

Theorem 4 *([3] Th. 3.2 and [19]). Let $\mathcal{Z} \subseteq 2^E$ and let ρ be a function $\rho : \mathcal{Z} \to \mathbb{Z}$. There is a matroid M on E for which $\mathcal{Z}$ is the set of cyclic flats and ρ is the rank function restricted to the sets in $\mathcal{Z}$, if and only if*

(Z0) $\mathcal{Z}$ *is a lattice under inclusion.*
(Z1) $\rho(0_{\mathcal{Z}}) = 0$.
(Z2) If $X, Y \in \mathcal{Z}$ *and* $X \subsetneq Y$, *then* $0 < \rho(Y) - \rho(X) < |Y| - |X|$.
(Z3) $\rho(X) + \rho(Y) \geq \rho(X \vee Y) + \rho(X \wedge Y) + |(X \cap Y) - (X \wedge Y)|$ *for all* $X, Y \in \mathcal{Z}$.

Definition 6. A matroid is *non-degenerate* if it does not have any loops or isthmuses. A matroid which has a loop or isthmus is *degenerate*.

For any matroid $M = (E, \rho)$, we observe that

$$0_{\mathcal{Z}} = \mathrm{cl}(\emptyset) = \{e \in E : \rho(e) = 0\} \text{ and } 1_{\mathcal{Z}} = \mathrm{cyc}(E) = \{e \in E : \rho(E - e) = \rho(E)\}.$$

Hence, $0_{\mathcal{Z}}$ and $E - 1_{\mathcal{Z}}$ are equal to the collection of loops and isthmuses, respectively. Consequently, we obtain the following lemma which gives a characterization of non-degenerate matroids via cyclic flats.

Lemma 2. *A matroid is non-degenerate if and only if* $0_{\mathcal{Z}} = \emptyset$ *and* $1_{\mathcal{Z}} = E$.

As an immediate consequence of the definition of cyclic flats, we have the following characterization of uniform matroids by their cyclic flats.

Proposition 4. *Let* $M = (E, \rho)$ *be a matroid and let* $0 < k < n$ *be positive integers. The following are equivalent:*

(i) M *is the uniform matroid* U_n^k
(ii) $\mathcal{Z} = \mathcal{Z}(M)$ *is the two element lattice with bottom element* $0_{\mathcal{Z}} = \emptyset$*, top element* $1_{\mathcal{Z}} = E$ *and* $\rho(1_{\mathcal{Z}}) = k$

Finally, it was proven in [23] that the cyclic flats determine the minimum distance of a matroid without isthmuses.

Proposition 5 *([23]). Let* $M = (E, \rho)$ *be a matroid without isthmuses. Then the minimum distance* d *satisfies*

$$d = \eta(E) + 1 - \max\{\eta(Z) : Z \in \mathcal{Z}(M) - E\}.$$

3. Cyclic flats of minors

In order to identify uniform minors of the matroid M, we will take the detour of identifying the cyclic flats of an arbitrary minor $M_{[A,B]}$. We will then use the fact that the minor in question is uniform if and only if $\mathcal{Z}(M_{[A,B]}) = \{\emptyset, B-A\}$, as in Proposition 4. Our first interest is in the case when X and Y are themselves cyclic flats. In this case we have a straightforward characterization of cyclic flats in $M|Y/X$, via the following two lemmas:

Lemma 3. *Let* M *be a matroid, and let* $X \subseteq Y \subseteq E(M)$ *be two sets with* $Y \in \mathcal{F}(M)$*. Then* $\mathcal{F}(M|Y/X) = \{F \subseteq Y - X, F \cup X \in \mathcal{F}(M)\}$.

Proof. A set S is a flat in $M|Y/X$ precisely if $\rho(S \cup X \cup i) > \rho(S \cup X)$ for all $i \in (Y - X) - S$. Since Y is a flat, the inequality $\rho(S \cup X \cup i) > \rho(S \cup X)$ will hold for all $i \in \bar{Y}$ regardless of S. Thus, S is flat in $M|Y/X$ if and only if $S \cup X$ is flat in M. □

Lemma 4. *Let* M *be a matroid, and let* $X \subseteq Y \subseteq E(M)$ *be two sets with* $X \in \mathcal{U}(M)$*. Then* $\mathcal{U}(M|Y/X) = \{U \subseteq Y - X, U \cup X \in \mathcal{U}(M)\}$.

This can be proven analogously to Lemma 3. However, we will prove it as a corollary of Lemma 3, in order to emphasize the importance of the notion of duality.

Proof. Notice that $\bar{X}$ is a flat in M^*. We now get for any $U \subseteq Y - X$ that

$$\begin{aligned} U \in \mathcal{U}(M|Y/X) &\overset{\text{Prop. 2}}{\iff} Y - X - U \in \mathcal{F}((M|Y/X)^*) \\ &\overset{\text{Prop. 1}}{\iff} Y - X - U \in \mathcal{F}(M^*|\bar{X}/\bar{Y}) \\ &\overset{\text{Lm. 3}}{\iff} (Y - X - U) \cup \bar{Y} \in \mathcal{F}(M^*) \\ &\iff \overline{X \cup U} \in \mathcal{F}(M^*) \\ &\overset{\text{Prop. 2}}{\iff} X \cup Y \in \mathcal{U}(M), \end{aligned}$$

where the fourth equivalence is simply the equality of sets

$$\overline{X \cup U} = (Y - X - U) \cup \bar{Y}$$

as $X \cup U \subseteq Y$. This completes the proof. □

The previous lemmas give the following immediate corollary:

Corollary 1. *Let $M = (E, \rho)$ be a matroid, and let $X \subseteq Y \subseteq E(M)$ be two sets with $X \in \mathcal{U}(M)$ and $Y \in \mathcal{F}(M)$. Then*

$$\mathcal{Z}(M|Y/X) = \{Z \subseteq Y - X, Z \cup X \in \mathcal{Z}(M)\},$$

with the rank function $\rho_{|Y/X}(Z) = \rho(Z \cup X) - \rho(X)$.

In particular, for any $X \subseteq Y \subseteq E$ with $X \in \mathcal{U}(M)$ and $Y \in \mathcal{F}(M)$, $\mathcal{Z}(M|Y/X)$ is isomorphic to an interval in $\mathcal{Z}(M)$. As a consequence, we get a sufficient condition for uniformity of minors, that only depends on the Hasse diagram of $\mathcal{Z}(M)$.

Theorem 5. *Let X and Y be two cyclic flats in M with $X \lessdot_{\mathcal{Z}(M)} Y$. Let $n = |Y| - |X|$ and $k = \rho(Y) - \rho(X)$. Then $M|Y/X \cong U_n^k$.*

Proof. By Corollary 1, we have $\mathcal{Z}(M|Y/X) = \{\emptyset, Y - X\}$ as there is no cyclic flat Z with $X \subset Z \subset Y$. Again by Corollary 1, we have $\rho(Y - X) = \rho(Y) - \rho(X) = k$. Thus, by Proposition 4, $M|Y/X$ is the uniform matroid U_n^k. □

Corollary 2. *Let M be a matroid that contains no U_n^k minors. Then, for every edge $X \lessdot_{\mathcal{Z}(M)} Y$ in the Hasse diagram of $\mathcal{Z}(M)$, we have $\rho(Y) - \rho(X) < k$ or $\eta(Y) - \eta(X) < n - k$.*

Proof. Assume for a contradiction that $X \lessdot_{\mathcal{Z}(M)} Y$ has $\rho(Y) - \rho(X) = k' \geq k$ and $\eta(Y) - \eta(X) = n' - k' \geq n - k$. Then by Theorem 5, $M|Y/X \cong U_{n'}^{k'}$, and so contains U_n^k as a minor by Lemma 1. □

Now, we are going to need formulas for how to compute the lattice operators in $\mathcal{Z}(M|Y/X)$ in terms of the corresponding operators in $\mathcal{Z}(M)$. These can be derived from corresponding formulas for the closure and cyclic operator. To derive these, we will need to generalize Corollary 1 to the setting where the restriction and contraction are not necessarily performed at cyclic flats.

Theorem 6. *For $X \subseteq Y \subseteq E$, we have*

1. $\mathcal{Z}(M|Y) = \{\mathrm{cyc}(Z \cap Y) : Z \in \mathcal{Z}(M)\}$.
2. $\mathcal{Z}(M/X) = \{\mathrm{cl}(X \cup Z) - X : Z \in \mathcal{Z}(M)\}$.
3. $\mathcal{Z}(M|Y/X) = \Big\{\mathrm{cl}\Big(X \cup \mathrm{cyc}\big(Z \cap Y\big)\Big) \cap \big(Y - X\big) : Z \in \mathcal{Z}(M)\Big\}$
$= \Big\{\mathrm{cyc}\Big(\mathrm{cl}\big(X \cup Z\big) \cap Y\Big) - X : Z \in \mathcal{Z}(M)\Big\}$.

Proof. 1. First, observe that the cyclic operator in $M|Y$ is the same as that in M, and that the flats in $M|Y$ are $\{F \cap Y : F \in \mathcal{F}(M)\}$. Thus we have

$$\mathcal{Z}(M|Y) = \{\mathrm{cyc}(F \cap Y) : F \in \mathcal{F}(M)\} \supseteq \{\mathrm{cyc}(Z \cap Y) : Z \in \mathcal{Z}(M)\}.$$

On the other hand, let $A \in \mathcal{Z}(M|Y)$, so $\mathrm{cyc}(A) = A$ and $\mathrm{cl}(A) \cap Y = A$. But the closure operator preserves cyclicity, so $\mathrm{cl}(A) \in \mathcal{Z}(M)$. We then observe that

$$A = \mathrm{cyc}(\mathrm{cl}(A) \cap Y) \in \{\mathrm{cyc}(Z \cap Y) : Z \in \mathcal{Z}(M)\}.$$

This proves the reverse inclusion

$$\mathcal{Z}(M|Y) = \{\mathrm{cyc}(F \cap Y) : F \in \mathcal{F}(M)\} \subseteq \{\mathrm{cyc}(Z \cap Y) : Z \in \mathcal{Z}(M)\}.$$

2. This is the dual statement of Statement 1, and so follows immediately by applying Statement 1 to the matroid $M^*|\bar{X}$.

Indeed, for a set $U \subseteq \bar{X}$ we have

$$\begin{aligned}
U \in \mathcal{Z}(M/X) &\iff \bar{X} - U \in \mathcal{Z}(M^*|\bar{X}) \\
&\iff \bar{X} - U = \mathrm{cyc}_{M^*}(Z \cap \bar{X}) \text{ for some } Z \in \mathcal{Z}(M^*) \\
&\iff \overline{\bar{X} - U} = \mathrm{cl}_M(\overline{Z \cap \bar{X}}) \text{ for some } Z \in \mathcal{Z}(M^*) \\
&\iff X \cup U = \mathrm{cl}_M(\bar{Z} \cup X) \text{ for some } Z \in \mathcal{Z}(M^*) \\
&\iff X \cup U = \mathrm{cl}_M(Z' \cup X) \text{ for some } Z' \in \mathcal{Z}(M).
\end{aligned}$$

Since $U \cap X = \emptyset$, this is equivalent to $U = \mathrm{cl}_M(Z' \cup X) - X$.

3. We first apply Statement 2 and then Statement 1 to the restricted matroid $M|Y$, and get

$$\mathcal{Z}(M|Y/X) = \{\mathrm{cl}_{|Y}(X \cup \mathrm{cyc}(Z \cap Y)) - X : Z \in \mathcal{Z}(M)\}.$$

Since $\mathrm{cl}_{|Y}(T) = \mathrm{cl}(T) \cap Y$ if $T \subseteq Y$, then we have

$$\mathcal{Z}(M|Y/X) = \{\mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)) \cap (Y - X) : Z \in \mathcal{Z}(M)\}.$$

For the second equality in Statement 3, we need to study the operator $\mathrm{cyc}_{/X}$. Suppose $T \subseteq E - X$. Using duality and the formula for $\mathrm{cl}_{|\bar{X}}$, we find that

$$\mathrm{cyc}_{/X}(T) = \mathrm{cyc}(X \cup T) - X.$$

Now we are ready to prove the last equality. Applying first Statement 1 and then Statement 2 to the contracted matroid M/X, we get

$$\mathcal{Z}(M|Y/X) = \{\mathrm{cyc}_{/X}((\mathrm{cl}(X \cup Z) - X) \cap Y) : Z \in \mathcal{Z}(M)\}.$$

Applying the formula for $\mathrm{cyc}_{/X}$, we obtain

$$\begin{aligned}\mathcal{Z}(M|Y/X) &= \{\mathrm{cyc}((\mathrm{cl}(X \cup Z) \cap Y - X) \cup X) - X : Z \in \mathcal{Z}(M)\} \\ &= \{\mathrm{cyc}(\mathrm{cl}(X \cup Z) \cap Y) - X : Z \in \mathcal{Z}(M)\},\end{aligned}$$

where the last equality follows as $X \subseteq \mathrm{cl}(X \cup Z)$. This concludes the proof. □

4. Sufficient conditions for uniformity

From Statement 3 of Theorem 6 we get two surjective maps $\mathcal{Z}(M) \to \mathcal{Z}(M|Y/X)$, given by

$$Z \mapsto \mathrm{cyc}(\mathrm{cl}(X \cup Z) \cap Y) - X \text{ and } Z \mapsto \mathrm{cl}\Big(X \cup \mathrm{cyc}\big(Z \cap Y\big)\Big) \cap \big(Y - X\big)$$

respectively. To identify uniform minors in M, we need to detect X and Y such that either, and thus both, of these maps have image $\{\emptyset, Y - X\}$.

4.1. Minors given by restriction or contraction only

We will begin by considering a simpler case when the minor is the result of a restriction only, *i.e.,* when the minor is given by $M|Y$. So, let $M = (E, \rho)$ be a matroid and Y an arbitrary subset of E. We can use Corollary 1 to restrict the amount of information we need to consider. Indeed, it is straightforward to see that

$$M|Y = M|\mathrm{cl}(Y) \setminus (\mathrm{cl}(Y) - Y). \tag{2}$$

Then, Theorem 6 states that the cyclic flats of $M|Y$ depend only on the cyclic flats of $M|\mathrm{cl}(Y)$. Furthermore, according to Corollary 1 the cyclic flats of $M|\mathrm{cl}(Y)$ are exactly the cyclic flats of M contained in $\mathrm{cl}(Y)$. Hence, we can restrict the study to the case when $M = (E, \rho)$ is a matroid and Y is a subset of full rank. Define $k := \rho(Y)$ and $n := |Y|$. With this setup, we obtain the following theorem.

Theorem 7. *Let $M = (E, \rho)$ be a matroid and Y a subset of full rank. $M|Y$ is isomorphic to the uniform matroid U_n^k if and only if either Y is a basis of M or the following two conditions are satisfied:*

1. *Y is a cyclic set of M.*
2. *For all $Z \in \mathcal{Z}(M)$ with $\rho(Z) < k$, $Z \cap Y$ is independent in M.*

Before stating the proof, we will need one simple but useful lemma about the properties of the closure and cyclic operators.

Lemma 5. *Let $M = (E, \rho)$ be a matroid and $Y \subseteq E$. Then*

1. $\mathrm{cl}(\mathrm{cyc}(Y)) \cap Y = \mathrm{cyc}(Y)$.
2. $\mathrm{cyc}(\mathrm{cl}(Y)) \cup Y = \mathrm{cl}(Y)$.

Proof. We prove Part 1 of the lemma; Part 2 follows immediately by duality. Since we know that $\mathrm{cyc}(Y) \subseteq Y$ and $\mathrm{cyc}(Y) \subseteq \mathrm{cl}(\mathrm{cyc}(Y))$, it is enough to show the inclusion $\mathrm{cl}(\mathrm{cyc}(Y)) \cap Y \subseteq \mathrm{cyc}(Y)$. Assume for a contradiction that $e \in \mathrm{cl}(\mathrm{cyc}(Y)) \cap Y - \mathrm{cyc}(Y)$. Then we have $\rho(\mathrm{cyc}(Y) \cup e) = \rho(\mathrm{cyc}(Y))$ because $e \in \mathrm{cl}(\mathrm{cyc}(Y))$. On the other hand, we have $\rho(\mathrm{cyc}(Y) \cup e) > \rho(\mathrm{cyc}(Y))$ because $e \in Y - \mathrm{cyc}(Y)$. This is a contradiction. □

Corollary 3. *Let $M = (E, \rho)$ be a matroid and $Y \subseteq E$. Then*

1. *$Y \in \mathcal{U}$ if and only if* $\mathrm{cl}(\mathrm{cyc}(Y)) = \mathrm{cl}(Y)$.
2. *$Y \in \mathcal{F}$ if and only if* $\mathrm{cyc}(\mathrm{cl}(Y)) = \mathrm{cyc}(Y)$.

