Codes, Matroids and Cyclic Flats

Vennix, Tom H.J.

Award date:
2024

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Master Thesis

Codes, Matroids and Cyclic Flats

Author:
T.H.J. (Tom) Vennix

Supervision:
dr. B. (Benjamin) Jany
dr. A. (Alberto) Ravagnani

Assessment committee:
dr. B. (Benjamin) Jany
dr. R.A. (Rudi) Pendavingh
dr. A. (Alberto) Ravagnani

Department of Mathematics and Computer Science

May 23, 2024

Abstract

In this thesis, we provide an overview of preliminary knowledge on matroid theory and coding theory and delve deep into properties of the closure and cyclic core operators on matroids. We prove a result connecting the cyclic flats of the matroid associated with a code's generator matrix to the non-degeneracy of certain subcodes. Furthermore, we provide a novel, yet remarkably simple way to construct the lattice of flats of a matroid without loops or coloops from its lattice of cyclic flats.

Contents

1 Introduction

Codes are an important object in today's mathematical landscape; they find application in numerous fields, such as cryptography, error correction and data storage. Matroid theory is a useful tool to study codes and gain an understanding of their properties; see, for instance, an application of matroid theory to information hiding through codes [1] and data storage through codes [2].

Connections between matroids and codes are an active area of mathematical research. Polynomials links have been established between codes and their associated matroids, see for instance [3]. In this thesis, we will focus on the matroid-theoretical side of these connections. In particular, we are interested in a thorough exploration of flats, cyclic sets and cyclic flats and in establishing connections between these classes of sets and the codes from which they arise. This will require some preliminary knowledge on both matroid theory and coding theory.

In the next two chapters, we will start with the former and provide a detailed overview of matroids, their rank functions, the closure operator and the cyclic core operator. Furthermore, we discuss a number of ways to construct new matroids from existing ones, among which we will discuss the dual matroid and contracted matroids. These two operations on matroids in particular will play an important part in the proofs of our main results in the final two chapters. In the penultimate chapter, we will also provide an overview on coding theory preliminaries, in order to illustrate the connections between codes and matroids and to motivate the results in the final chapter.

2 Preliminaries on matroid theory

Matroids are an important structure in mathematics; they formalise different forms of *independence* arise in various fields. One of the most crucial forms of independence is the idea of *linear independence* in linear algebra; this is also at the center of this thesis.

The contents of this chapter and the next are basic matroid theory. We follow Oxley [4] and Ardila [5]; proofs are included for self-containment.

2.1 Basic definitions

Imagine some finite-dimensional vector space and a finite collection of vectors inside this space. A subset of these vectors is said to be linearly independent if we cannot express any vector in the set as a linear combination of the others. As such, any arbitrary subset can be labelled as dependent or independent.

Example 1. Consider the following vectors in $\mathbb{R}^3$:

$$a = \begin{pmatrix}1\\0\\0\end{pmatrix},\ b = \begin{pmatrix}0\\1\\0\end{pmatrix},\ c = \begin{pmatrix}0\\0\\1\end{pmatrix},\ d = \begin{pmatrix}0\\0.5\\0.5\end{pmatrix},\ e = \begin{pmatrix}0\\1\\1\end{pmatrix},\ f = \begin{pmatrix}0\\0\\0\end{pmatrix}.$$

The set $\{a, b, c\}$ is linearly independent. The set $\{b, c, e\}$ is linearly dependent, as we can easily identify $b + c = e$. In this way, one can list all independent sets, resulting in the following list:

$$\varnothing, \{a\}, \{b\}, \{c\}, \{d\}, \{e\}, \{a, b\}, \{a, c\}, \{a, d\}, \{a, e\}, \{b, c\}, \{b, d\}, \{b, e\}, \{c, d\},$$
$$\{c, e\}, \{a, b, c\}, \{a, b, d\}, \{a, b, e\}, \{a, c, d\}, \{a, c, e\}.$$

With Example 1 in mind, we can formulate a set of properties that hold for any collection of vectors.

Proposition 1. Let V be a finite-dimensional vector space and let E be any set of vectors from V. Consider all linearly independent subsets of E. The following properties hold:

(i) $\varnothing$ is independent;

(ii) If a set X is independent, then every subset $Y \subseteq X$ is also independent;

(iii) If a set X is independent, but there exists another independent set Y of higher cardinality, then we can add some element of Y to X such that the resulting set is also independent.

Proof. Properties (i) and (ii) are easy to see, but property (iii) requires some work to verify. As above, assume X and Y are linearly independent sets of vectors with $|X| < |Y|$. Note that their independence implies that $\dim(\text{span}(X)) = |X|$ and $\dim(\text{span}(Y)) = |Y|$. We will argue by contradiction; to this end, assume there exists no $y \in Y \setminus X$ such that $X \cup \{y\}$ is linearly independent. This

implies that every $y \in Y \setminus X$ can be written as a linear combination of vectors in X. Since $Y = (Y \setminus X) \cup X$, this implies that every vector in Y can be written as a linear combination of vectors in X. But then $\text{span}(Y) \subseteq \text{span}(X)$, which is impossible as the dimension of $\text{span}(Y)$ is strictly larger than the dimension of $\text{span}(X)$. As such, property (iii) holds! □

As it turns out, we can obtain equivalent properties by examining the concept of *cycle-freeness* in graph theory. We will not explicitly cover graph theoretical concepts in this thesis; instead, we refer to Wilson [6].

Given a graph $G = (V, E)$, we can consider subgraphs of G on the same vertex set, yet containing only a subset of the original edges. These subgraphs are of the form $G_X = (V, X)$, where $X \subseteq E$.

Example 2. Consider the following graph with edge labels $\{a, b, c, d, e, f\}$:

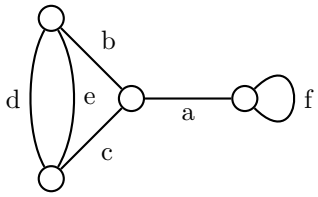

Figure 1: An example graph $G = (V, E)$

Note that the subgraph $G_{\{a,b,c\}}$ is cycle-free. A subgraph containing a cycle is, for instance, the subgraph $G_{\{b,c,e\}}$. If you list all possible subsets of edges for which the resulting subgraph is cycle-free, you obtain the exact same list as in the previous example.

As before, we can formulate a set of properties that should hold for graphs in general.

Proposition 2. Let $G = (V, E)$ be a graph and consider all subgraphs of the form $G_X = (V, X)$, where $X \subseteq E$. The following properties hold:

(i) $G_\varnothing$ is cycle-free;

(ii) If G_X is cycle-free, then G_Y is also cycle-free for any $Y \subseteq X$;

(iii) If G_X and G_Y are cycle-free with $|X| < |Y|$, then there exists some edge $y \in Y \setminus X$ such that the graph $G_{X \cup \{y\}}$ is also cycle-free.

Proof. As before, properties (i) and (ii) are easy to see, while property (iii) requires more work. The proof of this property requires one important insight: whenever an edge is added to the graph, this new edge either connects two components of the graph, or it closes at least one cycle in the graph. Since $G_X = (V, X)$ and $G_Y = (V, Y)$ are assumed to be cycle-free, this means every edge added to them connected two components, and therefore these graphs have $|V| - |X|$ and $|V| - |Y|$ components respectively.

Again, we will argue by contradiction. Assume there is no edge $y \in Y \setminus X$ such that $G_{X \cup \{y\}}$ is cycle-free; this means that adding any y to G_X closes a cycle and does not change the number of components of G_X. As such, we can add the entirety of $Y \setminus X$ to G_X, keeping its number of components the same all the way through. This means the graph $G_{X \cup Y}$ still has $|V| - |X|$ components. Now, imagine we remove all edges in $X \setminus Y$. When we are done, we obtain the graph G_Y with exactly $|V| - |Y|$ components. It should be clear that removing an edge can only increase the number of components, therefore we must have

$$|V| - |Y| \geq |V| - |X|.$$

This implies $|X| \geq |Y|$, which is a contradiction. As such, property (iii) holds! □

Evidently, these three properties capture some underlying structure which describes both linear independence in linear algebra and cycle-freeness in graph theory. Borrowing some terminology and notation from both areas, we can write these properties more abstractly to obtain our definition of a matroid.