Proof. The right implications are immediate as $Y \in \mathcal{U}$ means that $\mathrm{cyc}(Y) = Y$ and $Y \in \mathcal{F}$ means that $\mathrm{cl}(Y) = Y$. For the left implication in the first statement, notice that if $\mathrm{cl}(\mathrm{cyc}(Y)) = \mathrm{cl}(Y)$, then by Lemma 5 we have

$$Y = \mathrm{cl}(Y) \cap Y = \mathrm{cl}(\mathrm{cyc}(Y)) \cap Y = \mathrm{cyc}(Y) \cap Y = \mathrm{cyc}(Y),$$

so Y is cyclic. The second statement is the dual of the first. □

We now present the proof of Theorem 7.

Proof. We know that $M|Y \cong U_n^k$ if and only if Y is a basis of M or $\mathcal{Z}(M|Y) = \{\emptyset, Y\}$. On the other hand, we know by Theorem 6, that

$$\mathcal{Z}(M|Y) = \{\mathrm{cyc}(Z \cap Y) : Z \in \mathcal{Z}(M)\}.$$

Then we have that $M|Y \cong U_n^k$ if and only if $\mathrm{cyc}(Z \cap Y) \in \{\emptyset, Y\}$ for all $Z \in \mathcal{Z}(M)$.

Now consider the cyclic flat $Z_Y := \mathrm{cl}(\mathrm{cyc}(Y))$. Using Lemma 5, we have that

$$\mathrm{cyc}(Z_Y \cap Y) = \mathrm{cyc}(Y).$$

Two cases can occur. If $\mathrm{cyc}(Y) = \emptyset$ then Y was a basis of M and we end up with a minor isomorphic to U_k^k. If not, then $\mathrm{cyc}(Y)$ must be equal to Y. So, we have that $Y \in \mathcal{Z}(M|Y)$ if and only if Y is a cyclic set and we obtain the first condition. Since Y already has full rank, there is only one cyclic flat that contains Y, namely $\mathrm{cl}(\mathrm{cyc}(Y)) = E$. Therefore, for every other cyclic flat Z, *i.e.,* for all Z with $\rho(Z) < k$, we have that

$$\mathrm{cyc}(Z \cap Y) \subseteq Z \cap Y \neq Y.$$

However, by Theorem 6, $\mathrm{cyc}(Z \cap Y)$ is a cyclic flat of $M|Y$. Thus, for all $Z \in \mathcal{Z}(M)$ with $\rho(Z) < k$, we have $\mathrm{cyc}(Z \cap Y) = \emptyset$, or equivalently, $Z \cap Y$ is independent. Notice that, combined with the first condition, this implies immediately that $\mathcal{Z}(M|Y) = \{\emptyset, Y\}$. This concludes the proof. □

Corollary 4. *Let $M = (E, \rho)$ be a matroid and Y a subset of full rank. If $M|Y$ is isomorphic to U_n^k for $k < n$, then the ground set E must be a cyclic flat,* i.e., $E \in \mathcal{Z}(M)$.

Now we can do the same for M/X and use duality to get back to the restriction case. By minor properties, we have

$$M/X = M/\mathrm{cyc}(X)/(X - \mathrm{cyc}(X)). \tag{3}$$

Then, Corollary 1 states that the cyclic flats of $M/\mathrm{cyc}(X)$ correspond to the cyclic flats of M that contain $\mathrm{cyc}(X)$. Thus, we will consider a matroid $M = (E, \rho)$ and X an independent subset of E. Define $k := \rho(E) - \rho(X)$ and $n := |E - X|$. Then, we have the following dual statement of Theorem 7.

Theorem 8. *Let $M = (E, \rho)$ be a matroid and X an independent subset of E. M/X is isomorphic to the uniform matroid U_n^k if and only if either X is a basis of M or the following two conditions are satisfied:*

1. *X is a flat of M.*
2. *For all $Z \in \mathcal{Z}(M) - 0_{\mathcal{Z}}$, we have $\mathrm{cl}(X \cup Z) = E$.*

Corollary 5. *Let $M = (E, \rho)$ be a matroid and X an independent subset of E. If M/X is isomorphic to U_n^k for $0 < k$, then the empty set must be a cyclic flat,* i.e., $\emptyset \in \mathcal{Z}(M)$.

4.2. Minors given by both restriction and contraction

This part combines the two previous situations into a more general statement. We will see that, when we allow both a restriction and a contraction to occur, we lose some conditions on the matroid that are then replaced by conditions on the sets used in the minor.

Let $M = (E, \rho)$ be a matroid and $X \subset Y \subseteq E$ two sets. Combining minor properties (2) and (3) and Corollary 1, it is sufficient to only consider the cyclic flats between $\mathrm{cyc}(X)$ and $\mathrm{cl}(Y)$. In addition, we want to avoid some known cases, namely when Y is independent (we will obtain U_n^n) and when X has full rank (we will obtain U_n^0). Define $k := \rho(E) - \rho(X)$ and $n := |Y - X|$. We get the following theorem.

Theorem 9. *Let $M = (E, \rho)$ be a matroid and $X \subset Y \subseteq E$ two sets such that Y is a dependent full-rank set and X is an independent set with $\rho(X) < \rho(E)$. The minor $M|Y/X$ is isomorphic to a uniform matroid U_n^k if and only if*

1. $\mathrm{cl}(X) \cap Y = X$,
2. $Y - X \subseteq \mathrm{cyc}(Y)$, *and*
3. *for all $Z \in \mathcal{Z}(M)$ either $Z \cap Y$ is independent or $\mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)) = E$.*

Proof. Using Theorem 6, we have that $M|Y/X \cong U_n^k$ if and only if

$$\mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)) \cap (Y - X) \in \{\emptyset, Y - X\} \text{ for all } Z \in \mathcal{Z}(M).$$

Assuming condition 1, for any $Z \in \mathcal{Z}(M)$ with $Z \cap Y$ independent, we have

$$\mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)) \cap (Y - X) = \mathrm{cl}(X) \cap (Y - X) = \emptyset.$$

Assuming condition 2, for any $Z \in \mathcal{Z}(M)$ with $\mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)) = E$ we have

$$\mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)) \cap (Y - X) = Y - X.$$

Thus, conditions 1–3 imply that $M|Y/X$ is uniform.

Conversely, assume that $M|Y/X \simeq U_n^k$, and denote by ρ' the rank function on $M|Y/X$. Note that, since Y is dependent and X is not, and since $\rho(Y) > \rho(X)$, we have $0 < k < n$. Thus, for any $t \in Y - X$, we have

$$\rho(X \cup t) = \rho(X) + \rho'(t) = \rho(X) + 1,$$

so $t \notin \mathrm{cl}(X)$, which proves 1. Moreover,

$$\rho(Y-t) = \rho(X) + \rho'(Y-X-t) = \rho(X) + \rho'(Y-X) = \rho(Y),$$

so $t \in \mathrm{cyc}(Y)$, which proves 2.

It remains to show that for all $Z \in \mathcal{Z}(M)$, either $Z \cap Y$ is independent or $\mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)) = E$. We already know that

$$\mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)) \cap (Y - X) \in \{\emptyset, Y - X\} \text{ for all } Z \in \mathcal{Z}(M).$$

Let $Z \in \mathcal{Z}(M)$ be such that

$$\mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)) \cap (Y - X) = \emptyset.$$

Then $\mathrm{cyc}(Z \cap Y) \cap (Y - X) = \emptyset$, so $\mathrm{cyc}(Z \cap Y) \subseteq X$. But since X is independent, it can not contain any nontrivial cyclic set, so $\mathrm{cyc}(Z \cap Y) = \emptyset$ and $Z \cap Y$ is independent. Finally, let $Z \in \mathcal{Z}(M)$ be such that

$$\mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)) \cap (Y - X) = Y - X,$$

or in other words

$$Y - X \subseteq \mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)).$$

Since we also have $X \subseteq \mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y))$, it follows that

$$Y \subseteq \mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)).$$

Taking the closure of both sides, we get

$$E = \mathrm{cl}(Y) \subseteq \mathrm{cl}(X \cup \mathrm{cyc}(Z \cap Y)) \subseteq E.$$

This proves Condition 3. □

This theorem and the proof are only based on the first representation of the cyclic flats of $M|Y/X$ in Theorem 6. We can also state an equivalent theorem obtained using the second representation in Theorem 6.

Theorem 10. *Let $M = (E, \rho)$ be a matroid and $X \subset Y \subseteq E$ two sets such that Y is a dependent full-rank set and X is an independent set with $\rho(X) < \rho(E)$. The minor $M|Y/X$ is isomorphic to a uniform matroid $U_{k,n}$ if and only if*

1. $\mathrm{cl}(X) \cap Y = X$,
2. $Y - X \subseteq \mathrm{cyc}(Y)$, *and*
3. *for all $Z \in \mathcal{Z}(M)$ either $\mathrm{cl}(X \cup Z) \cap Y$ is independent or $\mathrm{cl}(X \cup Z) = E$.*

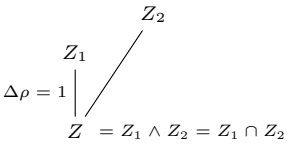

Fig. 1. Illustration of Lemma 6.

We conclude this section with a lemma that will be used later in our analysis, about pairs $Z \subset Z_1$ of cyclic flats with rank difference equal to one.

Lemma 6. *(See Fig. 1.) Let Z, Z_1, Z_2 be cyclic flats with $Z \subseteq Z_1$, $Z \subseteq Z_2$, $Z_1 \nsubseteq Z_2$ and $\rho(Z_1) = \rho(Z) + 1$. Then $Z_1 \cap Z_2 = Z$.*

Proof. The intersection $Z_1 \cap Z_2$ of two flats is a flat of rank $< \rho(Z_1)$, which contains Z by assumption. But Z is a flat of rank $\rho(Z_1) - 1$, so any set properly containing it has rank $\geq \rho(Z_1)$. It follows that $Z_1 \cap Z_2 = Z$. □

5. Reconstructing the lattice of flats

As the lattice of cyclic flats together with the induced rank function uniquely determines a matroid, it clearly also defines the lattice of flats $\mathcal{F}(M)$. However, reconstructing $\mathcal{F}(M)$ from $\mathcal{Z}(M)$ is not entirely straightforward. In order to do this, we will use the following notation.

Definition 7. Let $M = (E, \rho)$ be a matroid and let $A \subseteq E$. We will denote by $A^{\mathcal{F}}$ the set $\{e \in E - A | A \cup \{e\} \in \mathcal{F}(M)\}$.

In particular, we see that if A is not a flat, then $A^{\mathcal{F}}$ is at most a singleton, because otherwise A could be written as an intersection

$$A = \cap_{e \in A^{\mathcal{F}}} (A \cup \{e\})$$

of flats, and would thus be a flat itself. On the other hand, if A is a flat, then we get the following equivalent description of $A^{\mathcal{F}}$.

Lemma 7. *Let A be a flat in $M = (E, \rho)$ and $e \in E - A$. Then $e \in A^{\mathcal{F}}$ if and only if $\rho(A \cup \{e, f\}) = \rho(A) + 2$ for all $f \in E - A - \{e\}$.*

Proof. As A is a flat, $\rho(A \cup \{e\}) = \rho(A) + 1$ for all $e \in E - A$. For such e, $e \in A^{\mathcal{F}}$ if and only if $A \cup \{e\}$ is a flat, which it is precisely if

$$\rho(A \cup \{e\} \cup \{f\}) > \rho(A \cup \{e\}) = \rho(A) + 1$$

for all $f \in E - A - \{e\}$. □

From Lemma 7, it easily follows that $A \mapsto A^{\mathcal{F}}$ is an order-reversing set-valued map on the lattice of flats, and as a consequence also on the lattice of cyclic flats.

Lemma 8. *Let A and B be flats in $M = (E, \rho)$ with $A \subseteq B$. Then $A^{\mathcal{F}} \supseteq B^{\mathcal{F}}$.*

Proof. If $e \in B^{\mathcal{F}}$, then by Lemma 7 we have $\rho(B \cup \{e, f\}) = \rho(B) + 2$ for all $f \in E - B - \{e\}$. By submodularity of ρ, we then also get $\rho(A \cup \{e, f\}) = \rho(A) + 2$ for all $f \in E - B - \{e\}$. Moreover, for $f \in B - A$, we have

$$\begin{aligned}\rho(A \cup \{e, f\}) - \rho(A) &= (\rho(A \cup \{e, f\}) - \rho(A \cup \{f\})) + (\rho(A \cup \{f\}) - \rho(A)) \\ &\geq (\rho(B \cup \{e\}) - \rho(B)) + (\rho(A \cup \{f\}) - \rho(A)) \\ &= 1 + 1 = 2.\end{aligned}$$

Thus we have $\rho(A \cup \{e, f\}) = \rho(A) + 2$ for all $f \in E - A - \{e\}$, so $e \in A^{\mathcal{F}}$. □

To an arbitrary $A \subseteq E$, we will now associate two intervals in $\mathcal{Z}(M)$, both of which will yield the singleton $\{A\}$ if A is already a cyclic flat.

Definition 8. (See Fig. 2.) Let $A \subseteq E$, and let

$$A^{\vee} = \bigvee_{\substack{Z \subseteq A \\ Z \in \mathcal{Z}(M)}} Z \text{ and } A^{\wedge} = \bigwedge_{\substack{Z \supseteq A \\ Z \in \mathcal{Z}(M)}} Z.$$

Lemma 9. *Let $A \subseteq E$. Then we have the inclusions*

$$A^{\vee} \subseteq \mathrm{cl}(\mathrm{cyc}(A)) \subseteq \mathrm{cyc}(\mathrm{cl}(A)) \subseteq A^{\wedge}.$$

Proof. Every cyclic flat that is a subset of A is also a subset of $\mathrm{cyc}(A)$, so

$$\bigcup_{\substack{Z \subseteq A \\ Z \in \mathcal{Z}(M)}} Z \subseteq \mathrm{cyc}(A).$$

It then follows that

$$A^{\vee} = \mathrm{cl}\left(\bigcup_{\substack{Z \subseteq A \\ Z \in \mathcal{Z}(M)}} Z \right) \subseteq \mathrm{cl}(\mathrm{cyc}(A)).$$

Dually, every cyclic flat that contains A also contains $\mathrm{cl}(A)$, so

$$\bigcap_{\substack{Z \supseteq A \\ Z \in \mathcal{Z}(M)}} Z \supseteq \mathrm{cl}(A).$$

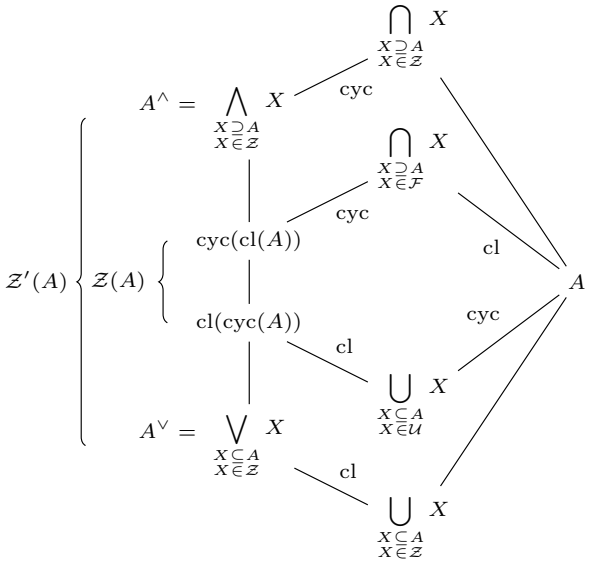

Fig. 2. Illustration of Definition 8 and Lemma 9.

It then follows that

$$A^\wedge = \mathrm{cyc}\left(\bigcap_{\substack{Z\supseteq A\\ Z\in\overline{\mathcal{Z}}(M)}} Z\right) \supseteq \mathrm{cyc}(\mathrm{cl}(A)).$$

Finally, as $A \subseteq \mathrm{cl}(A)$ we have that $\mathrm{cyc}(A) \subseteq \mathrm{cyc}(\mathrm{cl}(A))$, and as the latter is a flat by (1), we have $\mathrm{cl}(\mathrm{cyc}(A)) \subseteq \mathrm{cyc}(\mathrm{cl}(A))$. □

By Lemma 9 we can define the intervals

$$\mathcal{Z}(A) = [\mathrm{cl}(\mathrm{cyc}(A)), \mathrm{cyc}(\mathrm{cl}(A))]_{\mathcal{Z}(M)} \text{ and } \mathcal{Z}'(A) = [A^\vee, A^\wedge]_{\mathcal{Z}(M)},$$

and observe that $\mathcal{Z}(A) \subseteq \mathcal{Z}'(A)$.

The following lemma first occurred in [17]. We state it here for completeness.

Lemma 10. *Let $Z \in \mathcal{Z}$ satisfy $\rho(Z) + |A - Z| = \rho(A)$. Then $Z \in \mathcal{Z}(A)$.*

Proof. Note that, for any $Z \subseteq E$,

$$\rho(A) \leq \rho(A \cap Z) + |A - Z| \leq \rho(Z) + |A - Z|.$$

The first inequality is satisfied with equality if and only if $\mathrm{cyc}(A) \subseteq A \cap Z$, which implies $\mathrm{cyc}(A) \subseteq Z$. We claim that the second inequality is satisfied with equality only

if $Z \subseteq \mathrm{cl}(A)$. Indeed, if $Z \nsubseteq \mathrm{cl}(A)$ choose $z \in Z - \mathrm{cl}(A)$. Then $\rho(A) < \rho(A \cup \{z\})$, so by submodularity we have

$$\rho(Z \cap A) < \rho((Z \cap A) \cup \{z\}) \leq \rho(Z).$$

Therefore, any Z satisfying $\rho(Z) + |A - Z| = \rho(A)$ must also satisfy $\mathrm{cyc}(A) \subseteq Z \subseteq \mathrm{cl}(A)$, so $\mathrm{cl}(\mathrm{cyc}(A)) \subseteq \mathrm{cl}(Z)$ and $\mathrm{cyc}(Z) \subseteq \mathrm{cyc}(\mathrm{cl}(A))$. But, if Z is a cyclic flat, then $Z = \mathrm{cl}(Z) = \mathrm{cyc}(Z)$, and it follows that

$$Z \in [\mathrm{cl}(\mathrm{cyc}(A)), \mathrm{cyc}(\mathrm{cl}(A))] = \mathcal{Z}(A). \quad \square$$

Lemma 11. *Let $M = (E, \rho)$ be a matroid, and let $F \in \mathcal{F}(M)$. Then $F^\vee = \mathrm{cl}(\mathrm{cyc}(F)) = \mathrm{cyc}(\mathrm{cl}(F))$.*

Proof. Since F is a flat, we have $\mathrm{cyc}(\mathrm{cl}(F)) = \mathrm{cyc}(F) \subseteq F$. Since $F^\vee$ contains all cyclic flats that are contained in F, it thus also contains $\mathrm{cyc}(\mathrm{cl}(F))$. The inclusions

$$\mathrm{cyc}(\mathrm{cl}(F)) \subseteq F^\vee \subseteq \mathrm{cl}(\mathrm{cyc}(F)) \subseteq \mathrm{cyc}(\mathrm{cl}(F))$$

now show that the sets are equal. $\square$

Corollary 6. *Let $M = (E, \rho)$ be a matroid, and let $F \in \mathcal{F}(M)$. Then $F^\vee = \mathrm{cyc}(F) \subseteq F$.*

We are now ready to present a result which explicitly reconstructs $\mathcal{F}(M)$ from $\mathcal{Z}(M)$. Clearly, this result can immediately be dualized to obtain a description of $\mathcal{U}(M)$.

Proposition 6. *Let $M = (E, \rho)$ be a matroid, and let $F \subseteq E$ be a set with $F^\vee \subseteq F$. Then the following are equivalent*

(i) F *is a flat.*
(ii) $F^\vee = 1_{\mathcal{Z}(F)}$.
(iii) For every $Z \in \mathcal{Z}'(F) - \{F^\vee\}$ *it holds that*

$$|F \cap Z| - \rho(Z) < \eta(F^\vee).$$

(iv) Every set B *with* $F^\vee \subseteq B \subseteq F$ *is a flat, and if* $F \subsetneq F^\wedge$ *then* $|F| - \rho(F^\wedge) < \eta(F^\vee)$.
(v) For every set B *with* $F^\vee \subseteq B \subseteq F$ *and* $B \subsetneq B^\wedge$ *it holds that* $|B| - \rho(B^\wedge) < \eta(B^\vee)$.

Proof. (i)⇒(ii): Assume $F \in \mathcal{F}$, so $\mathrm{cyc}(F) \in \mathcal{Z}$. Then $\mathrm{cyc}(F)$ is a largest element of $\{Z \in \mathcal{Z} : Z \subseteq F\}$, so $\mathrm{cyc}(F) = F^\vee$. Moreover, we have $\mathrm{cl}(F) = F$, so

$$1_{\mathcal{Z}(F)} = \mathrm{cyc}(\mathrm{cl}(F)) = \mathrm{cyc}(F) = F^\vee.$$

(ii)⇒(i): As $F^\vee$ is a cyclic set contained in F, we also have $F^\vee \subseteq \mathrm{cyc}(F)$, so if (ii) holds, then we have

$$\mathrm{cyc}(\mathrm{cl}(F)) = F^\vee \subseteq \mathrm{cyc}(F) \subseteq \mathrm{cyc}(\mathrm{cl}(F)).$$

Thus $\mathrm{cyc}(F) = \mathrm{cyc}(\mathrm{cl}(F))$, so

$$\eta(F) = \eta(\mathrm{cyc}(F)) = \eta(\mathrm{cyc}(\mathrm{cl}(F))) = \eta(\mathrm{cl}(F)).$$

As we also have $\rho(F) = \rho(\mathrm{cl}(F))$, it follows that $F = \mathrm{cl}(F)$, so F is a flat.

(ii)⇒(iii): Assume that $F^\vee = 1_{\mathcal{Z}(F)}$, so $\mathcal{Z}(F) = \{F^\vee\}$. For every $Z \in \mathcal{Z}'(F) - \{F^\vee\}$, since $F^\vee \subseteq F$, we then have

$$|F| - \eta(F^\vee) = \rho(F^\vee) + |F - F^\vee| = \rho(F) < \rho(Z) + |F - Z| = \rho(Z) + |F| - |F \cap Z|,$$

where the inequality follows from Lemma 10 as $Z \notin \mathcal{Z}(F)$. Rewriting this inequality, we immediately get

$$|F \cap Z| - \rho(Z) < \eta(F^\vee).$$

(iii)⇒(ii): Assume that (iii) holds, and let $Z \in \mathcal{Z}'(F) - \{F^\vee\}$. Then we have

$$\eta(F^\vee) - |F^\vee - F| = \eta(F^\vee) > |F \cap Z| - \rho(Z) = \eta(Z) - |Z - F|.$$

In particular, we see that $Z \neq 1_{\mathcal{Z}(F)}$, so we must have $F^\vee = 1_{\mathcal{Z}(F)}$.

(iv) ⇒(i): If B is a flat for all $F^\vee \subseteq B \subseteq F$, then in particular $B = F$ is a flat.

(i) ⇒(iv) (assuming (ii)⇒(i)⇒(iii)): Let F be a flat with $F^\vee \subseteq B \subseteq F$. Then $F^\vee$ is a largest element of $\{Z \in \mathcal{Z} : Z \subseteq B\}$, so $B^\vee = F^\vee$. Also,

$$B^\vee \subseteq 1_{\mathcal{Z}(B)} \subseteq 1_{\mathcal{Z}(F)} = F^\vee = B^\vee,$$

so we have equality $B^\vee = 1_{\mathcal{Z}(B)}$. By the implication (ii)⇒(i), B is a flat. Now assume $F \subsetneq F^\wedge$. Since $F^\wedge \in \mathcal{Z}'(F) - \{F^\vee\}$, the implication (i)⇒(iii) yields

$$|F| - \rho(F^\wedge) = |F \cap F^\wedge| - \rho(F^\wedge) < \eta(F^\vee).$$

(v)⇒(iii): Let $Z \in \mathcal{Z}'(F) - \{F^\vee\}$ and set $B = F \cap Z$. Then $F^\vee \subseteq B \subseteq F$, and $1_{\mathcal{Z}(B)} \subseteq B^\wedge \subseteq Z$. If $1_{\mathcal{Z}(B)} \subsetneq Z$, then we get

$$|B| - \rho(Z) = |B| - (\rho(Z) + |B - Z|) < |B| - \rho(B) = \eta(B) = \eta(\mathrm{cyc}(B)) = \eta(F^\vee).$$

Now assume $1_{\mathcal{Z}(B)} = B^\wedge = Z$, so $B \subseteq Z = B^\wedge$. If $B \subsetneq B^\wedge$, then by (v) we have

$$|F \cap Z| - \rho(Z) = |B| - \rho(Z) \leq |B| - \rho(B^\wedge) < \eta(B^\vee) = \eta(F^\vee).$$

Finally, if $B = B^\wedge$, then B is a cyclic flat, so $B = F^\vee$ and $\mathcal{Z}(B) = \{B\}$. As $Z \neq F^\vee$ it follows that $Z \notin \mathcal{Z}(B)$, so

$$|B| - \rho(Z) = |B| - (\rho(Z) + |B - Z|) < |B| - \rho(B) = \eta(B) = \eta(\mathrm{cyc}(B)) = \eta(F^\vee).$$

(iv)⇔(v) (assuming (i)⇔(iv)): This follows immediately by induction over the size of the set $B - F^\vee$. □

6. Characterization of U_n^2 avoiding matroids from $\mathcal{Z}(M)$

We will use the derived description of $\mathcal{F}(M)$ together with Theorem 3 to detect whether U_n^2 is a minor of a matroid M described by its cyclic flats. We use the notation $(F, E)_{\mathcal{F}(M)}$ to denote the open interval between F and E in the lattice of flats $\mathcal{F}(M)$.

Lemma 12. *Let $M = (E, \rho)$ be a matroid, and $F \in \mathcal{F}(M)$ be a flat with $\rho(E) - \rho(F) = 2$. Then U_n^2 is a minor of M/F if and only if $|(F, E)_{\mathcal{F}(M)}| \geq n$.*

Proof. As F is a flat, every proper superset of F has rank $> \rho(E) - 2$, so the minor $M|B/A$ has rank < 2 whenever $F \subsetneq A$. Thus it is enough to show that there is a set $F \subseteq B \subseteq E$ with $M|B/F \cong U_n^2$ if and only if $|(F, E)_{\mathcal{F}(M)}| \geq n$.

For the right implication, assume that there is a subset $F \subseteq B \subseteq E$ such that $\mathrm{cl}(B) = E$ and $M|B/F \cong U_n^2$. Further, let $(B - F) = \{b_1, \ldots, b_n\}$. Now $\mathrm{cl}(F \cup b_i) \in (F, E)_{\mathcal{F}(M)}$ for $i = 1, \ldots, n$. Moreover, if $i \neq j$, as $\rho_{|B/F}(\{b_i, b_j\}) = 2$, we get that

$$\rho(F \cup \{b_i, b_j\}) = \rho(F) + 2 > \rho(F \cup b_i),$$

so $b(j) \notin \mathrm{cl}(F \cup b_i)$. It follows that the flats $\mathrm{cl}(F \cup b_i)$ are all distinct, so $|(F, E)_{\mathcal{F}(M)}| \geq n$.

For the left implication, let $B_1, \ldots, B_n$ be any n different flats in $(F, E)_{\mathcal{F}(M)}$. As $\rho(B_i) = \rho(F_1) + 1$, we get $B_i \cap B_j = F_1$ if $i \neq j$. Now, let $b_i \in B_i - F$ and let $B = F_1 \cup \{b_1, \ldots, b_n\}$. Then we get $\rho(F \cup \{b_i\}) = \rho(F) + 1$ for $i = 1, \ldots, n$, and $\rho(F \cup \{b_i, b_j\}) = \rho(F) + 2$ whenever $i \neq j$, and $\rho(F \cup B) \leq \rho(E) = \rho(F) + 2$. Thus we have $\rho_{|B/F}(A) = \min\{|A|, 2\}$, so $M|B/F \cong U_{2,n}$. □

Lemma 13. *Let $M = (E, \rho)$ be a matroid. Then for $n \geq 3$, U_n^2 is a minor of M if and only if there is a flat $F \in \mathcal{F}(M)$ with $F \subseteq 1_{\mathcal{Z}}$ such that $\rho(1_{\mathcal{Z}}) - \rho(F) = 2$ and $|(F, 1_{\mathcal{Z}})_{\mathcal{F}}| \geq n$.*

Proof. If $e \in E$ is an isthmus, it is also an isthmus in $M|B/A$ for every $A \subseteq B \subseteq E$ with $e \in B - A$. Thus, as U_n^2 is non-degenerate, it can only occur as a minor $M|B/A$ where $B - A$ contains no isthmuses. Moreover, if $e \in A$ is an isthmus, then $M|B/A \simeq M|(B-e)/(A-e)$. Thus, if U_n^2 is a minor of M, then it can be written as $M|B/A$ where B contains no isthmuses, so $B \subseteq 1_{\mathcal{Z}}$. By Theorem 3, if U_n^2 is a minor of $M|1_{\mathcal{Z}}$, it is isomorphic to $M|B/F$ for some flat $F \subseteq B \subseteq 1_{\mathcal{Z}}$ with $\rho(F) + 2 = \rho(B) = \rho(E)$. But by Lemma 12, this is equivalent to the condition $|(F, 1_{\mathcal{Z}})_{\mathcal{F}}| \geq n$. □

Note that the flats of corank 2 in $1_{\mathcal{Z}}$ are easily identifiable via Proposition 6. If such a flat F satisfies $F \cup e \in \mathcal{F}$ for all $e \in 1_{\mathcal{Z}} - F$, then $M|1_{\mathcal{Z}}/F$ is uniform of rank n. We will therefore focus on flats F of corank 2 such that $1_{\mathcal{Z}} - F^{\mathcal{F}} \neq \emptyset$, where

$$F^{\mathcal{F}} = \{e \in E - F | F \cup \{e\} \in \mathcal{F}(M)\}$$

as in Definition 7. The key to detecting copies of U_n^2 from $\mathcal{Z}(M)$ now lies in determining $|(F, 1_{\mathcal{Z}})_{\mathcal{F}}|$ for such flats F, via studying certain antichains in $\mathcal{Z}(M)$. These antichains are defined next.

Definition 9. Let $M = (E, \rho)$ be a matroid and let $F \in \mathcal{F}(M)$ be a flat with $\rho(F) = \rho(1_{\mathcal{Z}}) - 2$. We define $\Upsilon(F) = \Upsilon_M(F)$ as the collection

$$\Upsilon_M(F) = \left\{X \in \mathcal{Z}(M) : \rho(1_{\mathcal{Z}(M)}) - 1 = \rho(X) + |F - X|\right\},$$

and $\bar{\Upsilon}(F) = \bar{\Upsilon}_M(F)$ as the collection of inclusion-maximal elements in $\Upsilon(F)$.

Lemma 14. *Let $M = (E, \rho)$ be a matroid, and let F and H be flats in M with $F \lessdot_{\mathcal{F}} H$ and $|H - F| \geq 2$. Then $H - F \subseteq \mathrm{cyc}(H)$.*

Proof. Let $f \in H - F$. Then $F \subsetneq H - f$, so since F is a flat we get

$$\rho(F) < \rho(H - f) \leq \rho(H) = \rho(F) + 1.$$

It follows that $\rho(H - f) = \rho(H)$ so $f \in \mathrm{cyc}(H)$. □

Proposition 7. *Let $M = (E, \rho)$ be a matroid and let $F \subseteq 1_{\mathcal{Z}}$ be a flat with $\rho(F) = \rho(1_{\mathcal{Z}}) - 2$ and $1_{\mathcal{Z}} - F^{\mathcal{F}} \neq \emptyset$. Then*

$$\bar{\Upsilon}(F) = \{\mathrm{cyc}(\mathrm{cl}(F \cup e)) : e \in 1_{\mathcal{Z}} - F^{\mathcal{F}}\}.$$

Proof. For $e \in 1_{\mathcal{Z}} - F^{\mathcal{F}}$, let $H_e = \mathrm{cl}(F \cup e)$. Note that $F \lessdot_{\mathcal{F}} H_e$ and $|H_e - F| \geq 2$. The proof will proceed in three steps: the first two serve to show that $\mathrm{cyc}(H_e) \in \bar{\Upsilon}(F)$, and the third step shows that any $K \in \bar{\Upsilon}(F)$ can be written as $\mathrm{cyc}(H_e)$ for some $e \in 1_{\mathcal{Z}} - F^{\mathcal{F}}$.