Definition 1. A matroid is an ordered pair $M = (E(M), \mathcal{I}(M))$, where $E(M)$ is a finite set and $\mathcal{I}(M)$ is a collection of subsets of $E(M)$ that satisfy the following:

(I1) $\varnothing \in \mathcal{I}(M)$;

(I2) For any $I \in \mathcal{I}(M)$ and any $J \subseteq I$, we have that $J \in \mathcal{I}(M)$;

(I3) For any $I, J \in \mathcal{I}(M)$ with $|I| < |J|$, there exists some $j \in J \setminus I$ such that $I \cup \{j\} \in \mathcal{I}(M)$.

If $I \in \mathcal{I}(M)$, then I is said to be *independent*, else I is said to be *dependent*. $E(M)$ is referred to as the *ground set*.

Remark. Some notational remarks are in order:

- If it is clear from context which matroid we are considering, notational brevity compels us to write E and $\mathcal{I}$ instead of $E(M)$ and $\mathcal{I}(M)$.
- Properties (I2) and (I3) are often useful in matroid theoretical proofs; to this end, they are commonly referred to as the *hereditary property* and the *augmentation property* respectively. In particular, whenever we add an element to an independent set while maintaining its independence, we often say the set is *augmented* as a shorthand for invoking the augmentation property.
- To more easily refer to elements and subsets of the ground set E, these elements are commonly labelled by the numbers 1 through $n = |E|$. In turn, the ground set E is often written as $E = [n]$. This notation will be used interchangeably.

An important class of matroids, and a good example to provide as early as possible, are the uniform matroids.

Proposition 3. The *uniform matroid* of rank k on n elements (with $0 \leq k \leq n$), denoted $U_{n,k}$, is a matroid with ground set $E = [n]$ and collection of independent sets $\mathcal{I}_{n,k}$ given by

$$\mathcal{I}_{n,k} = \{I \subseteq [n] : |I| \leq k\}.$$

Proof. Proving that $U_{n,k}$ is a matroid means checking if conditions (I1)-(I3) are met by $\mathcal{I}_{n,k}$.

(I1) Since $k \geq 0$ and $|\varnothing| = 0$, we always have $|\varnothing| \leq k$ and therefore $\varnothing \in \mathcal{I}_{n,k}$.

(I2) $I \in \mathcal{I}_{n,k}$, so $|I| \leq k$. $J \subseteq I$, and therefore $|J| \leq |I| \leq k$, and so $J \in \mathcal{I}_{n,k}$.

(I3) Let $I, J \in \mathcal{I}_{n,k}$ with $|I| < |J|$. This implies $J \setminus I \neq \varnothing$; fix any $j \in J \setminus I$. Since $J \in \mathcal{I}_{n,k}$, we have $|J| \leq k$. We know $|I| < |J|$, so this means $|I| \leq k - 1$. Then $|I \cup \{j\}| \leq k$, and therefore $I \cup \{j\} \in \mathcal{I}_{n,k}$.

□

Example 3. The uniform matroid of rank 2 on 3 elements, $U_{3,2}$, has the following ground set and collection of independent sets:

$$E = [3] = \{1, 2, 3\}$$
$$\mathcal{I}_{3,2} = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$$

Oftentimes, listing every independent set of a matroid is a cumbersome process. As it turns out, property (I2) allows for some leeway when listing these sets.

Definition 2. A containment-wise maximal independent set of a matroid is called a *basis*. The collection of bases of a matroid $M = (E, \mathcal{I})$ is denoted $\mathcal{B}(M)$, or $\mathcal{B}$ where context permits.

Now, consider any independent set I. Either I is maximal, in which case it is a basis, or it is not maximal, in which case it can be augmented to become a basis. Therefore, instead of listing all independent sets of a matroid, it suffices to list only the bases; their subsets form the complete collection of independent sets. The bases of a matroid exhibit a special property.

Proposition 4. Let $M = (E, \mathcal{I})$ be a matroid. All bases of M are equicardinal.

Proof. We will argue by contradiction. Let B_1, B_2 be two bases of M and assume, without loss of generality, that $|B_1| < |B_2|$. Property (I3) states we can augment B_1 by some element in $b \in B_2 \setminus B_1$ and obtain the independent set $B_1 \cup \{b\}$, which strictly contains B_1. This contradicts maximality of B_1, and therefore bases cannot be of different cardinalities. □

Definition 3. Let $M = (E, \mathcal{I})$ be a matroid and let $X \subseteq E$. A containment-wise maximal independent set contained in X is called a *basis of* X.

Remark. In Section 2.3, we will show that all bases of a set X are also equicardinal, reminiscent of Proposition 4. For now, we will take this for granted.

We will now shift our perspective to dependent sets; recall Definition 1. If we know that a set $X \subseteq E$ is dependent, then any set Y containing X must also be dependent (else property (I2) would be violated). Therefore, instead of listing all dependent sets, it would suffice to list only the minimal dependent sets.

Definition 4. A containment-wise minimal dependent set of a matroid is called a *circuit*. The collection of circuits of a matroid $M = (E, \mathcal{I})$ is denoted $\mathcal{C}(M)$, or $\mathcal{C}$ where context permits.

Remark. It should be noted here that any dependent set D either is a circuit, or strictly contains a circuit. If we can say that D is not a minimal dependent set, that means we must be able to identify a dependent set strictly contained in D. This set is either a circuit, or we can remove another element from it to create a dependent set. Eventually, we must reach a circuit. This is the circuit-equivalent of the statement that any independent set either is a basis or can be augmented to become a basis.

It would be desirable for circuits to have a similar equicardinality proposition as is the case for bases, but unfortunately this is not the case. To see this, consider Example 2; the sets $\{f\}$ and $\{d, e\}$ are circuits of differing cardinality. The two different contexts discussed so far, linear algebra, and graph theory, provide some intuition why this is the case; different bases of the same finite-dimensional vector spaces always contain the same amount of vectors, whereas circuits in a graph can be of arbitrary length.

Definition 5. If a circuit contains exactly one element, this element is called a *loop* of the matroid. If a circuit contains exactly two elements, these elements are called *parallel elements* of the matroid. A matroid that does not contain loops or parallel elements is called a *simple matroid*.

Example 4. Looking back at Example 2, we can now say that f is a loop of the matroid. d and e are parallel elements. A circuit of cardinality 3 is given by $\{b, c, e\}$. An example of a basis is $\{a, b, c\}$; other bases can be found, but they will always be of the same cardinality.

Proposition 5. Let $M = (E, \mathcal{I})$ be a matroid, let C_1, C_2 be distinct circuits with non-empty intersection and let $e \in C_1 \cap C_2$. There exists a circuit $C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$.

Proof. Suppose $(C_1 \cup C_2) \setminus \{e\}$ does not contain a circuit; this means it is independent. Next, note that the set $C_2 \setminus C_1$ must be non-empty; otherwise, we would have $C_1 \subsetneq C_2$, which contradicts minimality of C_2. Therefore, we can identify some $f \in C_2 \setminus C_1$. Since C_2 is a circuit, $C_2 \setminus \{f\}$ is independent.

Now, identify the largest independent set $I \subseteq C_1 \cup C_2$ containing $C_2 \setminus \{f\}$.

We have that $f \notin I$, and there must also exist some $g \in C_1$ such that $g \notin I$. As such, $I \subseteq (C_1 \cup C_2) \setminus \{f, g\}$ and we can note

$$|I| \leq |(C_1 \cup C_2) \setminus \{f, g\}| < |(C_1 \cup C_2) \setminus \{e\}|.$$

Since $(C_1 \cup C_2) \setminus \{e\}$ is an independent set with larger cardinality than I, the augmentation property implies we can augment I. However, this contradicts maximality of I; as such, $(C_1 \cup C_2) \setminus \{e\}$ must be dependent, in which case it contains a circuit. □

Proposition 6. Let $M = (E, \mathcal{I})$ be a matroid, let $I \in \mathcal{I}$ and let $e \in E \setminus I$ such that $I \cup \{e\}$ is dependent. Then $I \cup \{e\}$ contains a unique circuit C with $e \in C$. This circuit is called the *fundamental circuit* and it is often denoted $C(e, I)$.

Proof. $I \cup \{e\}$ is dependent, so it must contain some circuit. Additionally, since I is independent, this circuit must contain e. To prove uniqueness, assume there are two such circuits: C_1 and C_2. By Proposition 5, there exists a circuit $C_3 \in (C_1 \cup C_2) \setminus \{e\} \subseteq I \setminus \{e\}$. This is a contradiction, so C must be unique. □

2.2 Rank function

Next, we will define the rank function of a matroid. The rank function is a central function in matroid theory, and it provides a convenient perspective on matroids which we will use to explore different concepts in Chapter 3.

Definition 6. Let $M = (E, \mathcal{I})$ be a matroid. We define its *rank function* $r : 2^E \to \mathbb{N} \cup \{0\}$ as follows:

$$r(X) = \max\{|I| : I \in \mathcal{I}, I \subseteq X\}$$

With Definition 3 in mind, this simply means that the rank of a set X is the cardinality of one of its bases. From a linear algebraic perspective, this implies precisely that the rank of a set of vectors is equal to the dimension of their span; this hopefully serves as intuitive justification as to why rank functions are such a central concept in matroid theory. Now, let us look back at some previously discussed examples and discuss their rank functions.

Example 5. Recall the set of vectors from Example 1:

$$a = \begin{pmatrix}1\\0\\0\end{pmatrix},\ b = \begin{pmatrix}0\\1\\0\end{pmatrix},\ c = \begin{pmatrix}0\\0\\1\end{pmatrix},\ d = \begin{pmatrix}0\\0.5\\0.5\end{pmatrix},\ e = \begin{pmatrix}0\\1\\1\end{pmatrix},\ f = \begin{pmatrix}0\\0\\0\end{pmatrix}.$$

We can now take any arbitrary subset of these vectors and identify its rank. For instance, $\{a, b, c\}$ is an independent set, and therefore its rank is $r(\{a, b, c\}) = 3$. The singleton $\{f\}$ is dependent; as such, the largest (and only) independent set contained in it is $\varnothing$, from which we obtain $r(\{f\}) = 0$. Similarly, the set $\{d, e\}$ is dependent whereas the sets $\{d\}$ and $\{e\}$ are independent, and so we can say $r(\{d\}) = r(\{e\}) = r(\{d, e\}) = 1$. Furthermore, note that $r(\{a, b, c, d, e, f\}) = 3$, as these vectors span $\mathbb{R}^3$.

Example 6. The uniform matroid $U_{n,k}$ has a rank function that can be expressed directly. Any set of cardinality $\leq k$ is independent and will therefore have rank equal to its cardinality. Any set of cardinality $> k$ will be dependent and have bases of cardinality k. As such, we can write:

$$r(X) = \min\{|X|, k\}$$

Remark. We will quickly note the following:

- A loop, like $\{f\}$ in Example 1, is a singleton of rank 0.
- Parallel elements, like $\{d, e\}$ in Example 1, form a 2-element set of rank 1.
- The rank of the ground set, $r(E)$, is referred to as the *rank of the matroid*. Commonly, this is denoted as $r(M)$ or simply by the variable k, as seen in our description of uniform matroids.

Proposition 7. Let $M = (E, \mathcal{I})$ be a matroid and let r denote its rank function. A set $X \subseteq E$ is independent if and only if $r(X) = |X|$.

Proof. Straightforward from Definition 6. □

Proposition 8. Let $M = (E, \mathcal{I})$ be a matroid and consider two arbitrary subsets $X, Y \subseteq E$. The rank function r has the following properties:

(R1) $0 \leq r(X) \leq |X|$;

(R2) $Y \subseteq X \Longrightarrow r(Y) \leq r(X)$;

(R3) $r(X) + r(Y) \geq r(X \cup Y) + r(X \cap Y)$.

Proof. Recall the definition of the rank function r:

$$r(X) = \max\{|I| : I \in \mathcal{I}, I \subseteq X\}.$$

(R1) and (R2) follow rather directly from this definition. (R3) requires more work. First of all, let B be a basis of $X \cap Y$, such that we know

$$r(X \cap Y) = |B|.$$

Next, we want to augment B to obtain a basis B' of $X \cup Y$. Denote $B_X = B' \cap (X \setminus Y)$ and $B_Y = B' \cap (Y \setminus X)$. Note that B, B_X and B_Y are pairwise disjoint and $B \cup B_X \cup B_Y = B'$. Finally, note that $B \cup B_X$ (resp. $B \cup B_Y$) is an independent set contained in X (resp. Y). Therefore, we can state the following:

$$\begin{aligned} r(X \cup Y) = |B'| &= |B| + |B_X| + |B_Y| \\ r(X) \geq |B \cup B_X| &= |B| + |B_X| \\ r(Y) \geq |B \cup B_Y| &= |B| + |B_Y|. \end{aligned}$$

Finally, we have

$$\begin{aligned} r(X) + r(Y) &\geq |B| + |B_X| + |B| + |B_Y| \\ &= |B| + |B_X| + |B_Y| + |B| \\ &= r(X \cup Y) + r(X \cap Y) \end{aligned}$$

and we are done. □

Property (R3), known as *submodularity*, is an important property that allows us to describe the behaviour of matroids and their rank functions in a considerably intuitive fashion. In the remainder of this section, we will be exploring some basic consequences of submodularity.

Proposition 9. Let $M = (E, \mathcal{I})$ be a matroid, let $X \subseteq E$ and let $e \in E \setminus X$. Then

$$r(X) \leq r(X \cup \{e\}) \leq r(X) + 1.$$

Proof. The first inequality follows from property (R2), also known as *monotonicity*, of the rank function. For the second inequality, we apply submodularity to X and $\{e\}$. We get

$$\begin{aligned} & r(X) + r(\{e\}) \geq r(X \cup \{e\}) + r(\varnothing) \\ \implies & r(X \cup \{e\}) \leq r(X) + r(\{e\}) \leq r(X) + 1. \end{aligned}$$

□

Remark. Proposition 9 tells us that, whenever we add an element to a set, its rank either stays constant or increases by 1. This relates to some of our previous discussions as follows:

Rank stays constant

- We added an edge that closed a cycle in the graph.
- We added a vector that was already in the span of the other vectors.
- More generally, we added an element that contributed no new 'information'.

Rank increases by 1

- We added an edge that connected two components of the graph.
- We added a vector that was outside of the other vectors' span, thereby increasing the dimension of the span.
- More generally, we added an element that did contribute new 'information'.

The lens of potentially adding new 'information' is a convenient way to look at rank functions. Intuitively, there are some properties that follow naturally from this perspective, and they can be proven formally using submodularity.

Proposition 10. Let $M = (E, \mathcal{I})$ be a matroid. Let $A \subseteq B \subseteq E$ and let $e \in E \setminus B$. If $r(B \cup \{e\}) = r(B) + 1$, then $r(A \cup \{e\}) = r(A) + 1$.

Proof. We apply submodularity to $A \cup \{e\}$ and B. We get

$$\begin{aligned} r(A \cup \{e\}) + r(B) &\geq r(B \cup \{e\}) + r(A) \\ r(A \cup \{e\}) + r(B) &\geq r(B) + 1 + r(A) \\ r(A \cup \{e\}) &\geq r(A) + 1 \\ r(A \cup \{e\}) &= r(A) + 1 \end{aligned}$$

where the last step follows from Proposition 9. □

Corollary 1. There are a number of ways to rephrase this result:

(i) Let $M = (E, \mathcal{I})$ be a matroid. Let $A \subseteq B \subseteq E$ and let $e \in E \setminus B$. If $r(A \cup \{e\}) = r(A)$, then $r(B \cup \{e\}) = r(B)$.

(ii) Let $M = (E, \mathcal{I})$ be a matroid. Let $A \subseteq B \subseteq E$ and let $e \in A$. If $r(B \setminus \{e\}) = r(B) - 1$, then $r(A \setminus \{e\}) = r(A) - 1$.

(iii) Let $M = (E, \mathcal{I})$ be a matroid. Let $A \subseteq B \subseteq E$ and let $e \in A$. If $r(A \setminus \{e\}) = r(A)$, then $r(B \setminus \{e\}) = r(B)$.

Remark. Proposition 10 simply states that, if an element adds new 'information' to a large set B, then it should also add 'information' to a smaller set A contained in B. The Corollaries are simply different ways of expressing the same phenomenon.