$\underline{\mathrm{cyc}(H_e) \in \Upsilon(F)}$: We have

$$\rho(1_{\mathcal{Z}}) - 1 = \rho(F) + 1 = \rho(H_e) = \rho(\mathrm{cyc}(H_e)) + |H_e - \mathrm{cyc}(H_e)|.$$

But by Lemma 14 we have $H_e - \mathrm{cyc}(H_e) = F - \mathrm{cyc}(H_e)$, so

$$\rho(1_{\mathcal{Z}}) - 1 = \rho(\mathrm{cyc}(H_e)) + |F - \mathrm{cyc}(H_e)|.$$

Thus by definition, $\mathrm{cyc}(H_e) \in \Upsilon(F)$.

$\underline{\mathrm{cyc}(H_e) \in \bar{\Upsilon}(F)}$: Assume for a contradiction that $\mathrm{cyc}(H_e)$ is not inclusion-maximal in $\Upsilon(F)$, and that $K \in \Upsilon(F)$ is a cyclic flat with $\mathrm{cyc}(H_e) \subseteq K$ and

$$\rho(1_{\mathcal{Z}}) - 1 = \rho(K) + |F - K|.$$

Then $H_e - K = F - K$, because by Lemma 14 $H_e - F \subseteq \mathrm{cyc}(H_e) \subseteq K$. Moreover, as H_e is a flat,

$$K \notin \{\mathrm{cyc}(H_e)\} = \mathcal{Z}(H_e),$$

so $\rho(K) + |H_e - K| > \rho(H_e)$. This yields the chain of inequalities

$$\rho(1_{\mathcal{Z}}) - 1 = \rho(K) + |F - K| = \rho(K) + |H_e - K| > \rho(H_e) = \rho(F) + 1,$$

which contradicts the assumption $\rho(1_{\mathcal{Z}}) = \rho(F) + 2$. Thus $\mathrm{cyc}(H_e)$ is inclusion-maximal in $\Upsilon(F)$.

$\underline{\bar{\Upsilon}(F) \subseteq \{\mathrm{cyc}(H_e) : e \in 1_{\mathcal{Z}} - F^{\mathcal{F}}\}}$: Let $K \in \bar{\Upsilon}(F)$. If $K \subseteq F$, then as K is cyclic we would have

$$K \subseteq \mathrm{cyc}(F) \subseteq \mathrm{cyc}(\mathrm{cl}(F \cup e)) \in \Upsilon(F)$$

for any $e \in 1_{\mathcal{Z}} - F^{\mathcal{F}}$. This contradicts the maximality of K.

We thus have $K - F \neq \emptyset$, or in other words $K \cap F \subsetneq K$, so $\rho(K \cap F) < \rho(K)$. It follows that

$$\rho(1_{\mathcal{Z}}) - 2 = \rho(F) \leq \rho(K \cap F) + |F - K| \leq \rho(K) + |F - K| - 1 = \rho(1_{\mathcal{Z}}) - 2.$$

In particular we have equality $\rho(F) = \rho(K \cap F) + |F - K|$, meaning that $\mathrm{cyc}(F) \subseteq K \cap F$.

As K is cyclic, we have $|K - F| \geq 2$. On the other hand, since $\mathrm{cyc}(F) \subseteq K$ we have $|F - K| + \rho(F \cap K) = \rho(F)$. Thus

$$\rho(F) + 1 = \rho(1_{\mathcal{Z}}) - 1 = \rho(K) + |F - K| = \rho(K) + \rho(F) - \rho(F \cap K),$$

so $\rho(K) = \rho(K \cap F) + 1$. It follows that for any $e \in K - F$, $F \cup e \notin \mathcal{F}$ and $K \subseteq \mathrm{cl}(F \cup e) = H_e$. Since K is cyclic, we also get $K \subseteq \mathrm{cyc}(H_e) \in \Upsilon(F)$. But K was assumed to be maximal in $\Upsilon(F)$, which shows that $K = \mathrm{cyc}(H_e)$. □

Theorem 11. *Let $M = (E, \rho)$ be a matroid and let $F \subseteq 1_{\mathcal{Z}}$ be a flat with $\rho(F) = \rho(1_{\mathcal{Z}}) - 2$. Then*

$$|(F, 1_{\mathcal{Z}})_{\mathcal{F}}| = |1_{\mathcal{Z}} - F| - \sum_{Z \in \bar{\Upsilon}(F)} (|Z - F| - 1).$$

Proof. There is a natural surjective map $1_{\mathcal{Z}} - F \to (F, 1_{\mathcal{Z}})_{\mathcal{F}}$ given by $e \mapsto \mathrm{cl}(F \cup e)$. This map is injective on $F^{\mathcal{F}} - F$, because for $e \in F^{\mathcal{F}} - F$ we have $F \cup e = \mathrm{cl}(F \cup e)$.

So $|(F, 1_{\mathcal{Z}})_{\mathcal{F}}| - |F^{\mathcal{F}} - F|$ is the number of sets $H_e = \mathrm{cl}(F \cup e)$ where $e \in 1_{\mathcal{Z}} - F^{\mathcal{F}}$, and each such set corresponds to $|H_e - F|$ elements of $1_{\mathcal{Z}} - F^{\mathcal{F}}$. By Proposition 7, the cyclic operator is a bijection from this collection to $\bar{\Upsilon}(F)$, so

$$|(F, 1_{\mathcal{Z}})_{\mathcal{F}}| - |F^{\mathcal{F}} - F| = |\{H_e : e \in 1_{\mathcal{Z}} - F^{\mathcal{F}}\}| = |\bar{\Upsilon}(F)|.$$

By Lemma 14, we also have $|\mathrm{cyc}(H_e) - F| = |H_e - F|$ for $e \in 1_{\mathcal{Z}} - F^{\mathcal{F}}$, so

$$\sum_{Z \in \bar{\Upsilon}(F)} |Z - F| = |1_{\mathcal{Z}} - F^{\mathcal{F}}|,$$

and hence

$$\sum_{Z \in \bar{\Upsilon}(F)} |(Z - F) - 1| = |1_{\mathcal{Z}} - F^{\mathcal{F}}| - |\bar{\Upsilon}(F)|.$$

Combining this, we get

$$|(F, 1_{\mathcal{Z}})_{\mathcal{F}}| = |F^{\mathcal{F}} - F| + |\bar{\Upsilon}(F)| = |1_{\mathcal{Z}} - F| - \sum_{Z \in \bar{\Upsilon}(F)} |(Z - F) - 1|. \quad \square$$

The dual version of Theorem 11 identifies U_n^{n-2} minors of M via a reconstruction of $\mathcal{U}(M)$. In particular, this yields two different ways to characterize U_4^2-avoiding matroids, by either reconstructing the upper part of $\mathcal{F}(M)$, or by reconstructing the lower part of $\mathcal{U}(M)$.

Corollary 7. *Let M be a matroid. The following three conditions are equivalent.*

(i) *M is binary.*

(ii) *For every flat $F \subseteq 1_{\mathcal{Z}}$ with $\rho(F) = \rho(1_{\mathcal{Z}}) - 2$ it holds that*

$$|1_{\mathcal{Z}} - F| - \sum_X (|X - F| - 1) < 4,$$

where the sum is taken over all inclusion-maximal $X \in \mathcal{Z}(M)$ such that $\rho(1_{\mathcal{Z}(M)}) - 1 = \rho(X) + |F - X|$.

(iii) *For every cyclic set $U \supseteq 0_{\mathcal{Z}}$ with $\eta(U) = |0_{\mathcal{Z}}| + 2$ it holds that*

$$|U - 0_{\mathcal{Z}}| - \sum_X (|U - X| - 1) < 4,$$

where the sum is taken over all inclusion-minimal $X \in \mathcal{Z}(M)$ such that $|0_{\mathcal{Z}}| + 1 + \rho(X) = |X \cap U|$.

Proof. (i)⇔(ii) By Theorem 11, Condition ii is equivalent to $|(F, 1_{\mathcal{Z}(M)})| < 4$. By Lemma 12, this is equivalent to U_4^2 not being a minor of M, which is equivalent to M being binary by Theorem 1.

(i)⇔(iii) For any set $U \subseteq E$, we have $U - 0_{\mathcal{Z}}(M) = 1_{\mathcal{Z}}(M^*) - \bar{U}$. Moreover, U is a cyclic set in M if and only if $\bar{U}$ is a flat in M^*, and $\eta(U) = |0_{\mathcal{Z}}| + 2$ if and only if $\rho^*(\bar{U}) = \rho^*(1_{\mathcal{Z}(M^*)}) - 2$, where ρ^* is the rank function of M^*. Therefore, Condition (iii) holds for M if and only if Condition (ii) holds for the dual matroid M^*. We have already proven that this is equivalent to M^* being binary. But M^* is binary if and only if M is. This completes the proof. □

7. Covering relations in $\mathcal{Z}(M)$ and atomicity

For the rest of the paper, we focus our study on binary matroids and their lattice of cyclic flats. The first consequence of restricting to binary matroids deals with the covering relations in the lattice of cyclic flats. By Theorem 1, a matroid is representable over $\mathbb{F}_2$ if and only if it avoids U_4^2 as a minor. In this case, Corollary 2 tells us that for $X \lessdot_{\mathcal{Z}} Y$ we cannot simultaneously have $\rho(Y) - \rho(X) > 1$ and $\eta(Y) - \eta(X) > 1$. On the other hand, we know by Theorem 3.2 in [3] or by direct calculation, that we always have $\rho(Y) - \rho(X) \geq 1$ and $\eta(Y) - \eta(X) \geq 1$. Thus, if M is representable over $\mathbb{F}_2$, then every edge $X \lessdot_{\mathcal{Z}} Y$ in the Hasse diagram of $\mathcal{Z}(M)$ satisfies exactly one of the following:

(i) $\rho(Y) - \rho(X) = l > 1$. We call such an edge a *rank edge*, and label it $\rho = l$. Such an edge corresponds to a U_{l+1}^l minor in M.
(ii) $\eta(Y) - \eta(X) = l > 1$. We call such an edge a *nullity edge*, and label it $\eta = l$. Such an edge corresponds to a U_{l+1}^1 minor in M.
(iii) $\rho(Y) - \rho(X) = 1$ and $\eta(Y) - \eta(X) = 1$. We call such an edge an *elementary edge*. Such an edge corresponds to a U_2^1 minor in M.

We illustrate this phenomenon in an example.

Example 1. Let $M = ([6], \rho)$ be the binary matroid generated by the matrix

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

The Hasse diagram of its lattice of cyclic flats is displayed in Fig. 3. We have that $\rho(\{1,2,3\}) = 2$ and $\eta(\{1,2,3\}) = 1$. Therefore, in $\mathcal{Z}(M)$, the covering relation $\emptyset \lessdot \{1,2,3\}$ is a rank edge. On the other hand, since $\eta([6]) = 3$, the covering relation $\{1,2,3\} \lessdot [6]$ is a nullity edge. Finally, one the right-hand side of the Hasse diagram, every covering relation in the chain $\emptyset \lessdot \{5,6\} \lessdot \{3,4,5,6\} \lessdot [6]$ is an elementary edge.

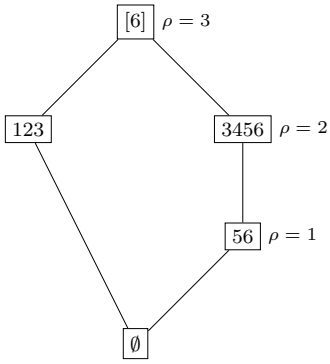

Fig. 3. Lattice of cyclic flats of the matroid from Example 1.

As we will see in the next sections of this paper, the dual relation of being a rank or a nullity edge plays a crucial role in understanding the lattice of cyclic flats. This relation also affects the possible parameters of a matroid and in particular its minimum distance. The study of the connection between the nullity edges and the minimum distance of a matroid is the topic of Section 9. We give here a first glimpse of this connection.

We remark that the condition $d \geq 3$ is equivalent to the matroid M being cosimple. Indeed, $d = 1$ if and only if M^* has no loops, and $d = 2$ if and only if M^* has parallel edges but no loops.

Lemma 15. *If $M = (E, \rho)$ is a binary matroid with minimum distance $d \geq 3$ then every edge $Z \lessdot E$ is a nullity edge.*

Proof. Since the minimum distance is greater than 1, this implies that M contains no isthmuses and $1_{\mathcal{Z}} = E$. Now by Proposition 5, the minimum distance satisfies the relation

$$d = \eta(E) + 1 - \max\{\eta(Z) : Z \in \mathcal{Z}(M) \text{ such that } Z \lessdot E\}.$$

Therefore, if $Z \in \mathcal{Z}(M)$ is such that $Z \lessdot E$, we have that $2 \leq \eta(E) - \eta(Z)$ and the edge $Z \lessdot E$ is a nullity edge. □

Avoiding a U_4^2 minor is not the only characterization of binary matroids. In fact, it was proven in [12] that a binary matroid can be characterized by the relation between its circuits and the circuits of its dual matroid or directly by the symmetric difference of its circuits.

Theorem 12 *([12]). Let M be a matroid. The following are equivalent*

1. *M is binary.*
2. *Let C and C^* be a circuit and a co-circuit respectively. Then $|C \cap C^*|$ is even.*
3. *Let $C_1, \ldots, C_k$ be circuits. Then the symmetric difference $C_1 \triangle \ldots \triangle C_k$ is a disjoint union of circuits.*

This naturally leads us to consider the relation between circuits and cyclic flats of a binary matroid. For this, we restrict our study to simple binary matroids. Recall that a matroid $M = (E, \rho)$ is *simple* if $\rho(S) = 2$ for all two element sets $S \subseteq E$. In particular, simple binary matroids correspond to binary codes whose generator matrices have no zero columns and no repeated columns. We begin by an immediate consequence of the rank edges on the atoms of $\mathcal{Z}(M)$.

Lemma 16. *Let $M = (E, \rho)$ be a simple binary matroid. Then Z is an atom of $\mathcal{Z}(M)$ if and only if $\eta(Z) = 1$.*

Proof. Since M is simple, we have $\emptyset = 0_{\mathcal{Z}}$. Furthermore, it also means that, for all cyclic flats $Z \neq \emptyset$, we have $\rho(Z) > 1$. Hence, every atom Z_{at} will have a rank edge, *i.e.*, $\eta(Z_{at}) = 1$. □

The next two lemmas link atoms in $\mathcal{Z}(M)$ to certain minimal circuits in M.

Lemma 17. *Let $M = (E, \rho)$ be a simple binary matroid. Let C be a circuit of M. Then $\mathrm{cl}(C)$ is an atom of $\mathcal{Z}(M)$ if and only if $\mathrm{cl}(C) = C$.*

Proof. By Lemma 16, $\mathrm{cl}(C)$ is an atom of $\mathcal{Z}(M)$ if and only if $\eta(\mathrm{cl}(C)) = 1$. But since C is a circuit, we have $\eta(C) = 1$. Now $\eta(\mathrm{cl}(C)) = 1 + |\mathrm{cl}(C) - C|$. Hence $\mathrm{cl}(C)$ is an atom if and only if $\mathrm{cl}(C) = C$. □

Lemma 18. *Let $M = (E, \rho)$ be a simple binary matroid that contains no isthmuses. Let $e \in E$ and C be a circuit of minimal length containing e. Then $\mathrm{cl}(C) = C$.*

Proof. Consider a binary representation $\{x_f\}_{f \in M}$ of M. We can express x_e by a linear combination of elements $\{x_f : f \in C \setminus \{e\}\}$. Since C is a binary circuit, we will need all elements in $C \setminus \{e\}$ with coefficients equal to 1. Hence

$$x_e = \sum_{f \in C \setminus \{e\}} x_f.$$

Assume for a contradiction that there exists $e' \in \mathrm{cl}(C) - C$. Then

$$x_{e'} = \sum_{f \in D \subseteq C} x_f.$$

Since M is binary and simple, we have $2 \leq |D| < |C|$.

If $e \in D$, then we have found a circuit smaller than C containing e, which is a contradiction to the minimality of C.

If $e \notin D$, then

$$x_e = \sum_{f \in D} x_f + \sum_{f' \in (C \setminus \{e\}) \setminus D} x_{f'} = x_{e'} + \sum_{f' \in (C \setminus \{e\}) \setminus D} x_{f'}.$$

Thus, e is in the circuit $\{e\} \cup \{e'\} \cup ((C \setminus \{e\}) \setminus D)$ with cardinality $|\{e'\} \cup (C \setminus D)| < |C|$ by the fact that $|D| \geq 2$. Again, this is a contradiction to the minimality of C. Hence $\mathrm{cl}(C) = C$. □

In a matroid without isthmuses, every element e is contained in some circuit by definition. Combining Lemma 17 and 18, we thus obtain the following result.

Lemma 19. *Let $M = (E, \rho)$ be a simple binary matroid that contains no isthmuses. Then every element $e \in E$ is contained in an atom.*

We have enough results to prove the main result of this section, which states that the lattice of cyclic flats of a simple binary matroid with no isthmuses is atomic.

Theorem 13. *Let $M = (E, \rho)$ be a simple binary matroid that contains no isthmuses. Then the lattice of cyclic flats $\mathcal{Z}(M)$ is atomic.*

Proof. By Lemma 19, for every $e \in E$, there exists an atom $Z^e_{at} \in \mathcal{Z}(M)$ with $e \in Z^e_{at}$. Thus,

$$\bigvee_{e \in M} Z^e_{at} \supseteq \bigcup_{e \in M} Z^e_{at} = E.$$

For a cyclic flat $Y \in \mathcal{Z}(M)$, we can restrict the matroid to $M|Y = (Y, \rho)$. Since $\mathcal{Z}(M|Y) = \{Z : Z \subseteq Y, Z \in \mathcal{Z}(M)\}$ by Corollary 1 and $M|Y$ contains no isthmus, we are back to the previous case. Hence

$$Y = \bigvee_{e \in Y} Z^e_{at}$$

and this proves that $\mathcal{Z}(M)$ is atomic. □

Indeed, we have proven a slightly stronger property than atomicity. Namely, any element in $\mathcal{Z}(M)$ is equal not only to the join, but also to the union of all the atoms that it contains. As we can see in Example 1, it is crucial that the matroid is simple for the lattice of cyclic flats to be atomic. As a corollary, we obtain that the lattice of cyclic flats of a binary non-degenerate matroid is coatomic if the minimum distance is greater than 2.

Corollary 8. *Let $M = (E, \rho)$ be a binary non-degenerate matroid. If the minimum distance $d \geq 3$, then $\mathcal{Z}(M)$ is coatomic.*

Proof. M being non-degenerate implies that M^* is also non-degenerate. Let Z^* be an atom of $\mathcal{Z}(M^*)$. By dual property, we have that $E - Z^*$ is a coatom of $\mathcal{Z}(M)$. Now Lemma 15 implies that $\rho^*(Z^*) = \eta(E) - \eta(E - Z^*) \geq 2$. Hence M^* contains no parallel elements and Theorem 13 implies that $\mathcal{Z}(M^*)$ is atomic. □

Finally, by combining the previous results, we obtain a relation between the atoms and the coatoms of $\mathcal{Z}(M)$.

Lemma 20. *Let $M = (E, \rho)$ be a binary simple matroid with no isthmuses and $d \geq 3$. Then for every atom Z_a and coatom Z^c of $\mathcal{Z}(M)$ we have that $|Z_a \setminus Z^c|$ is even.*

Proof. Every atom of $\mathcal{Z}(M)$ is a circuit of M by Lemma 16. Since $d \geq 3$, M^* is simple and every coatom of $\mathcal{Z}(M)$ is the complement of a cocircuit. Therefore, by Theorem 12, we have that $|Z_a \cap (E - Z^c)| = |Z_a \setminus Z^c|$ is even. □

8. Matroids with lattices of cyclic flats of height 3

In this section, we study binary matroids when their lattice of cyclic flats has height 3. Under this assumption, every atom of $\mathcal{Z}(M)$ is also a coatom, which makes the structure of $\mathcal{Z}(M)$ very rigid. First, we focus on matroids of rank 2 and derive formulas that relate the nullity of the ground set, the number of atoms and the nullity of these atoms. Although technical, these formulas will be very useful in the next section when we study recursive structures in the lattice of cyclic flats.

Secondly, we extend the study of height-three lattices to binary matroids with arbitrary rank. It turns out that only a few binary simple matroids can have a lattice of cyclic flats of height 3. In this part, we prove the non-existence of simple matroids with lattice of cyclic flats of height 3 depending on the size and rank and give the complete classification of these matroids when $\eta(E)$ is greater than or equal to 3.

8.1. Matroids of rank 2 or nullity 2

We start by considering matroids of rank 2. For binary matroids, U_3^2 is the unique simple matroid of rank 2 that contains no isthmuses and has a lattice of cyclic flats of height 2. If the nullity of M is larger than 1, it implies that some elements are parallel and thus the lattice of cyclic flats has height 3. Using this fact, we can express the nullity of M depending on the nullity of the atoms and the number of atoms.

Lemma 21. *Let $M = (E, \rho)$ be a binary non-degenerate (n, k, d)-matroid with rank $k = 2$. Let $\Upsilon_\emptyset$ be the set of atoms of $\mathcal{Z}(M)$. Then, we have the following relations:*

- *If $\Upsilon_\emptyset = \{E\}$, then $\eta(E) = 1$.*
- *If $|\Upsilon_\emptyset| = 1$ and $\Upsilon_\emptyset \neq \{E\}$, then $\eta(E) = \eta(Z) + 1$ with $\{Z\} = \Upsilon_\emptyset$.*
- *If $|\Upsilon_\emptyset| = 2$ and $E = \bigcup_{Z \in \Upsilon_\emptyset} Z$, then $\eta(E) = \sum_{Z \in \Upsilon_\emptyset} \eta(Z)$.*
- *If $|\Upsilon_\emptyset| = 2$ and $E - \bigcup_{Z \in \Upsilon_\emptyset} Z \neq \emptyset$, then $\eta(E) = 1 + \sum_{Z \in \Upsilon_\emptyset} \eta(Z)$.*
- *if $|\Upsilon_\emptyset| = 3$, then $\eta(E) = 1 + \sum_{Z \in \Upsilon_\emptyset} \eta(Z)$.*

Proof. Let G be the matrix associated to the matroid M. Since G is a binary matrix of rank 2, there are only three possible choices for the columns of G, namely the vectors $\binom{1}{0}$, $\binom{0}{1}$ and $\binom{1}{1}$. Then, the size of E can be counted as $|E| = \#\binom{1}{0} + \#\binom{0}{1} + \#\binom{1}{1}$. Furthermore, every time one vector is repeated, it will create a cyclic flat of rank 1 in $\mathcal{Z}(M)$. Thus, if $\Upsilon_\emptyset$ is the set of these cyclic flats, we have

$$|E| = \sum_{Z \in \Upsilon_\emptyset} |Z| + |E - \bigcup_{Z \in \Upsilon_\emptyset} Z|.$$

Since we also know their rank, we can transform the previous equation into an equation on the nullity. Now splitting this equation depending on the value of $|\Upsilon_\emptyset|$ will give the result (notice that since we assume no isthmuses, $|\Upsilon_\emptyset| = 1$ forces the two other vectors to appear in G). □

More interestingly, the previous formulas can be generalized as local relations on arbitrary binary matroids. Indeed, if two cyclic flats have a rank difference of 2, we can use contraction and deletion to obtain a rank 2 matroid and apply Lemma 21. Furthermore, by minor properties, these relations can be directly expressed in M instead of in the minor obtained from M.

Lemma 22. *Let $M = (E, \rho)$ be a binary matroid and let $Z_1, Z_2 \in \mathcal{Z}(M)$ such that $Z_1 \subset Z_2$ and $\rho(Z_2) - \rho(Z_1) = 2$. Define $\Upsilon = \{Z : Z \in \mathcal{Z}(M),\ Z_1 \lessdot Z \lessdot Z_2\}$. Then, we have the following relations.*

- *If $|\Upsilon| = 0$, then $\eta(Z_2) = \eta(Z_1) + 1$.*
- *If $|\Upsilon| = 1$, then $\eta(Z_2) = \eta(Z) + 1$ with $\{Z\} = \Upsilon$.*
- *If $|\Upsilon| = 2$ and $Z_2 = \bigcup_{Z \in \Upsilon} Z$, then $\eta(Z_2) = \sum_{Z \in \Upsilon} \eta(Z) - \eta(Z_1)$.*
- *If $|\Upsilon| = 2$ and $Z_2 - \bigcup_{Z \in \Upsilon} Z \neq \emptyset$, then $\eta(Z_2) = 1 + \sum_{Z \in \Upsilon} \eta(Z) - \eta(Z_1)$.*
- *If $|\Upsilon| = 3$, then $\eta(Z_2) = 1 + \sum_{Z \in \Upsilon} \eta(Z) - 2\eta(Z_1)$.*

Proof. The minor $M|Z_2/Z_1$ is a binary non-degenerate matroid. Hence we can apply Lemma 21 with ground set $Z_2 - Z_1$ and nullity function $\eta_{M|Z_2/Z_1} = \eta_{M/Z_1}$. Now if $A \subset Z_2 - Z_1$, then $\eta_{M|Z_2/Z_1}(A) = \eta(A \cup Z_1) - \eta(Z_1)$. Using this with Lemma 21 will give the result. □

The next lemma is the dual version of the previous lemma.

Lemma 23. *Let $M = (E, \rho)$ be a binary matroid and let $Z_1, Z_2 \in \mathcal{Z}(M)$ be such that $Z_1 \subset Z_2$ and $\eta(Z_2) - \eta(Z_1) = 2$. Define $\Upsilon = \{Z : Z \in \mathcal{Z}(M),\ Z_1 \lessdot Z \lessdot Z_2\}$. Then, we have the following relations.*

- *If $|\Upsilon| = 0$, then $\rho(Z_2) = \rho(Z_1) + 1$.*

- *If* $|\Upsilon| = 1$, *then* $\rho(Z) = \rho(Z_1) + 1$ *with* $\{Z\} = \Upsilon$.
- *If* $|\Upsilon| = 2$ *and* $Z_1 = \bigcap_{Z \in \Upsilon} Z$, *then* $\sum_{Z \in \Upsilon} \rho(Z) = \rho(Z_1) + \rho(Z_2)$.
- *If* $|\Upsilon| = 2$ *and* $\left(\bigcap_{Z \in \Upsilon} Z \right) - Z_1 \neq \emptyset$, *then* $\sum_{Z \in \Upsilon} \rho(Z) = 1 + \rho(Z_1) + \rho(Z_2)$.
- *If* $|\Upsilon| = 3$, *then* $\sum_{Z \in \Upsilon} \rho(Z) = 1 + \rho(Z_1) + 2\rho(Z_2)$.

8.2. Matroids of arbitrary rank

In this part, we relax the condition on the rank while still forcing the lattice of cyclic flats to have height 3. We will see that, in fact, only a few simple binary matroids satisfy this condition and we will completely characterize them. We first treat the case when the matroids contain parallel elements.

Proposition 8. *Let* $M = (E, \rho)$ *be a binary non-degenerate* (n, k, d)*-matroid with* $k \geq 3$. *If* $\mathcal{Z}(M)$ *has height 3 and* M *contains parallel elements, then* $d = 2$.

Proof. Let $e \in E$ be one of the parallel elements. Since $\mathcal{Z}(M)$ has height 3, the lattice of cyclic flats contains the chain $\emptyset \lessdot \mathrm{cl}(e) \lessdot E$. Now $\rho(\mathrm{cl}(e)) = \rho(e) = 1$. Then we have that $\mathrm{cl}(e) \lessdot E$ is a rank edge, implying that $\eta(E) = \eta(\mathrm{cl}(e)) + 1$. Hence $d = \eta(E) + 1 - \max\{\eta(Z) : Z \in \mathcal{Z}(M) - E\} \leq \eta(E) + 1 - \eta(\mathrm{cl}(e)) = 2$, and since M is non-degenerate, we have $d = 2$. □

Thus, it is always possible to increase the nullity of M by adding parallel elements. However, if $\mathcal{Z}(M)$ has height 3, then the minimum distance is always equal to 2. We focus now on simple matroids and start by an upper bound on the intersection between two atoms.

Lemma 24. *Let* $M = (E, \rho)$ *be a binary simple* (n, k, d)*-matroid with no isthmuses and* $k \geq 3$. *If* $\mathcal{Z}(M)$ *has height 3 and for every atom* $Z \in \mathcal{Z}(M)$ *we have* $\rho(Z) = k - 1$, *then*

$$|Z_1 \cap Z_2| \leq \frac{k}{2}, \text{ for all } Z_1, Z_2 \in \mathcal{Z}(M) - E.$$

Proof. Let $Z_1, Z_2 \in \mathcal{Z}(M) - E$. If one of them is the empty set, then the result is trivial. Assume now that neither of them are empty. Since $\mathcal{Z}(M)$ has height 3, Z_1 and Z_2 must be atoms of $\mathcal{Z}(M)$ with parameters $\rho(Z_i) = k - 1$, $\eta(Z_i) = 1$ and $|Z_i| = k$ for $1 \leq i \leq 2$. Furthermore, Z_1 and Z_2 are also circuits in M. By Theorem 12, $Z_1 \triangle Z_2$ is a disjoint union of circuits. Using the fact that $Z_1 \cup Z_2 = Z_1 \triangle Z_2 \uplus Z_1 \cap Z_2$, we have that

$$|Z_1 \triangle Z_2| = |Z_1 \cup Z_2| - |Z_1 \cap Z_2| = |Z_1| + |Z_2| - 2|Z_1 \cap Z_2| = 2k - 2|Z_1 \cap Z_2|.$$

Now the smallest size of a circuit in M is k, since otherwise a circuit C of size less than k will yield a cyclic flat $\mathrm{cl}(C)$ of $\mathcal{Z}(M)$ of rank less than $k-1$, and thus contradict our assumptions. This implies that $|Z_1 \triangle Z_2| \geq k$ and hence $|Z_1 \cap Z_2| \leq \frac{k}{2}$. □

We now prove one of the main results of this section. The next proposition states the non-existence of simple matroids with lattice of cyclic flats of height 3 and large rank and nullity. In fact, as soon as the rank is larger than or equal to 5, the only possible such matroids have nullity 2 and thus need to satisfy the relations in Lemma 23.

Proposition 9. *Let $M = (E, \rho)$ be a binary simple (n, k, d)-matroid with no isthmuses. If $\mathcal{Z}(M)$ has height 3 and $k \geq 5$, then $\eta(E) = 2$ and $d = 2$.*

Proof. If there exists $Z \in \mathcal{Z}(M) - \emptyset$ with $\rho(Z) < k-1$, then $Z \lessdot E$ is a rank edge and $\eta(E) = \eta(Z) + 1 = 2$.

Assume now that every atom of $\mathcal{Z}(M)$ has rank $k-1$ and assume for a contradiction that $\eta(E) > 2$. The goal is to use Theorem 11 and Corollary 7 to obtain a contradiction on the fact that M is binary.

Let Z_a be an atom of $\mathcal{Z}(M)$. Remember that $\rho(Z_a) = k-1$ and $|Z_a| = k$. Choose $F \subset Z_a$ with $|F| = k-2$. Since the smallest size of a circuit is k, we have that $F \in \mathcal{F}(M)$ and is independent. Since $1_{\mathcal{Z}} = E$, using $\Upsilon(F)$ as defined in Definition 9 we have

$$\begin{aligned}\Upsilon(F) &= \{X \in \mathcal{Z}(M) : \rho(E) - 1 = \rho(X) + |F - X|\} \\ &= \{X \in \mathcal{Z}(M) - E : k - 1 = k - 1 + |F - X|\} \\ &= \{X \in \mathcal{Z}(M) - E : F \subset X\}.\end{aligned}$$

By Lemma 24, if X and X' are both atoms of $\mathcal{Z}(M)$, then $|X \cap X'| \leq \frac{k}{2}$. Since $k \geq 5$, we have $k - 2 > \frac{k}{2}$. This implies that Z_a is the unique cyclic flat different from E that contains F. Hence $\Upsilon(F) = \{Z_a\}$. By Theorem 11 and since $\eta(E) > 2$, we have

$$|(F, E)_{\mathcal{F}}| = |E - F| - |Z_a - F| + 1 = n - k + 1 \geq 4.$$

Therefore, by Corollary 7, M is not binary, which contradicts our assumption. Thus, we have $\eta(E) \leq 2$. Since there exist atoms with nullity equal to 1, we get $\eta(E) = 2$. Finally, the minimum distance is given by $d = \eta(E) + 1 - \max\{\eta(Z) : Z \in \mathcal{Z}(M) - E\} = 2$. □

The next proposition goes further by giving an upper bound on the nullity when the rank is equal to 4.