There is one important consequence of this proposition and its corollaries that we want to specifically highlight.

Proposition 11. Let $M = (E, \mathcal{I})$ be a matroid. Let $A \subseteq E$ and let $X \subseteq E \setminus A$ be a set of arbitrary cardinality with the property that, for all $x \in X$, we have $r(A \cup \{x\}) = r(A)$. Then $r(A \cup X) = r(A)$.

Proof. Suppose $|X| = m$ and fix some order of elements in X, i.e. $X = \{x_1, \ldots, x_m\}$. We have $r(A \cup \{x_1\}) = r(A)$ by assumption. Since $A \subseteq A \cup \{x_1\}$ and $r(A \cup \{x_2\}) = r(A)$, we can apply Corollary 1(i) to find $r(A \cup \{x_1, x_2\}) = r(A \cup \{x_1\}) = r(A)$. But then, we can do the same for x_3: we have $A \subseteq A \cup \{x_1, x_2\}$ and $r(A \cup \{x_3\}) = r(A)$, so we can apply Corollary 1(i) to find $r(A \cup \{x_1, x_2, x_3\}) = r(A \cup \{x_1, x_2\}) = r(A)$. This process continues until we have added all $x \in X$ and we find $r(A \cup X) = r(A)$. □

It is important to note here that rank properties (R1)-(R3) not only follow from the independent set definition of a matroid; they can actually be used as a defining axiom system for matroids. We will show this next.

Proposition 12. Let $M = (E, r)$ be a matroid and define $\mathcal{I}$ as the collection of sets I that satisfy $r(I) = |I|$. Then $\mathcal{I}$ satisfies the independent set axioms (I1)-(I3).

Proof. We will check (I1)-(I3) one-by-one.

(I1) Note that $|\varnothing| = 0$. Therefore, (R1) tells us that $0 \leq r(\varnothing) \leq |\varnothing| = 0$. This means $r(\varnothing) = 0 = |\varnothing|$, which implies $\varnothing \in \mathcal{I}$.

(I2) Fix any $x^* \in X$. Proposition 9, which was a consequence of (R3) and hence invocable here, implies that $r(X \setminus \{x^*\})$ can only equal $r(X) - 1$ or $r(X)$. However, since $r(X) = |X|$, we cannot have $r(X \setminus \{x^*\}) = r(X) = |X|$ as this would violate (R1); as such, $r(X \setminus \{x^*\}) = r(X) - 1 = |X| - 1 = |X \setminus \{x^*\}|$, so $X \setminus \{x^*\} \in \mathcal{I}$. Now, our desired result follows by deleting one-by-one the elements of $X \setminus Y$ from X until we obtain the set $Y \in \mathcal{I}$.

(I3) Let $X, Y \in \mathcal{I}$ such that $|X| < |Y|$. We will argue by contradictions, i.e. assume there exists no $y \in Y$ such that $X \cup \{y\} \in \mathcal{I}$. Note that this implies $r(X \cup \{y\}) = r(X) = |X|$, as the alternative by Proposition 9 would have $X \cup \{y\}$ be independent, and this is true for all $y \in Y \setminus X$. But then, we can invoke Proposition 11 to find $r(X \cup Y) = r(X \cup (Y \setminus X)) = r(X)$. (R2) implies $r(Y) \leq r(X \cup Y)$, but then, we find by independence of X and Y that

$$|Y| = r(Y) \leq r(X \cup Y) = r(X) = |X|.$$

This contradicts our initial assumption that $|Y| > |X|$. As such, there must exist some y^* such that $r(X \cup \{y^*\}) = r(X) + 1 = |X \cup \{y^*\}|$, in which case we have $X \cup \{y^*\} \in \mathcal{I}$.

□

We have constructed properties of rank functions that followed from the independent set axioms, but were consequently able to show that rank functions with those exact properties give rise to a collection of independent sets that automatically satisfies the independent set axioms. Therefore, this allows us to use the rank function properties as a non-trivially equivalent definition of matroids.

Definition 7. Two axiom systems are called *cryptomorphic* if they equivalently describe the same object, but their equivalence is not obvious.

Using this knowledge, we can freely switch between presenting matroids as an ordered pair $(E, \mathcal{I})$ and as an ordered pair (E, r). The latter presentation of matroids is most common and will also be more convenient for our work, hence we are hereby switching to the (E, r) notation.

Before moving on to the next section, however, it should be noted that these are not the only cryptomorphic axiom systems for matroids. In fact, one can define matroids also through their bases or their circuits; for completeness, we will include these formulations as well, without proof.

Proposition 13. Let $M = (E, \mathcal{B})$ be an ordered pair, where E is a finite set and $\mathcal{B}$ is a collection of subsets of E. Then M is a matroid with collection of bases $\mathcal{B}$ if the following are satisfied:

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

(B2) For distinct $A, B \in \mathcal{B}$ and any $a \in A$, there must exist some $b \in B$ such that $A \setminus \{a\} \cup \{b\} \in \mathcal{B}$.

Property (B2) is known as the *basis exchange property*, and it implies that we can turn any basis into any other basis by performing a sequence of element swaps. In particular, this implies all bases have the same cardinality, as we would expect by Proposition 4.

Proposition 14. Let $M = (E, \mathcal{C})$ be an ordered pair, where E is a finite set and $\mathcal{C}$ is a collection of subsets of E. Then M is a matroid with collection of circuits $\mathcal{C}$ if the following are satisfied:

(C1) $\varnothing \notin \mathcal{C}$;

(C2) For any $C \in \mathcal{C}$ and any $X \subset C$, we have $X \notin \mathcal{C}$;

(C3) For distinct (but not disjoint) $C_1, C_2 \in \mathcal{C}$ and any $c \in C_1 \cap C_2$, there must exist a circuit $C_3 \in \mathcal{C}$ such that $C_3 \subseteq C_1 \cup C_2 \setminus \{c\}$.

We have already seen property (C3) in the form of Proposition 5.

2.3 Operations on matroids

Now that we have defined matroids and considered their rank functions, we will consider operations that allow us to define new matroids from existing ones. We will start by defining the dual matroid, and subsequently look at three central operations in matroid theory: direct sum, restriction and contraction. Simultaneously, we will be providing, without proof, the rank functions of these newly constructed matroids.

Proposition 15. Let $M = ([n], r)$ be a matroid with collection of bases $\mathcal{B}(M)$. Its dual matroid, denoted M^*, is the matroid with ground set E, collection of bases

$$\mathcal{B}(M^*) = \{E \setminus B : B \in \mathcal{B}(M)\}.$$

and rank function

$$r^*(X) = |X| + r(E \setminus X) - r(M)$$

for all $X \subseteq E$.

Proof. By Proposition 4, all bases of M are equicardinal, say of cardinality k. All bases of M^* then have cardinality $n-k$. Collecting all subsets of these bases gives the collection of independent sets $\mathcal{I}(M^*)$, and matroid properties (I1)-(I3) hold by construction. □

Proposition 16. Let $M_1 = (E_1, r_1)$ and $M_2 = (E_2, r_2)$ be two matroids with disjoint ground sets, i.e. $E_1 \cap E_2 = \varnothing$. The *direct sum* of M_1 and M_2, denoted $M_1 \oplus M_2$, is the matroid with ground set $E(M_1 \oplus M_2) = E_1 \cup E_2$, collection of independent sets

$$\mathcal{I}(M_1 \oplus M_2) = \{I_1 \cup I_2 : I_1 \in \mathcal{I}(M_1), I_2 \in \mathcal{I}(M_2)\}$$

and rank function

$$\rho(X) = r_1(X \cap E_1) + r_2(X \cap E_2)$$

for all $X \subseteq E_1 \cup E_2$.

Proof. As in Proposition 3, showing this is a matroid is done through checking matroid properties (I1)-(I3).

(I1) M_1 and M_2 are matroids, therefore $\varnothing \in \mathcal{I}(M_1)$ and $\varnothing \in \mathcal{I}(M_2)$. Therefore, $\varnothing = \varnothing \cup \varnothing \in \mathcal{I}$.