Proposition 10. *Let $M = (E, \rho)$ be a binary simple (n, k, d)-matroid with no isthmuses and $k = 4$. If $\mathcal{Z}(M)$ has height 3 then $n \leq 8$ or equivalently, $\eta(E) \leq 4$.*

Proof. If there exists $Z \in \mathcal{Z}(M) - \emptyset$ with $\rho(Z) < k-1$, then $Z \lessdot E$ is a rank edge and $\eta(E) = \eta(Z) + 1 = 2$.

Assume now that every atom of $\mathcal{Z}(M)$ has rank $k-1$. Let $F \subset E$ such that $|F| = k-2$. Since the smallest size of a circuit is k, we have that $F \in \mathcal{F}(M)$ and is independent. By the same argument as in the proof of Proposition 9, we get that

$$\Upsilon(F) = \{X \in \mathcal{Z}(M) - E : F \subset X\}.$$

By Theorem 11 and since $k = 4$, we have

$$|(F, E)_{\mathcal{F}}| = |E - F| - \sum_{Z \in \Upsilon(F)} (|Z - F| - 1) = n - 2 - |\Upsilon(F)|.$$

By Corollary 7, we need $n - 2 - |\Upsilon(F)| \leq 3$ or equivalently $n \leq 5 + |\Upsilon(F)|$. On the other hand, we have $n \geq |F| + |\Upsilon(F)| \cdot 2$. By combining the two equations, we get

$$2 + 2|\Upsilon(F)| \leq 5 + |\Upsilon(F)| \iff |\Upsilon(F)| \leq 3.$$

Hence we obtain $n \leq 8$. □

The previous propositions restrict the candidates for simple and cosimple matroids with height-three lattices to $k \leq 4$ and $n \leq 8$. We pursue by studying the structure of the lattice of cyclic flats of simple matroids with feasible size and rank. In particular, we prove that matroids satisfying these conditions are unique up to isomorphism.

Proposition 11. *Up to isomorphism, there is a unique binary simple* $(6, 3, 3)$*-matroid with no isthmuses.*

Proof. Let $M = (E, \rho)$ be a binary simple $(6, 3, 3)$-matroid with no isthmuses. We start by proving that $\mathcal{Z}(M)$ has a unique configuration by counting the number of atoms.

Since M is simple with $k = 3$ and $\eta(E) = 3$, $\mathcal{Z}(M)$ has height 3 by Lemma 15. Let Z_a be an atom of $\mathcal{Z}(M)$. We have $\rho(Z_a) = 2$, $\eta(Z_a) = 1$, and $|Z_a| = 3$. As the size of an atom is odd, by Lemma 20 and Lemma 24 for all atoms Z_1 and Z_2, we have $Z_1 \cap Z_2 = 1$. Since $|Z_1 \cup Z_2| \leq 5$, but $|E| = 6$ and since there always exists an atom for every coordinate by Lemma 19, the number of atoms is at least 3.

Denote by Z_1, Z_2, and Z_3 the first three atoms. Notice that they have to intersect pairwise in a different element because $|E| = 6$. We have $|Z_1 \Delta Z_2 \Delta Z_3| = 3$. Then, by Theorem 12 on the symmetric difference, these three elements form an extra atom. Hence, the number of atoms is at least 4. Now the number of atoms is upper bound by $\binom{6}{2}/3 = 5$ since every pair will define a unique atom with 3 elements. However we cannot have 5 atoms. Indeed, by the inclusion–exclusion principle, we would have

$$\left| \bigcup_{i=1}^{5} Z_i \right| = 5|Z_1| - 10|Z_1 \cap Z_2| = 5$$

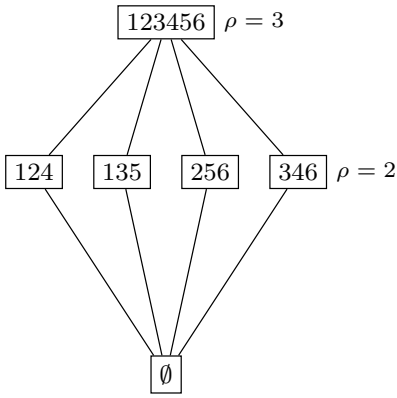

Fig. 4. Lattice of cyclic flats of the binary $(6, 3, 3)$-matroid.

because every triple has an empty intersection. But this is not possible since already $|Z_1 \cup Z_2 \cup Z_3| = |E| = 6$. Hence, $\mathcal{Z}(M)$ has 4 atoms and has a unique configuration.

Now suppose $E = \{a, b, c, d, e, f\}$ and $Z_1 = \{a, b, c\}$. By the previous part, we have $|Z_1 \cap Z_i| = 1$ for all $i \in \{2, 3, 4\}$ with a different element for each intersection. So, let $a \in Z_2, b \in Z_3$ and $c \in Z_4$. We complete Z_2 with some of the remaining elements to get $Z_2 = \{a, d, e\}$. Since $|Z_2 \cap Z_3| = 1$, we choose $d \in Z_3$. The only possible choice for the last element in Z_3 is therefore f and we have $Z_3 = \{b, d, f\}$. Finally Z_4 has a non-trivial intersection with Z_2 and Z_3 so it has to be $Z_4 = \{c, e, f\}$. Hence we have uniquely reconstructed the lattice of cyclic flats up to a permutation of the groundset which implies that M is unique up to isomorphism. □

Fig. 4 displays the lattice of cyclic flats of the binary $(6, 3, 3)$-matroid with generator matrix

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

This is isomorphic to the graphical matroid $M(K_4)$ associated to the complete graph on four nodes.

The second simple matroid of rank 3 that has a lattice of cyclic flats of height 3 is the Fano plane F_7. Its associated code is the simplex $(7, 3, 4)$-code where the generator matrix contains every possible column except the all-zero column. By construction, it is unique given its parameters $(n, k, d) = (7, 3, 4)$, and it has the maximum number of atoms which is $\binom{7}{2}/3 = 7$. Its dual F_7^* is associated to the $(7, 4, 3)$ Hamming code, which also has a lattice of cyclic flats of height 3 with 7 atoms.

Finally, we study the last possible set of parameters.

Proposition 12. *There is a unique, up to isomorphism, binary simple* $(8, 4, 4)$*-matroid with no isthmuses.*

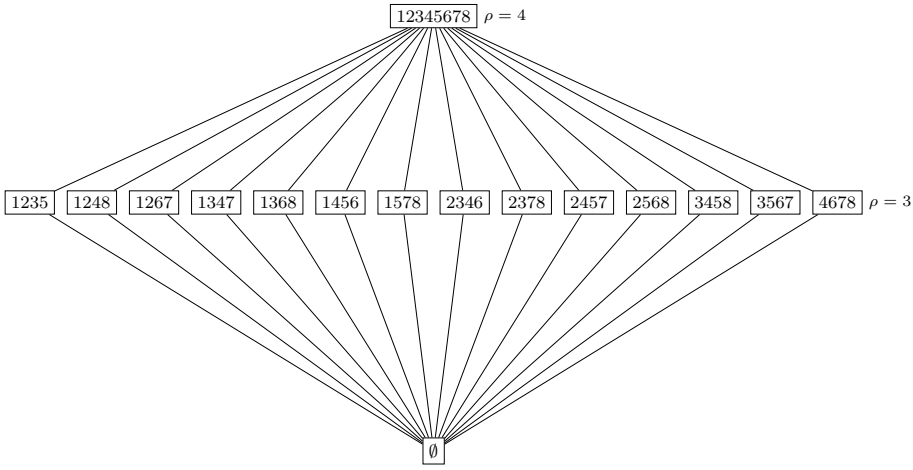

Fig. 5. Lattice of cyclic flats of the binary $(8, 4, 4)$-matroid.

Proof. Let $M = (E, \rho)$ be a binary simple $(8, 4, 4)$-matroid with no isthmuses. All coatoms in $\mathcal{Z}(M)$ must then have nullity at most $8 - 4 = 4$, and by Lemma 15, they also have rank 3. It follows that all coatoms have rank 3 and size 4, and are thus also atoms, so $\mathcal{Z}(M)$ has height three. We again start by proving that $\mathcal{Z}(M)$ has a unique configuration by counting the number of atoms.

Let $e \in E$. The number of atoms can be split into two groups: the set A of atoms containing e and the set B of atoms not containing e. By Theorem 6, the number of nontrivial cyclic flats containing e is at least the number of nontrivial cyclic flats in $\mathcal{Z}(M/\{e\})$. Since M/e is isomorphic to the $(7, 3, 4)$-matroid, we have that $|A| \geq 7$. Now $|B|$ is at least the number of atoms in $\mathcal{Z}(M|(E - \{e\}))$. The matroid $M|(E - \{e\})$ is isomorphic to the $(7, 4, 3)$-matroid which also contains 7 non-trivial cyclic flats so $|B| \geq 7$. As the total number of atoms in an $(8, 4, 4)$-matroid cannot exceed $\binom{8}{3}/4 = 14$, $\mathcal{Z}(M)$ indeed contains 14 atoms and has a unique configuration. Furthermore, M is also the unique extension by one element of the Simplex $(7, 3, 4)$-matroid such that the contraction M/e yields again the Simplex matroid and the deletion $M \setminus e$ yields the dual of this Simplex matroid, the $(7, 4, 3)$-matroid. □

This $(8, 4, 4)$-matroid is known as the affine geometry of rank 4 over F_2, denoted AG$(3, 2)$ in Oxley's notation. The corresponding binary code is the Reed–Muller code RM$(1, 3)$. The lattice of cyclic flats is displayed in Fig. 5 with the generator matrix

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

We can now summarize the previous results.

Theorem 14. *Let $M = (E, \rho)$ be a binary simple (n, k, d)-matroid with no isthmuses. If $\mathcal{Z}(M)$ has height 3, then either $\eta(E) = 2$ or M is isomorphic to one of the matroids listed below:*

- $M(K_4)$ — *a $(6, 3, 3)$-matroid with 4 atoms.*
- F_7 — *a $(7, 3, 4)$-matroid with 7 atoms.*
- F_7^* — *a $(7, 4, 3)$-matroid with 7 atoms.*
- $AG(3, 2)$ — *a $(8, 4, 4)$-matroid with 14 atoms.*

Corollary 9. *Let $M = (E, \rho)$ be a binary simple matroid with no isthmuses. If $\mathcal{Z}(M)$ has height 3 then $\eta(E) \leq 4$ and $d \leq 4$.*

9. Recursive structure on coatoms level

This section is devoted to understanding the consequences of the minimum distance to the shape of the top part of the lattice of cyclic flats. We already saw in Lemma 15 that requiring the minimum distance to be greater than 2 forces all coatoms to have the same rank. Let us give this property a name for an arbitrary cyclic flat.

Definition 10. A cyclic flat Z of a binary matroid M is *blunt* if for all $Z' \in \mathcal{Z}(M)$ such that $Z' \lessdot Z$, we have $\rho(Z') = \rho(Z) - 1$. In other words, every covering relation of a blunt cyclic flat is either a nullity edge or an elementary edge.

Thus, for a binary matroid $M = (E, \rho)$, E being blunt is a necessary condition to have $d \geq 3$. In this section, we study how the value of the minimum distance creates a recursive structure consisting of blunt cyclic flats in $\mathcal{Z}(M)$. In the second part, we state the equivalent notion of residual codes for binary matroids, which naturally leads to a version of the Griesmer bound for binary matroids. Finally, we discuss the relation between coatoms of $\mathcal{Z}(M)$ and codewords of the associated linear code. Before we begin, let us fix some notation.

Notation 1. We will usually denote a coatom by a superscripted Z such as Z^1 or Z^c. If $M = (E, \rho)$ is an (n, k, d)-matroid, then Z^d denotes a cyclic flat with maximal nullity, *i.e.*, we have $d = \eta(E) + 1 - \eta(Z^d)$. Notice that if $\rho(Z^d) = k - 1$, we have $|Z^d| = n - d$.

9.1. Existence of rank $k - 2$ cyclic flats and recursive structure

In order to get a recursive structure consisting of blunt cyclic flats, we are interested in the level below the coatoms level and in particular, in the cyclic flats of rank $k - 2$.

Proposition 13. *Let $M = (E, \rho)$ be a binary non-degenerate (n, k, d)-matroid and let $Z^d \in \mathcal{Z}(M)$ be a coatom with maximal nullity. If Z^d is not blunt, then $d \leq 4$.*

Proof. First, notice that if E is not blunt then $d = 2$ by Lemma 15. Assume now that all coatoms have a rank equal to $k-1$. Since Z^d is not blunt, there exists a $Z_1 \in \mathcal{Z}(M)$ such that $Z_1 \lessdot Z^d$ and $\rho(Z_1) < \rho(Z^d) - 1 = k - 2$.

Now the proof is a direct consequence of the classification of simple matroids with lattice of cyclic flats of height 3 in Section 8. Indeed, we will prove that M/Z_1 is simple with no isthmuses and its lattice of cyclic flats has height 3.

Since $Z_1 \lessdot Z^d$ is a rank edge, we have $\eta(Z^d) = \eta(Z_1) + 1$. This implies that if Z^1 is a cyclic flat such that $Z_1 \lessdot Z^1$, then Z^1 is a coatom with $\rho(Z^1) = k-1$ because otherwise, there is a coatom Z^2 of $\mathcal{Z}(M)$ that covers Z^1 and $\eta(Z^2) \geq \eta(Z_1) + 2$, which contradicts the fact that $\eta(Z^d)$ is maximal. Hence, by Theorem 6, $\mathcal{Z}(M/Z_1)$ has height 3.

The matroid M/Z_1 is also simple with no isthmuses as the contraction by a cyclic flat will not create any loops or isthmuses. Plus, for all coatoms $Z^c \in \mathcal{Z}(M)$ with $Z_1 \lessdot Z^c$, we have $\rho(Z^c) - \rho(Z_1) \geq k - 1 - (k-3) = 2$, which means that there are no parallel elements in M/Z_1. Thus, M/Z_1 corresponds to the type of lattice studied in Section 8.

Finally, to prove the proposition, we link the minimum distance d to the minimum distance of M/Z_1. We have

$$\begin{aligned} d_{M/Z_1} &= \eta_{M/Z_1}(E - Z_1) + 1 - \max\{\eta_{M/Z_1}(\tilde{Z}) : \tilde{Z} \in \mathcal{Z}(M/Z_1) - (E - Z_1)\} \\ &= \eta(E) - \eta(Z_1) + 1 - \max\{\eta(Z - Z_1) : Z \in \mathcal{Z}(M) - E \text{ and } Z_1 \subseteq Z\} \\ &= \eta(E) - \eta(Z_1) + 1 - \max\{\eta(Z) : Z \in \mathcal{Z}(M) - E \text{ and } Z_1 \subseteq Z\} + \eta(Z_1) \\ &= \eta(E) + 1 - \eta(Z^d) \\ &= d. \end{aligned}$$

Hence, by the classification obtained in Section 8 and, in particular, by Corollary 9, we have $d = d_{M/Z_1} \leq 4$. □

We now present two examples where no coatoms are blunt and the matroids have minimum distance 3 and 4 respectively.

Example 2. Let M be the binary $(10, 6, 3)$-matroid obtained by the dual of the complete graph K_5 and G the following generator matrix of M:

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

We can see that there is no cyclic flat of rank 4, since if Z_a is an atom of $\mathcal{Z}(M)$ then the contracted matroid M/Z_a is isomorphic to the $(6, 3, 3)$-matroid having a lattice of cyclic flats of height 3. The configuration of the lattice of cyclic flats is displayed in Fig. 6.