(I2) Let $I \in \mathcal{I}(M_1 \oplus M_2)$, denote $I_1 = I \cap E_1$ and $I_2 = I \cap E_2$ and note that $I_1 \in \mathcal{I}(M_1)$ and $I_2 \in \mathcal{I}(M_2)$. Furthermore, take any $J \subseteq I$ and similarly denote $J_1 = J \cap E_1$ and $J_2 = J \cap E_2$. Since $J \subseteq I$, we have $J_1 \subseteq I_1$ and $J_2 \subseteq I_2$. From the hereditary property in M_1 and M_2, we infer that $J_1 \in \mathcal{I}(M_1)$ and $J_2 \in \mathcal{I}(M_2)$, and therefore $J = J_1 \cup J_2 \in \mathcal{I}(M_1 \oplus M_2)$.

(I3) Let $I, J \in \mathcal{I}(M_1 \oplus M_2)$ with $|I| < |J|$. Taking I_1, I_2, J_1 and J_2 as before, we note that at least one of $|I_1| < |J_1|$ and $|I_2| < |J_2|$ must hold; without loss of generality, assume $|I_1| < |J_1|$. The augmentation property in M_1 allows us to augment I_1 with some $j \in J_1 \setminus I_1$. The resulting set $I_1 \cup \{j\}$ is independent in M_1, and therefore the set $I_1 \cup \{j\} \cup I_2 = I \cup \{j\}$ is independent in $M_1 \oplus M_2$.

Finally, note that we can apply this proof inductively to obtain the same result for the direct sum of a larger amount of matroids. □

Example 7. In the previous section, we were introduced to an important class of matroids: uniform matroids. A second important class of matroids is obtained by taking direct sums of uniform matroids; such matroids are called *partition matroids*. For instance, take $U_{3,2}$ as before and consider its direct sum with $U_{2,1}$, where we will denote the ground set by $\{a, b\}$. The direct sum $U_{3,2} \oplus U_{2,1}$ is then the matroid with ground set $\{1, 2, 3, a, b\}$ and collection of independent sets given by

$$\begin{aligned}\mathcal{I}(U_{3,2} \oplus U_{2,1}) = &\{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{a\}, \{b\}, \{1,a\}, \{1,b\},\\ &\{2,a\}, \{2,b\}, \{3,a\}, \{3,b\}, \{1,2,a\}, \{1,2,b\}, \{1,3,a\}, \{1,3,b\},\\ &\{2,3,a\}, \{2,3,b\}\}\end{aligned}$$

Note that this is a different matroid from $U_{5,3}$; sets such as $\{a, b\}$ and $\{1, a, b\}$, which would be independent in $U_{5,3}$, are found to be dependent in $U_{3,2} \oplus U_{2,1}$.

Proposition 17. Let $M = (E, r)$ be a matroid and consider any subset $S \subseteq E$. The *restriction* of M to S, denoted $M|S$, is a matroid with ground set S, collection of independent sets

$$\mathcal{I}(\mathcal{M}|\mathcal{S}) = \{I \subseteq S : I \in \mathcal{I}(M)\}.$$

and rank function

$$\rho(X) = r(X)$$

for all $X \subseteq S$.

Proof. Matroid properties (I1) and (I2) are directly inherited from M; the augmentation property, (I3), might require some elaboration. Take $I, J \in \mathcal{I}(M|S)$ such that $|I| < |J|$ and note that $I \cup J \subseteq S$. I, J are independent sets of $M|S$, which implies by definition they are also independent sets of M. M is a matroid, so we can augment I with some $j \in J \setminus I$. The resulting independent set $I \cup \{j\}$ is a subset of S, and is therefore also independent in $M|S$. □

Remark. Recall Definition 3. A basis of a set X is precisely the same as a basis of the matroid $M|X$. As such, Proposition 4 tells us immediately that the bases of X are equicardinal.

Proposition 18. Let $M = (E, r)$ be a matroid and consider any subset $T \subseteq E$. Fix some basis B of T. The *contraction* of M by T, denoted M/T, is a matroid with ground set $E \setminus T$, collection of independent sets

$$\mathcal{I}(M/T) = \{I \subseteq E \setminus T : I \cup B \in \mathcal{I}(M)\}.$$

and rank function

$$\rho(X) = r(X \cup B) - r(B)$$

for all $X \subseteq E \setminus T$.

Proof. As before, matroid properties (I1) and (I2) are directly inherited from M, whereas property (I3) takes a little additional work. Take $I, J \in \mathcal{I}(M/T)$ such that $|I| < |J|$ and note that $I \cup J \subseteq E \setminus T$. I, J are independent sets of M/T, which implies by definition that $I \cup B$ and $J \cup B$ are independent sets of M. As $I \cap B = J \cap B = \varnothing$, we find that $|I \cup B| < |J \cup B|$. M is a matroid, so we can augment $I \cup B$ with some $j \in (J \cup B) \setminus (I \cup B) = J \setminus I$. The resulting independent set is $I \cup \{j\} \cup B$, and as $I \cup \{j\} \subseteq E \setminus T$, we have that $I \cup \{j\}$ is independent in M/T. □

These operations will feature prominently in the chapters to come.

3 Closure, cyclic core and cyclic flats

This chapter is about two important operators in matroid theory: *closure* and *cyclic core*. These operators have been studied in the past, for example by Oxley [4] and Freij-Hollanti et al. [2]; as such, the results in the sections to come are not new and proofs are again largely included for self-containment.

These operators will allow us to define closed and open sets, as well as sets which are open and closed simultaneously. Additionally, we will discuss how these operators interact with the operations on matroids defined in Section 2.3.

3.1 The closure operator

Definition 8. Let $M = (E, r)$ be a matroid. The *closure* operator $\mathrm{cl} : 2^E \to 2^E$ takes a set $X \subseteq E$ and maps it to the following set:

$$\mathrm{cl}(X) = \{e \in E : r(X \cup \{e\}) = r(X)\}$$

Example 8. Recall the graph from Example 2:

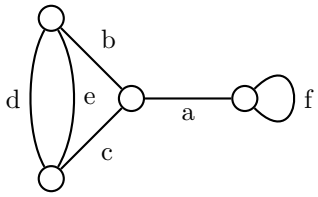

Figure 2: An example graph $G = (V, E)$

Consider the set $\{a, d\}$. We should identify all elements we can individually add to $\{a, d\}$ to close a cycle. These elements are e and f. Note that adding both b and c would also close a cycle, but this is not allowed; we are only looking for individual elements that close cycles. Therefore, we can state that $\mathrm{cl}(\{a, d\}) = \{a, d, e, f\}$.

Proposition 19. Let $M = (E, \mathcal{I})$ be a matroid. For all $X \subseteq E$, we have $r(\mathrm{cl}(X)) = r(X)$, i.e. closure preserves rank.

Proof. This is equivalent to Proposition 11. □

Proposition 20. Let $M = (E, \mathcal{I})$ be a matroid. For all $X, Y \subseteq E$ and $x, y \in E$, we have:

(1) $X \subseteq \mathrm{cl}(X)$;

(2) $Y \subseteq X \implies \mathrm{cl}(Y) \subseteq \mathrm{cl}(X)$;

(3) $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$;

(4) If $y \in \mathrm{cl}(X \cup \{x\}) \setminus \mathrm{cl}(X)$, then $x \in \mathrm{cl}(X \cup \{y\})$.

Proof. (1) This follows straightforwardly from the definition.

(2) Let $y \in \mathrm{cl}(Y)$, i.e. $r(Y \cup \{y\}) = r(Y)$. We can apply Corollary 1(i) to find $r(X \cup \{y\}) = r(X)$, i.e. $y \in \mathrm{cl}(X)$.

(3) By (1), we have that $\mathrm{cl}(X) \subseteq \mathrm{cl}(\mathrm{cl}(X))$. As such, we need to show $\mathrm{cl}(\mathrm{cl}(X)) \subseteq \mathrm{cl}(X)$. Let $e \in \mathrm{cl}(\mathrm{cl}(X))$; by definition, this means that $r(\mathrm{cl}(X) \cup \{e\}) = r(\mathrm{cl}(X)) = r(X)$. Note that $X \subseteq X \cup \{e\} \subseteq \mathrm{cl}(X) \cup \{e\}$; since $r(X) = r(\mathrm{cl}(X) \cup \{e\})$, monotonicity of the rank function implies $r(X \cup \{e\}) = r(X)$, i.e. $e \in \mathrm{cl}(X)$.