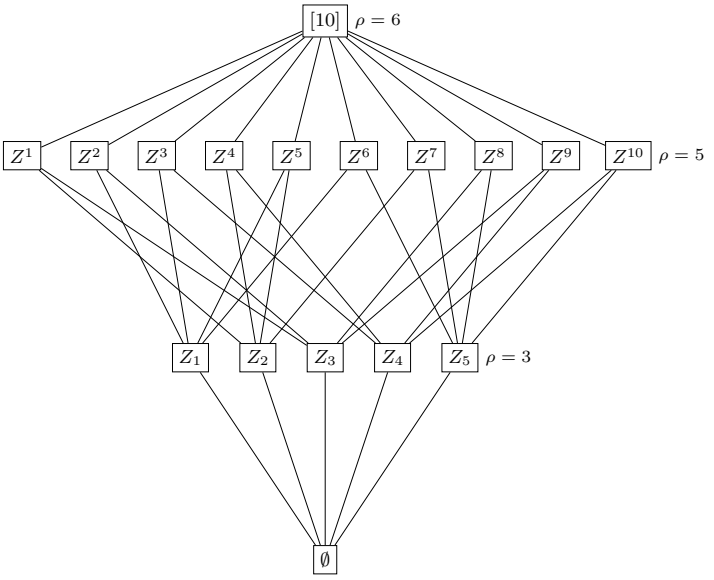

Fig. 6. Configuration of the lattice of cyclic flats of $M^*(K_5)$.

Example 3. The second example is the binary Reed–Muller code RM$(2,4)$ giving a $(16,11,4)$-matroid. Here, all atoms of $\mathcal{Z}(M)$ have rank 7 and if Z_a is one of them, then the contracted matroid M/Z_a is isomorphic to the $(8,4,4)$-matroid, which has a lattice of cyclic flats of height 3. Thus, there are no cyclic flats of rank 9.

Now, we extend Proposition 13 to coatoms with different size, *i.e.*, bound the minimum distance when there is a coatom $Z^c \in \mathcal{Z}(M)$ which is not blunt. We emphasize that while coatoms $Z^d \in \mathcal{Z}(M)$ with maximal nullity always exist, coatoms with size less than Z^d might not exist. For example, matroids coming from Simplex codes have only coatoms with maximal size. However, depending on the parameters (n,k,d), we can use some techniques to guarantee the existence of smaller coatoms as demonstrated in Example 4.

We start by giving a lower bound on the number of coatoms of $\mathcal{Z}(M)$ covering a cyclic flat of rank $k-2$ when $d \geq 3$.

Lemma 25. *Let $M = (E,\rho)$ be a binary non-degenerate (n,k,d)-matroid with $d \geq 3$, Z_1 a cyclic flat with $\rho(Z_1) = k-2$ and Υ_{Z_1} the set of coatoms covering Z_1. Then we have $|\Upsilon_{Z_1}| \geq 2$.*

Proof. If $d \geq 3$, then Corollary 8 states that $\mathcal{Z}(M)$ is co-atomic. Thus, there are at least two coatoms that cover a rank-$(k-2)$ cyclic flat. □

We can now formulate an upper bound on d when a coatom $Z^c \in \mathcal{Z}(M)$ is not blunt. The bound is expressed in terms of the gap between the nullity of Z^c and the maximal nullity of a coatom, or equivalently, between their size difference.

Proposition 14. *Let $M = (E, \rho)$ be a binary non-degenerate (n, k, d)-matroid with $d \geq 3$ and $Z^d \in \mathcal{Z}(M)$ be such that $|Z^d| = n - d$. If there exists a coatom $Z^c \in \mathcal{Z}(M)$ not blunt with $|Z^c| < |Z^d|$, then*

$$d \leq 2(\eta(Z^d) - \eta(Z^c) + 1) = 2(|Z^d| - |Z^c| + 1).$$

Proof. Since Z^c is not blunt, there exists a cyclic flat $Z_1 \lessdot Z^c$ with $\rho(Z_1) < k - 2$. If there are no cyclic flats of rank $k-2$ that contain Z_1, then let Z_m be the biggest cyclic flat with respect to the rank that contains Z_1 and is below a coatom, *i.e.*, if $Z' \in \mathcal{Z}(M)$ is such that $Z_1 \subseteq Z'$ then either $\rho(Z') \geq k - 1$ or $\rho(Z') \leq \rho(Z_m)$. Now, by the same arguments as in the proof of Proposition 13, M/Z_m is simple with no isthmuses and has a lattice of cyclic flats of height 3. Therefore, by Corollary 9 we have $d \leq d_{M/Z_m} \leq 4$.

Suppose now that there exists $Z_2 \in \mathcal{Z}(M)$ such that $Z_1 \subset Z_2$ and $\rho(Z_2) = k - 2$. We can apply Lemma 22 to get a bound on the minimum distance d. Let Υ_{Z_2} be the set of coatoms containing Z_2. By Lemma 25, we have $|\Upsilon_{Z_2}| \geq 2$ which reduces the possible cases in Lemma 22. We also use the fact that since $\eta(Z_1) = \eta(Z^c) - 1$, we have $\eta(Z_2) \geq \eta(Z^c)$.

1. If $|\Upsilon_{Z_2}| = 3$, then we have

$$\eta(E) = 1 + \sum_{Z \in \Upsilon_{Z_2}} \eta(Z) - 2\eta(Z_2) \leq 1 + 3\eta(Z^d) - 2\eta(Z^c) \iff$$
$$\eta(E) + 1 - \eta(Z^d) \leq 2(\eta(Z^d) - \eta(Z^c) + 1) \iff$$
$$d \leq 2(\eta(Z^d) - \eta(Z^c) + 1).$$

2. If $|\Upsilon_{Z_2}| = 2$ and $E - (\bigcup_{Z \in \Upsilon_{Z_2}} Z) \neq \emptyset$, then we have

$$\eta(E) = 1 + \sum_{Z \in \Upsilon_{Z_2}} \eta(Z) - \eta(Z_2) \leq 1 + 2\eta(Z^d) - \eta(Z^c) \iff$$
$$d \leq 2 + (\eta(Z^d) - \eta(Z^c)).$$

3. if $|\Upsilon_{Z_2}| = 2$ and $E = \bigcup_{Z \in \Upsilon_{Z_2}} Z$, then we have

$$\eta(E) = \sum_{Z \in \Upsilon_{Z_2}} \eta(Z) - \eta(Z_2) \leq 2\eta(Z^d) - \eta(Z^c) \iff$$
$$d \leq 1 + (\eta(Z^d) - \eta(Z^c)).$$

Hence, the general upper bound for d is the largest of the three bounds obtained above and we have indeed that $d \leq 2(\eta(Z^d) - \eta(Z^c) + 1)$. □

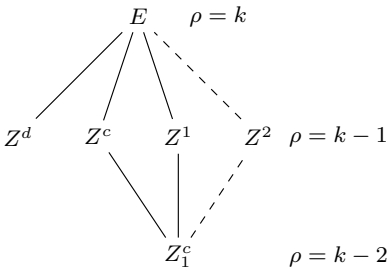

Fig. 7. Illustration of the hypotheses in Lemma 26.

The strength of this proposition does not really reside in the bound on the minimum distance but in its contrapositive as it gives a sufficient condition for a coatom of $\mathcal{Z}(M)$ to be blunt. In order to extend the bluntness property into a recursive structure, we study the minimum distance of $M|Z^c$, the matroid restricted to a coatom $Z^c \in \mathcal{Z}(M)$. We start by a technical lemma which relates $d_{M|Z^c}$, d, and the nullity of certain coatoms of $\mathcal{Z}(M)$. The hypotheses of the next lemma are illustrated in Fig. 7.

Lemma 26. *Let $M = (E, \rho)$ be a binary non-degenerate (n, k, d)-matroid with $d \geq 3$ and Z^d a cyclic flat with maximal nullity. Let $Z^c \in \mathcal{Z}(M)$ be a blunt coatom with rank $\rho(Z^c) = k-1$, $Z_1^c \in \mathcal{Z}(M)$ such that $d_{M|Z^c} = \eta(Z^c) + 1 - \eta(Z_1^c)$, and $\Upsilon_{Z_1^c}$ the set of coatoms containing Z_1^c. We denote the coatoms in $\Upsilon_{Z_1^c}$ by Z^c, Z^1 and if it exists, by Z^2.*

Then, $d_{M|Z^c}$ satisfies one of the following.

1. *If $|\Upsilon_{Z_1^c}| = 3$, then $2d_{M|Z^c} = d + \eta(Z^d) + \eta(Z^c) - (\eta(Z^1) + \eta(Z^2))$.*
2. *If $|\Upsilon_{Z_1^c}| = 2$ and $E - (Z^c \cup Z^1) \neq \emptyset$, then $d_{M|Z^c} = d - 1 + \eta(Z^d) - \eta(Z^1)$.*
3. *If $|\Upsilon_{Z_1^c}| = 2$ and $E = Z^c \cup Z^1$, then we have $d_{M|Z^c} = d + \eta(Z^d) - \eta(Z^1)$.*

Proof. Since Z^c is blunt, we have that $\rho(Z_1^c) = k-2$ and we can use Lemma 22. We check all possible cases in Lemma 22 depending on $\Upsilon_{Z_1^c}$. Notice that by Lemma 25, we have $|\Upsilon_{Z_1^c}| \geq 2$.

1. If $|\Upsilon_{Z_1^c}| = 3$, then we have

$$\eta(E) = 1 + \eta(Z^c) + \sum_{Z \in \Upsilon_{Z_1^c} - Z^c} \eta(Z) - 2\eta(Z_1^c)$$

$$\iff$$

$$d_{M|Z^c} = \eta(E) - \eta(Z^d) + \eta(Z^d) - \sum_{Z \in \Upsilon_{Z_1^c} - Z^c} \eta(Z) + \eta(Z^c) - \eta(Z^c) + \eta(Z_1^c)$$

$$\iff$$

$$d_{M|Z^c} = d - 1 + \eta(Z^d) - \sum_{Z \in \Upsilon_{Z_1^c} - Z^c} \eta(Z) + \eta(Z^c) - (d_{M|Z^c} - 1)$$

$$\iff$$

$$2d_{M|Z^c} = d + \eta(Z^d) + \eta(Z^c) - (\eta(Z^1) + \eta(Z^2)).$$

2. If $|\Upsilon_{Z_1^c}| = 2$ and $E - (Z^c \cup Z^1) \neq \emptyset$, then we have

$$\begin{aligned} \eta(E) = 1 + \eta(Z^c) + \eta(Z^1) - \eta(Z_1^c) &\iff \\ d_{M|Z^c} = \eta(E) - \eta(Z^d) + \eta(Z^d) - \eta(Z^1) &\iff \\ d_{M|Z^c} = d - 1 + \eta(Z^d) - \eta(Z^1). & \end{aligned}$$

3. if $|\Upsilon_{Z_1^c}| = 2$ and $E = Z^c \cup Z^1$, then we have

$$\begin{aligned} \eta(E) = \eta(Z^c) + \eta(Z^1) - \eta(Z_1^c) &\iff \\ d_{M|Z^c} = d + \eta(Z^d) - \eta(Z^1). \quad \square & \end{aligned}$$

From the previous lemma, we can derive a lower bound on $d_{M|Z^c}$, which is easier to estimate.

Proposition 15. *Let $M = (E, \rho)$ be a binary non-degenerate (n, k, d)-matroid and $Z^d \in \mathcal{Z}(M)$ a cyclic flat with maximal nullity. If $Z^c \in \mathcal{Z}(M)$ is a blunt coatom of rank $k-1$, then*

$$d_{M|Z^c} \geq \frac{d - (\eta(Z^d) - \eta(Z^c))}{2}.$$

Proof. Since Z^c is a cyclic flat, we have directly that $d_{M|Z^c} \geq 2$. Now if $d = 2$, we have

$$\frac{2 - (\eta(Z^d) - \eta(Z^c))}{2} \leq 1 \leq d_{M|Z^c}.$$

If $d \geq 3$, this proposition is a direct consequence of the previous Lemma 26. Namely, for all $Z \in \mathcal{Z}(M) - E$ we have $\eta(Z) \leq \eta(Z^d)$. By replacing the unknown nullities in Lemma 26 with $\eta(Z^d)$, we get three lower bounds on $d_{M|Z^d}$. Therefore, the general bound is the smallest lower bound, which is when $|\Upsilon_{Z_1^c}| = 3$ and $d_{M|Z^c} \geq \frac{d-(\eta(Z^d)-\eta(Z^c))}{2}$. $\square$

The contrapositives of Propositions 13 and 14 reveal how the minimum distance forces many coatoms $Z^c \in \mathcal{Z}(M)$ to be blunt. Now, given the lower bound on the minimum distance $d_{M|Z^c}$ provided by Proposition 15, we can apply again Propositions 13 and 14 to the restricted matroid $M|Z^c$ leading to more blunt cyclic flats. By repeating this process, we obtain decreasing chains of blunt cyclic flats with upper bounded nullity in $\mathcal{Z}(M)$. The next example illustrates the strength of Propositions 14 and 15 for the study of the lattice of cyclic flats together with specific techniques on the relation between the nullity and the minimum distance.

Example 4. Let $M = (E, \rho)$ be a binary simple $(11, 4, 5)$-matroid. Since the minimum distance is equal to 5, we know by Lemma 15 that E is blunt and all coatoms have rank 3. Moreover, by Proposition 5 there is a coatom $Z^d \in \mathcal{Z}(M)$ with size 6 and rank 3. By Proposition 13, Z^d is blunt and $\eta(Z^d) = 3 > 1$. Proposition 15 implies that $d_{M|Z^d} \geq \lceil \frac{d}{2} \rceil = 3$. Since the maximal minimum distance for a $(6, 3, d_{M|Z^d})$ matroid is 3, we have directly that $d_{M|Z^d} = 3$. Now by Theorem 14, $M|Z^d$ is isomorphic to the $(6, 3, 3)$-matroid studied in Section 8. Therefore, there are exactly 4 cyclic flats contained in Z^d with size 3 and rank 2.

Let $Z_1^d \in \mathcal{Z}(M)$ be such that $Z_1^d \lessdot Z^d$. We can apply Lemma 26 to obtain the nullity of the other coatoms containing Z_1^d. Indeed, since $d_{M|Z^d} = 3 < d - 1 = 4$, we know by Lemma 26 that $\Upsilon_{Z_1^d}$, the set of coatoms containing Z_1^d, has size $|\Upsilon_{Z_1^d}| = 3$. Let Z^1 and Z^2 be the two other coatoms in $\Upsilon_{Z_1^d}$. The first formula in Lemma 26 simplifies as $\eta(Z^1) + \eta(Z^2) = 5$. Now the maximal nullity of a coatom is $\eta(Z^d) = 3$. Thus we have $\eta(Z^1) = 3$ and $\eta(Z^2) = 2$. Hence, there exist coatoms with size 5 and rank 3. Now we know that Z^2 properly contains a cyclic flat, namely Z_1^d, and any such cyclic flat must have nullity 1, so

$$d_{M|Z^2} = \eta(Z^2) + 1 - \max_{Z < Z^2} \eta(Z) = 2.$$

In summary, M contains at least 5 different cyclic flats $(6, 3, 3)$, 4 cyclic flats $(5, 3, 2)$ and 8 atoms $(2, 1, 2)$. It is, in fact, possible to obtain the remaining cyclic flats by using some arguments about the intersection between two coatoms but this is rather long and mostly specific to this particular example. We can now double check our results by finding a particular generator matrix for M and displaying the lattice of cyclic flats. Let G be the following matrix:

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

The matroid $M(G)$ is indeed a simple $(11, 4, 5)$-matroid and its lattice of cyclic flats is displayed in Fig. 8.

9.2. Residual codes and the Griesmer bound

The final part of this section is dedicated to reformulating two notions in coding theory known as residual codes and the Griesmer bound for binary matroids. For more information about these two notions, we refer the reader to [10, Section 2.7]. The main result is an extension of Proposition 15 to arbitrary binary matroids which is the exact correspondent of the existence of residual codes for binary linear codes. As a direct consequence, we obtain the Griesmer bound for binary matroids.