(4) Let $y \in \mathrm{cl}(X \cup \{x\}) \setminus \mathrm{cl}(X)$, i.e. we have $r(X \cup \{x, y\}) = r(X \cup \{x\})$ but $r(X \cup \{y\}) = r(X) + 1$. Now, note that

$$\begin{aligned} r(X) + 1 &= r(X \cup \{y\}) \\ &\leq r(X \cup \{x, y\}) \\ &= r(X \cup \{x\}) \\ &\leq r(X) + 1 \end{aligned}$$

so these ranks are all equal. This means $r(X \cup \{x, y\}) = r(X \cup \{y\})$, and so $x \in \mathrm{cl}(X \cup \{y\})$.

□

Definition 9. Let $M = (E, r)$ be a matroid. A subset $F \subseteq E$ that is equal to its closure, i.e. $F = \mathrm{cl}(F)$, is called *closed* or, more commonly, *flat*. The collection of flats is denoted $\mathcal{F}(M)$, or $\mathcal{F}$ where context permits.

By Proposition 20, any set that we can identify as the closure of another set, is a flat. In Example 2, the set $\{a, d, e, f\}$ is therefore a flat. A trivial example of a flat would be $\{a, b, c, d, e, f\}$; no elements can be added, so this set is certainly closed.

Proposition 21. Let $M = (E, r)$ be a matroid, let $F_1, F_2 \in \mathcal{F}(M)$ and let $X \subseteq E$. Then $F_1 \cap F_2$ is a flat.

Proof. Denote $F = F_1 \cap F_2$ and consider any $e \in E \setminus F_1$. Applying submodularity to F_1 and $F \cup \{e\}$ gives

$$\begin{aligned} r(F_1) + r(F \cup \{e\}) &\geq r(F_1 \cup (F \cup \{e\})) + r(F_1 \cap (F \cup \{e\})) \\ &= r(F_1 \cup \{e\}) + r(F) \\ &= r(F_1) + 1 + r(F) \end{aligned}$$

which implies $r(F \cup \{e\}) = r(F) + 1$ for all $e \in E \setminus F_1$. By symmetry, the same holds for all $e \in E \setminus F_2$. Since $E \setminus F = (E \setminus F_1) \cup (E \setminus F_2)$, we have $r(F \cup \{e\}) = r(F) + 1$ for all $e \in E \setminus F$ as required. This proves $F_1 \cap F_2$ is closed. □

3.2 The cyclic core operator

Definition 10. Let $M = (E, r)$ be a matroid. The *cyclic core* operator $\text{cyc} : 2^E \to 2^E$ takes a set $X \subseteq E$ and maps it to the following set:

$$\text{cyc}(X) = \{x \in X : r(X \setminus \{x\}) = r(X)\}$$

Example 9. In the graph from Example 2, consider the entire ground set $\{a, b, c, d, e, f\}$. Other than a, every element in the ground set is part of some cycle; therefore, only individually removing a would cause the rank to decrease. We can conclude that $\text{cyc}(\{a, b, c, d, e, f\}) = \{b, c, d, e, f\}$.

Proposition 22. Let $M = (E, r)$ be a matroid. For all $X, Y \subseteq E$, we have:

(1) $\text{cyc}(X) \subseteq X$;

(2) $Y \subseteq X \implies \text{cyc}(Y) \subseteq \text{cyc}(X)$.

Proof. (1) This follows straightforwardly from the definition.

(2) Let $y \in \text{cyc}(Y)$, i.e. $r(Y \setminus \{y\}) = r(Y)$. We can apply Corollary 1(iii) to find $r(X \setminus \{y\}) = r(X)$, i.e. $y \in \text{cyc}(X)$.

□

Definition 11. Let $M = (E, r)$ be a matroid. A subset $U \subseteq E$ that is equal to its cyclic core, i.e. $U = \text{cyc}(U)$, is called *open* or, more commonly, *cyclic*. The collection of cyclic sets is denoted $\mathcal{U}(M)$, or $\mathcal{U}$ where context permits.

Proposition 23. Let $M = (E, r)$ be a matroid, let C be any circuit of M and let $X \subseteq E$. We have

(1) $\text{cyc}(C) = C$, i.e. circuits are cyclic;

(2) Let $x \in X$. If $r(X \setminus \{x\}) = r(X)$, then X contains a circuit containing x;

(3) $\text{cyc}(X)$ is the union of all circuits contained in X;

(4) $\text{cyc}(\text{cyc}(X)) = \text{cyc}(X)$.

Proof. (1) C is, by definition, a minimal dependent set. This implies removing any element from C creates an independent set. Therefore, for any $c \in C$, this means $r(C) = r(C \setminus \{c\}) = |C| - 1$. As such, $C \subseteq \text{cyc}(C)$. Finally, Proposition 22 implies $C = \text{cyc}(C)$. Therefore, C is cyclic.

(2) Identify a basis B of $X \setminus \{x\}$. Note that $r(B) = r(X \setminus \{x\}) = r(X)$, and therefore B is also a basis of X. Proposition 6 implies $B \cup \{x\}$ contains a fundamental circuit $C(x, B)$. Finally, this means $C(x, B) \subseteq B \cup \{x\} \subseteq X$, i.e. X contains a circuit containing x.

(3) Take any circuit $C \subseteq X$. By Proposition 22, we have that $C = \text{cyc}(C) \subseteq \text{cyc}(X)$, so C is contained in $\text{cyc}(X)$. Now, let $x \in X$ be such that x is in no circuit contained in X. By (2), this means $r(X \setminus \{x\}) = r(X) - 1$, i.e. $x \notin \text{cyc}(X)$.

(4) By (3), $\text{cyc}(X)$ is the union of all circuits contained in X; this means every $x \in \text{cyc}(X)$ is an element of some circuit $C_x \subseteq \text{cyc}(X)$. But then $C_x \subseteq \text{cyc}(\text{cyc}(X))$, as $\text{cyc}(\text{cyc}(X))$ is the union of all circuits contained in $\text{cyc}(X)$. Therefore, $\text{cyc}(X) \subseteq \text{cyc}(\text{cyc}(X))$. The reverse inclusion is precisely Proposition 22.

□

By Proposition 23, any set that we can identify as the cyclic core of another set, is cyclic. In Example 2, this applies to $\{b, c, d, e, f\}$, which we identified as the cyclic core of $\{a, b, c, d, e, f\}$. Trivially, the empty set is cyclic.

Proposition 24. Let U_1 and U_2 be cyclic sets. Their union $U_1 \cup U_2$ is cyclic.

Proof. This follows straightforwardly from Proposition 23. □

Definition 12. Let $M = (E, r)$ be a matroid and let $X \subseteq E$. The *nullity* of X is the quantity $\eta(X) = |X| - r(X)$.

Proposition 25. Let $M = (E, \mathcal{I})$ be a matroid. For all $X \subseteq E$, we have $\eta(\text{cyc}(X)) = \eta(X)$, i.e. cyclic core preserves nullity.

Proof. In general, we can decompose $X = \text{cyc}(X) \cup Y$, where $Y = \{x \in X : r(X-x) = r(X)-1\}$; in Chapter 5, we will delve deeper into this decomposition. Fix some arbitrary order of the elements in Y, i.e. $Y = \{y_1, ..., y_k\}$ and imagine removing these elements one-by-one from X. If, at any point, the rank of the remaining set does *not* decrease when y_i is removed, then that means y_i was an element in some circuit of M contained in X. But circuits contained in X are contained in $\text{cyc}(X)$, and so this gives rise to a contradiction. As such, removing an element in $X - \text{cyc}(X)$ from X decreases both the rank and the cardinality of the resulting set at every step of the way, and therefore $|X| - r(X)$ is preserved by cyc. □

3.3 Cyclic flats

In the previous two sections, we have separately defined the closure and cyclic core operators and discussed some of their basic properties. In this section, we will consider what happens when these operators meet.

Proposition 26. Let $M = (E, r)$ be a matroid. We can state the following about its closure operator cl and cyclic core operator cyc:

(1) cl preserves cyclicity;

(2) cyc preserves flatness.