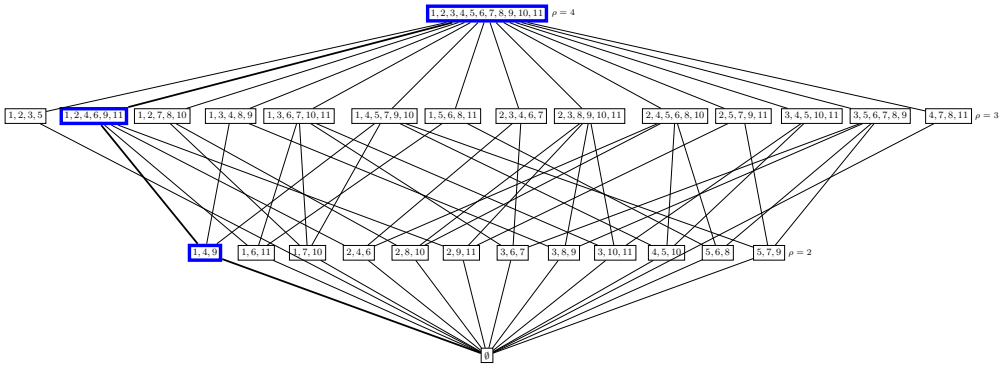

Fig. 8. Lattice of cyclic flats of the binary $(11, 4, 5)$-matroid from Example 4.

Theorem 15. *If $M = (E, \rho)$ is a binary (n, k, d)-matroid, then there exists $A \subset E$ such that $M|A$ is a binary $(n - d, k - 1, d')$-matroid with $d' \geq \frac{d}{2}$.*

Corollary 10. *For a binary (n, k, d)-matroid, we have*

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil .$$

We start by the proof of Theorem 15.

Proof. Let $M = (E, \rho)$ be a binary (n, k, d)-matroid. We separate the proof into three cases in which we give an explicit construction of the set A with the required parameters. Notice that the covering relations of the lattice $\mathcal{Z}(M)$ are not affected by the existence of loops nor is the minimum distance since the nullity of all cyclic flats increases evenly by the number of loops. Thus, without loss of generality, we assume that M contains no loops. Notice also that if M contains no isthmuses then the restriction to a cyclic flat will not create any isthmuses.

1. Suppose M contains no isthmuses and $d \geq 3$. Let $Z^d \in \mathcal{Z}(M)$ with $|Z^d| = n - d$.
   - If Z^d is blunt, then Proposition 15 guarantees that $d_{M|Z^d} \geq \frac{d}{2}$. Thus, we can choose $A = Z^d$.
   - If Z^d is not blunt, then Lemma 15 implies that $d_{M|Z^d} = 2$. By Proposition 13, we have $d \leq 4$. So indeed $d_{M|Z^d} \geq \frac{d}{2}$ and we can choose $A = Z^d$.
2. Suppose M contains no isthmuses and $d = 2$.
   - If there exists $Z^d \in \mathcal{Z}(M)$ with maximal nullity and $\rho(Z^d) = k-1$, then $|Z^d| = n-d$ and $d_{M|Z^d} \geq 2$. So indeed $d_{M|Z^d} \geq \frac{d}{2} = 1$ and we can choose $A = Z^d$.
   - Assume there is no such Z^d. Let Z be such that $Z \lessdot E$ and $\eta(Z) = \eta(E) + 1 - d = \eta(E) - 1$. Now M/Z is isomorphic to a uniform matroid U^m_{m+1} with $m = k - \rho(Z)$. This implies that if $B \subset E - Z$ with $|B| = m-1$, then $\rho(Z \cup B) = \rho(Z) + |B| = k-1$. We also have that $|Z \cup B| = |Z| + |B| = \rho(Z) + \eta(Z) + m - 1 = k - 1 + \eta(E) - 1 =$

$n-2=n-d$. Finally, the minimum distance is $d_{M|Z\cup B}=1=\frac{d}{2}$. Thus, we can choose $A=Z\cup B$.

3. Finally, suppose M contains some isthmuses. This implies that the minimum distance d is equal to 1. Let H be a hyperplane of M. H has parameters $\rho(H)=k-1$, $|H|=n-1$, and $d_{M|H}\geq 1\geq\frac{d}{2}$. Thus, we can choose $A=H$. □

We give a proof of Corollary 10 for completeness. This proof follows a standard proof of the Griesmer bound by using residual codes as in [10, Theorem 2.7.4].

Proof. Notice first that if $d_{M|Z}\geq\frac{d}{2}$ then $d_{M|Z}\geq\lceil\frac{d}{2}\rceil$. We will now prove the statement by induction on k.

If $k=1$, then the conclusion is trivial since it says that $n\geq d$. Let $k>1$ and assume that the statement is true for any binary matroid with rank $k-1$. By Theorem 15, there exists a subset $A\subset E$ such that $M|A$ has size $n-d$, dimension $k-1$ and minimum distance $d_{M|A}\geq\lceil\frac{d}{2}\rceil$. By applying the induction hypothesis on $M|A$, we have

$$n-d\geq\sum_{i=0}^{k-2}\left\lceil\frac{d_{M|A}}{2^i}\right\rceil\geq\sum_{i=0}^{k-2}\left\lceil\frac{\lceil\frac{d}{2}\rceil}{2^i}\right\rceil=\sum_{i=0}^{k-2}\left\lceil\frac{d}{2^{i+1}}\right\rceil.$$

Now, we add d to both sides to get

$$n\geq\sum_{i=0}^{k-1}\left\lceil\frac{d}{2^i}\right\rceil.\quad\square$$

By combining the two previous proofs, we can understand the Griesmer bound as an evaluation of the parameters of a chain contained almost entirely in $\mathcal{Z}(M)$. Indeed, every subset $A\subset E$ that we constructed in the proof of Theorem 15 is a flat if not directly a cyclic flat. Furthermore, since $\mathcal{Z}(M|F)$ is a sub-lattice of $\mathcal{Z}(M)$ when F is a flat, performing the recursive steps of choosing residual codes can be viewed as taking a decreasing chain in the lattice of cyclic flats completed by the lattice of flats for every encounter of a rank edge. Finally, as illustrated in the next example, the construction of such a chain can be directly extracted from the proof of Theorem 15.

Example 5. Let M be the binary $(11,4,5)$-matroid given in Example 4. M achieves the Griesmer bound since we have $11=\sum_{i=0}^{3}\lceil\frac{5}{2^i}\rceil=5+3+2+1$. Now we construct a decreasing chain $E\succcurlyeq Z^d\succcurlyeq Z_1^d\succcurlyeq\emptyset$ in $\mathcal{Z}(M)$ by taking at every step a cyclic flat with maximal nullity contained in the previous one. By labeling the columns of the generator matrix G from 1 to 11, one such chain is given by $[11]\succcurlyeq\{1,2,4,6,9,11\}\succcurlyeq\{1,4,9\}\succcurlyeq\emptyset$ and is displayed in blue in Fig. 8.

In Example 4, we saw that $M|Z^d$ is a $(6,3,3)$-matroid and $M|Z_1^d$ is a $(3,2,2)$-matroid. Since $\emptyset\lessdot Z_1^d$ is a rank edge, we complete the chain by adding the flat $\{e\}\in\mathcal{F}(M)$ with $e\in Z_1^d$. Hence we have $n=d+d_{M|Z^d}+d_{M|Z_1^d}+d_{M|\{e\}}=5+3+2+1=\sum_{i=0}^{3}\lceil\frac{5}{2^i}\rceil$.

The previous proofs give a new understanding of the Griesmer bound and they are, in fact, deeply connected with the standard proofs in coding theory. The existence of residual codes is usually proven by using a codeword with desired weight and puncturing on its support [10]. Therefore, to show the link between the different proofs, we demonstrate the relation between codewords of a binary linear code and coatoms of the lattice of cyclic flats in the associated matroid.

Lemma 27. *Let $\mathcal{C}$ be a binary non-degenerate $[n,k,d]$ linear code with $d \geq 3$ and let c be a codeword of $\mathcal{C}$ with weight* $\mathrm{wt}(c) < 2d-2$. *Then, $Z_c = E - \mathrm{supp}(c)$ is a coatom of $\mathcal{Z}(M)$.*

Proof. Let $S = \mathrm{supp}(c)$. We have that $|Z_c| = |E| - |S| = n - \mathrm{wt}(c)$. Assume for a contradiction that $\rho(Z_c) < k-1$. Then there exists c' a codeword of $\mathcal{C}$ different from c such that $c'_i = 0$ for all $i \in Z_c$. Now let $\alpha \in \mathbb{F}_2$ such that at least $\mathrm{wt}(c)/2$ coordinates of $c'_{|S}$ equal α. Then, we have

$$d \leq \mathrm{wt}(c' - \alpha c) \leq \mathrm{wt}(c) - \frac{\mathrm{wt}(c)}{2} = \frac{\mathrm{wt}(c)}{2}$$

which contradicts the hypothesis on $\mathrm{wt}(c)$. Thus, the rank of Z_c is $k-1$.

Z_c is a flat, since otherwise, c does not have weight $\mathrm{wt}(c)$. It remains to prove that Z_c is cyclic. Assume for a contradiction that there exists $e \in Z_c$ such that $\rho(Z_c - \{e\}) < \rho(Z_c)$. Since there is an isthmus in $M|Z_c$, this implies that $d_{M|Z_c} = 1$ and there is a codeword $\hat{c}$ such that $\mathrm{wt}(\hat{c}_{|Z_c}) = 1$. Let $\beta \in \mathbb{F}_2$ be such that at least $\mathrm{wt}(c)/2$ coordinates of $\hat{c}_{|S}$ equal β. Then, we have

$$d \leq \mathrm{wt}(\hat{c} - \beta c) \leq \mathrm{wt}(c) + 1 - \frac{\mathrm{wt}(c)}{2} = \frac{\mathrm{wt}(c)+2}{2} < \frac{2d-2+2}{2} = d$$

which is a contradiction. Hence, Z_c is a cyclic flat of rank $k-1$ and thus a coatom of $\mathcal{Z}(M)$. □

Lemma 28. *Let M be a binary non-degenerate (n,k,d)-matroid with $d \geq 3$. Let Z_c be a coatom of $\mathcal{Z}(M)$ with $|Z_c| > n - 2d + 2$. Then, there exists a codeword c in $\mathcal{C}_M$, the linear code associated to M, such that* $\mathrm{supp}(c) = E - Z_c$.

Proof. Let G_M be a generator matrix of M. Since $d \geq 3$, we have $\rho(Z^d) = k-1$ and in particular, $G_{M|Z^d}$ the submatrix of G_M restricted to the columns indexed by Z^d, has rank $k-1$. Since G_M has k rows, one of the rows in $G_{M|Z^d}$ is dependent of the others. This implies that there is a codeword c in $\mathcal{C}_M$ such that $c_j = 0$ for all $j \in Z^d$. Since $|Z^d| > n - 2d + 2$, we have $\mathrm{wt}(c) < 2d-2$ and $\mathrm{supp}(c) \subseteq E - Z_c$. By Lemma 27, $E - \mathrm{supp}(c)$ is a coatom of $\mathcal{Z}(M)$ and $Z_c \subseteq E - \mathrm{supp}(c)$. Hence, $Z_c = E - \mathrm{supp}(c)$ since Z_c is already a coatom of $\mathcal{Z}(M)$. □

By combining the two previous lemmas, we get the following result.

Proposition 16. *Let $\mathcal{C}$ be a non-degenerate binary $[n, k, d]$ linear code and M_C the associated matroid. Then, there is a bijective map between the codewords of weight less than $2d-2$ and the coatoms of $\mathcal{Z}(M_C)$ of size greater than $n-2d+2$.*

Thus, this result shows the relation between the small weight codewords of a binary linear code and the cyclic flats with a large size of the matroid associated to the code.

10. Conclusion

In this paper, we presented the first steps towards the characterization of the lattice of cyclic flats of representable matroids over $\mathbb{F}_q$. In the first part of the paper, we derived two natural maps from $\mathcal{Z}(M)$ to the lattice of cyclic flats of a minor $M|Y/X$. Then, we showed how to reconstruct the lattice of flats from $\mathcal{Z}(M)$ and we computed the largest n for which the uniform matroid U_n^2 is a minor of M, from the lattice of cyclic flats. In the second part, we focused on binary matroids and the structure of their lattice of cyclic flats. We proved that the lattice of cyclic flats of a binary simple matroid with no isthmuses is atomic. Furthermore, we classified the binary matroids with lattice of cyclic flats of height 3. Finally, we defined the class of blunt cyclic flats for binary matroids and demonstrated the relation between blunt cyclic flats and the minimum distance of a matroid. As a consequence of this relation, we reproved the Griesmer bound for binary codes.

Acknowledgments

The work of M. Grezet, C. Hollanti, and T. Westerbäck was supported in part by The Academy of Finland [grant numbers 276031, 282938, and 303819] and by the Technical University of Munich – Institute for Advanced Study, funded by the German Excellence Initiative and the EU 7th Framework Programme [grant number 291763], via a Hans Fischer Fellowship. R. Freij-Hollanti was supported by the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG) [grant number WA3907/1-1].

References

[1] S. Ball, On sets of vectors of a finite vector space in which every subset of basis size is a basis, J. Eur. Math. Soc. 14 (3) (2012) 733–748.
[2] G. Birkhoff, Lattice Theory, 3rd edition, Colloquium Publications, vol. 25, American Mathematical Society, 1967.
[3] J.E. Bonin, A. de Mier, The lattice of cyclic flats of a matroid, Ann. Comb. 12 (2) (2008) 155–170.
[4] H.H. Crapo, G.-C. Rota, On the Foundations of Combinatorial Theory: Combinatorial Geometries, MIT Press, 1970.
[5] J.N. Eberhardt, Computing the Tutte polynomial of a matroid from its lattice of cyclic flats, Electron. J. Comb. 21 (3) (2014) 3–47.

[6] J. Geelen, B. Gerards, G. Whittle, Solving Rota's conjecture, Not. Am. Math. Soc. 61 (7) (2014) 736–743.
[7] M. Grezet, R. Freij-Hollanti, T. Westerbäck, C. Hollanti, On binary matroid minors and applications to data storage over small fields, in: International Castle Meeting on Coding Theory and Applications, 2017, pp. 139–153.
[8] M. Grezet, R. Freij-Hollanti, T. Westerbäck, O. Olmez, C. Hollanti, Bounds on binary locally repairable codes tolerating multiple erasures, in: The International Zurich Seminar on Information and Communication (IZS), Proceedings, Zurich, Switzerland, 2018, pp. 103–107.
[9] P. Huang, E. Yaakobi, H. Uchikawa, P.H. Siegel, Cyclic linear binary locally repairable codes, in: Proceedings of the IEEE Information Theory Workshop, IEEE, 2015, pp. 1–5.
[10] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, 2010.
[11] D. Mayhew, M. Newman, G. Whittle, Yes, the "missing axiom" of matroid theory is lost forever, Trans. Am. Math. Soc. 370 (8) (2018) 5907–5929.
[12] J. Oxley, Matroid Theory, 2nd edition, Oxford Graduate Texts in Mathematics, vol. 21, Oxford University Press, 2011.
[13] D.S. Papailiopoulos, A.G. Dimakis, Locally repairable codes, in: Proceedings of the IEEE International Symposium on Information Theory, 2012, pp. 2771–2775.
[14] K. Prideaux, Matroids, cyclic flats, and polyhedra, Master's thesis, Victoria University of Wellington, 2016.
[15] G.-C. Rota, Combinatorial theory, old and new, in: Actes du Congrès International des Mathématiciens (Nice, 1970), 1971, pp. 229–233.
[16] B. Segre, Curve razionali normali e k-archi negli spazi finiti, Ann. Mat. Pura Appl. 39 (1) (1955) 357–379.
[17] K. Shoda, Large families of matroids with the same Tutte polynomial, Ph.D. thesis, George Washington University, 2012.
[18] N. Silberstein, A. Zeh, Anticode-based locally repairable codes with high availability, Des. Codes Cryptogr. 86 (2) (2018) 419–445.
[19] J.A. Sims, Some problems in matroid theory, Ph.D. thesis, University of Oxford, 1980.
[20] R.P. Stanley, Enumerative Combinatorics, vol. 1, 2nd edition, Cambridge University Press, 2011.
[21] W.T. Tutte, A homotopy theorem for matroids, I, II, Trans. Am. Math. Soc. 88 (1) (1958) 144–174.
[22] P. Vámos, The missing axiom of matroid theory is lost forever, J. Lond. Math. Soc. 2 (3) (1978) 403–408.
[23] T. Westerbäck, R. Freij-Hollanti, T. Ernvall, C. Hollanti, On the combinatorics of locally repairable codes via matroid theory, IEEE Trans. Inf. Theory 62 (10) (2016) 5296–5315.