Proof. (1) Let U be a cyclic set and consider its closure $\text{cl}(U)$. Fix any $e \in \text{cl}(U)$. We have two cases:

Case 1: $e \in U$. Since U is cyclic, we have $r(U \setminus \{e\}) = r(U)$. By Corollary

1(iii), this implies $r(\mathrm{cl}(U) \setminus \{e\}) = r(\mathrm{cl}(U))$.

Case 2: $e \notin U$. Note that $U \subseteq \mathrm{cl}(U) \setminus \{e\} \subseteq \mathrm{cl}(U)$. Monotonicity of the rank function gives

$$r(U) \leq r(\mathrm{cl}(U) \setminus \{e\}) \leq r(\mathrm{cl}(U)).$$

Since $r(U) = r(\mathrm{cl}(U))$, this means $r(\mathrm{cl}(U) \setminus \{e\}) = r(\mathrm{cl}(U))$. Since e was chosen arbitrarily, this holds for all $e \in \mathrm{cl}(U)$.

Combining these cases, we find that $r(\mathrm{cl}(U) \setminus \{e\}) = r(\mathrm{cl}(U))$ for all $e \in \mathrm{cl}(U)$, i.e. $\mathrm{cl}(U)$ is cyclic.

(2) Let F be a flat and consider its cyclic core $\mathrm{cyc}(F)$. Note that, since $\mathrm{cyc}(F) \subseteq F$, we have that $\mathrm{cl}(\mathrm{cyc}(F)) \subseteq \mathrm{cl}(F) = F$. As such, any element $e \in E \setminus F$ cannot possibly be in the closure of $\mathrm{cyc}(F)$. Fix any $f \in F \setminus \mathrm{cyc}(F)$. Since $f \notin \mathrm{cyc}(F)$, we have that $r(F \setminus \{f\}) = r(F) - 1$. We apply submodularity on $\mathrm{cyc}(F) \cup \{f\}$ and $F \setminus \{f\}$:

$$\begin{aligned} r(\mathrm{cyc}(F) \cup \{f\}) + r(F \setminus \{f\}) &\geq r(F) + r(\mathrm{cyc}(F)) \\ r(\mathrm{cyc}(F) \cup \{f\}) + r(F) - 1 &\geq r(F) + r(\mathrm{cyc}(F)) \\ r(\mathrm{cyc}(F) \cup \{f\}) &\geq r(\mathrm{cyc}(F)) + 1 \end{aligned}$$

Since, by Proposition 9, $r(\mathrm{cyc}(F) \cup \{f\}) - r(\mathrm{cyc}(F)) \in \{0, 1\}$, this means that $r(\mathrm{cyc}(F) \cup \{f\}) = r(\mathrm{cyc}(F)) + 1$. As such, f is not in the closure of $\mathrm{cyc}(F)$. This shows that $\mathrm{cl}(\mathrm{cyc}(F)) \subseteq \mathrm{cyc}(F)$. The reverse inclusion is true by definition, so we conclude $\mathrm{cyc}(F) = \mathrm{cl}(\mathrm{cyc}(F))$. As such, $\mathrm{cyc}(F)$ is a flat.

□

Proposition 26 provides an interesting avenue of constructing sets in matroid; it allows us to take a flat (resp. cyclic set), take its cyclic core (resp. closure) and obtain a set that is simultaneously cyclic and flat.

Definition 13. Let $M = (E, r)$ be a matroid. A set $X \subseteq E$ that is both cyclic and flat is called a *cyclic flat*. The collection of cyclic flats is denoted $\mathcal{Z}(M)$, or $\mathcal{Z}$ where context permits.

The cyclic flats of a matroid form a lattice; a detailed discussion of lattices falls outside of the scope of this thesis, so we refer to Chapter 9 of [3] for a matroid-centric overview of lattice theory. However, we will note that the join and meet of two cyclic flats Z_1 and Z_2 are precisely

$$\begin{aligned} Z_1 \vee Z_2 &= \mathrm{cl}(Z_1 \cup Z_2) \\ Z_2 \wedge Z_2 &= \mathrm{cyc}(Z_1 \cap Z_2), \end{aligned}$$

which can easily be recognised as cyclic flats by combining Propositions 21, 24 and 26.

Remark. The flats of a matroid and the cyclic sets of a matroid also form lattices. This knowledge is not strictly relevant for the results we present, but this remark allows us to refer to these collections as lattices without causing confusion.

In Section 2.2, we saw equivalent definitions for matroids through their rank function, their bases and circuits. It turns out it is possible to do this through their cyclic flats as well; Bonin and De Mier [7] provide a cryptomorphic axiom system for matroids in terms of their cyclic flats, which we present here without proof.

Proposition 27. Let $M = (E, \mathcal{Z}, r)$ be an ordered triplet, where E is a finite set, $\mathcal{Z}$ is a collection of subsets of Z and $r : 2^{\mathcal{Z}} \to \mathbb{N} \cup \{0\}$ is an integer-valued function on Z. Then M is a matroid with lattice of cyclic flats Z and rank function r as described in Proposition 28 if the following are satisfied:

(Z1) $\mathcal{Z}$ is a lattice under inclusion;

(Z2) $r(0_{\mathcal{Z}}) = 0$;

(Z3) For all $X, Y \in \mathcal{Z}$ with $X \subsetneq Y$, we have $0 < r(Y) - r(X) < |Y| - |X|$;

(Z4) For all $X, Y \in \mathcal{Z}$, we have

$$r(X) + r(Y) \geq r(X \vee Y) + r(X \wedge Y) + |(X \cap Y) \setminus (X \wedge Y)|.$$

Correspondingly, we should be able to relate a matroid's rank function to its lattice of cyclic flats and their ranks.

Proposition 28. Let $M = (E, r)$ be a matroid and denote its collection of cyclic flats by $\mathcal{Z}$. Then

$$r(X) = |X| + \min_{Z \in \mathcal{Z}} \{r(Z) - |X \cap Z|\}$$

Proof. Freij-Hollanti et al. [8] provide the following result:

$$r(X) = \min_{Z \in \mathcal{Z}} \{r(Z) + |X \setminus Z|\}$$

By noting that $|X \setminus Z| = |(X \cup Z) \setminus Z| = |X \cup Z| - |Z| = |X| - |X \cap Z|$, we can rewrite this in the following ways:

$$r(X) = \min_{Z \in \mathcal{Z}} \{r(Z) + |X \cup Z| - |Z|\}$$
$$r(X) = \min_{Z \in \mathcal{Z}} \{r(Z) + |X| - |X \cap Z|\}$$

In particular, the last equality contains an $|X|$ term which does not depend on Z, so we can pull it outside of the minimum. This gives the expression we set out to prove. □

Next, we will discuss a number of ideas related to cyclic flats; these will feature in our later work.

Proposition 29. Let $M = (E, r)$ be a matroid and let $M^* = (E, r^*)$ be its dual. Then, for all $e \in E$, we have

$$e \text{ is a loop of } M^* \iff e \text{ is in no circuits of } M.$$

Such elements are called *coloops* of M.

Proof. ($\Longrightarrow$) Let e be a loop of M^*; since it is a loop, it is not an element of any basis of M^*. This implies e is in every basis of M. Now, assume there exists some circuit $C \in \mathcal{C}(M)$ with $e \in C$. By definition, $C \setminus \{e\}$ is independent, and can be augmented to become a basis. However, the resulting basis would have to contain e (as e is in every basis), but then this basis would contain the entirety of C and therefore be dependent; a contradiction. As such, e is in no circuits of M.

($\Longleftarrow$) Let e be in no circuits of M. This means adding e to any set $X \in E$ can only increase its rank in M, as adding e will never close a circuit. As such, e must be in every basis of M, which implies e is in no basis of M^*. Now, consider the singleton set $\{e\}$ in M^*. If it were independent, we would be able to augment it to become a basis. However, this basis would then contain $\{e\}$, which we know to be impossible; therefore, the set $\{e\}$ is dependent and e is a loop of M^*. □

Proposition 30. Let $M = (E, r)$ be a matroid. We have

$$\varnothing \text{ and } E \text{ are cyclic flats of } M \iff M \text{ has no loops or coloops}$$

Proof. ($\Longrightarrow$) Suppose $\varnothing$ and E are cyclic flats of M. $\varnothing$ is a flat, so adding any element will increase its rank; as such, every singleton set is independent, and therefore M has no loops. Furthermore, E is cyclic, which implies any element $e \in E$ is in some circuit C of M. By Proposition 29, this means M^* has no loops, or equivalently M has no coloops.

($\Longleftarrow$) Note that $\varnothing$ is cyclic and E is flat by definition. M has no loops, therefore any singleton set has rank 1, and so $\varnothing$ is closed (adding any element would increase its rank). Furthermore, M has no coloops, and therefore any element $e \in E$ is in some circuit of M; this implies E is cyclic. □

Definition 14. Let $M = (E, r)$ be a matroid and let $Z_1, Z_2 \in \mathcal{Z}(M)$. We say that Z_2 *covers* Z_1 if $Z_1 \subset Z_2$ and there is no $Z \in \mathcal{Z}(M)$ such that $Z_1 \subset Z \subset Z_2$.

In the upcoming sections, we will consider how the closure and cyclic core operations interact with duality, restriction and contraction as defined in Section 2.3. We will quickly discuss the direct sum here.

Proposition 31. Let $M_1 = (E_1, r_1)$ and $M_2 = (E_2, r_2)$ be matroids. Consider their direct sum $M_1 \oplus M_2 = (E_1 \cup E_2, r)$. We have

(1) $\mathcal{F}(M_1) \oplus \mathcal{F}(M_2) \cong \mathcal{F}(M_1 \oplus M_2)$

(2) $\mathcal{U}(M_1) \oplus \mathcal{U}(M_2) \cong \mathcal{U}(M_1 \oplus M_2)$

(3) $\mathcal{Z}(M_1) \oplus \mathcal{Z}(M_2) \cong \mathcal{Z}(M_1 \oplus M_2)$

Proof. The structures on the left hand side all consist of pairs of sets (X, Y) with $X \subseteq E_1$ and $Y \subseteq E_2$; we map them to the right-hand-side structures through the isomorphism $\phi(X, Y) = X \cup Y$. The reverse mapping would be $\psi(S) = (S \cap E_1, S \cap E_2)$. The matroid-theoretical part of this proof is straightforward. □

3.4 Notes on duality

Flats and cyclic sets turn out to be dual concepts; if X is a flat (resp. cyclic set) of a matroid, then its complement $E \setminus X$ is a cyclic set (resp. flat) of the dual matroid.

Proposition 32. Let $M = (E, r)$ be a matroid and let $M^* = (E, r^*)$ be its dual. We have that $r^*(M^*) = |E| - r(M)$.

Proof. Recalling that $r(E) = r(M)$ and $r^*(E) = r^*(M^*)$ by the same convention, the results follows immediately from taking $X = E$ in Proposition 15. □

Definition 15. Let $M = (E, r)$ be a matroid of rank k. A flat of rank $k - 1$ is called a *hyperplane*. The collection of hyperplanes is denoted $\mathcal{H}(M)$, or $\mathcal{H}$ where context permits.

Proposition 33. Let $M = (E, r)$ be a matroid and let $M^* = (E, r^*)$ be its dual.

(1) If C is a circuit of M, then $E \setminus C$ is a hyperplane of M^*.

(2) If U is a cyclic set of M, then $E \setminus U$ is a flat of M^*.

Proof. (1) Recall that

$$r^*(X) = |X| + r(E \setminus X) - r(M).$$

C is a circuit of M, i.e. $r(C \setminus \{c\}) = r(C)$ for all $c \in C$. Furthermore, since C is a circuit, $C \setminus \{c\}$ is independent for all $c \in C$, so we can make the stronger statement $r(C \setminus \{c\}) = r(C) = |C| - 1$ for all $c \in C$. To show that $E \setminus C$ is a hyperplane of M^*, we need to show that $r^*(E \setminus C \cup \{c\}) = r^*(E \setminus C) + 1$ for all $c \in C$ and that $r^*(E \setminus C) = r(M^*) - 1$. The second part follows from Proposition 32, since

$$\begin{aligned} r^*(E \setminus C) &= |E \setminus C| + r(C) - r(M) \\ &= |E| - |C| + |C| - 1 - r(M) \\ &= |E| - r(M) - 1 \\ &= r^*(M^*) - 1. \end{aligned}$$

Additionally, fix any $c \in C$. We have

$$\begin{aligned} r^*(E \setminus C \cup \{c\}) &= |E \setminus C \cup \{c\}| + r(C \setminus \{c\}) - r(M) \\ &= |E \setminus C| + 1 + r(C) - r(M) \\ &= |E \setminus C| + r(C) - r(M) + 1 \\ &= r^*(E \setminus C) + 1 \end{aligned}$$

and that concludes the proof.

(2) By Proposition 23, U is the union of all circuits contained in U, i.e.

$$U = \bigcup C_k$$

for all circuits $C_k \subseteq U$ of M. Note that

$$E \setminus U = E \setminus \left(\bigcup C_k\right) = \bigcap (E \setminus C_k)\,.$$

By (1), these sets $E \setminus C_k$ are all hyperplanes of M^*; in particular, they are all flat. We can repeatedly apply Proposition 21(1) to find that $E \setminus U$ is a flat of M^*.

□

The reverse direction of Proposition 33 can be proven completely analogously, except we are missing one ingredient: all flats would need to be obtainable as intersections of hyperplanes. This is true, but proving it takes more work than showing all cyclic sets are unions of circuits. Let us proceed with this.

Proposition 34. Let $M = (E, r)$ be a matroid and let $X, Y \subseteq E$. We have

(1) If $X \subseteq \mathrm{cl}(Y)$ and $\mathrm{cl}(Y) \subseteq \mathrm{cl}(X)$, then $\mathrm{cl}(X) = \mathrm{cl}(Y)$.

(2) If $Y \subseteq \mathrm{cl}(X)$, then $\mathrm{cl}(X \cup Y) = \mathrm{cl}(X)$.

(3) If $X \subseteq Y$ and $r(X) = r(Y)$, then $\mathrm{cl}(X) = \mathrm{cl}(Y)$.

(4) If B is a basis of X, then $\mathrm{cl}(B) = \mathrm{cl}(X)$.

Proof. In this proof, we will freely invoke parts of Proposition 20 whenever needed. Continually referring

(1) We have $\mathrm{cl}(Y) \subseteq \mathrm{cl}(X)$ by assumption; therefore, if we can show $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$, then we have our desired result by mutual inclusion. From $X \subseteq \mathrm{cl}(Y)$, we can infer that $\mathrm{cl}(X) \subseteq \mathrm{cl}(\mathrm{cl}(Y)) = \mathrm{cl}(Y)$, and we are done.

(2) Since $X \subseteq X \cup Y$, we have that $\mathrm{cl}(X) \subseteq \mathrm{cl}(X \cup Y)$. Next, we have $X \cup Y \subseteq \mathrm{cl}(X) \cup Y = \mathrm{cl}(X)$ since $Y \subseteq \mathrm{cl}(X)$. Then $\mathrm{cl}(X \cup Y) \subseteq \mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$. Again, we can conclude by mutual inclusion that $\mathrm{cl}(X \cup Y) = \mathrm{cl}(X)$.

(3) If $X = Y$, then this is obviously true. Instead, assume $Y \setminus X \neq \varnothing$ and take any $y \in Y \setminus X$. Then $X \subseteq X \cup \{y\} \subseteq Y$, we have by monotonicity of the rank function that $r(X) \leq r(X \cup \{y\}) \leq r(Y)$. Since $r(X) = r(Y)$, we have $r(X) = r(X \cup \{y\})$, which shows $y \in \mathrm{cl}(X)$. Since y was chosen arbitrarily, we have $Y \setminus X \subseteq \mathrm{cl}(X)$, and therefore $Y = (Y \setminus X) \cup X \subseteq \mathrm{cl}(X)$. This implies $\mathrm{cl}(Y) \subseteq \mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$. Lastly, since $X \subseteq Y \subseteq \mathrm{cl}(Y)$, so applying (1) gives our desired result.

(4) Since $B \subseteq X$ and $r(B) = r(X)$, this follows immediately from (3).

□

Proposition 35. Let $M = (E, r)$ be a matroid and let $X, Y \in \mathcal{F}(M)$ such that $X \subseteq Y$ and $r(X) = r(Y) - 1$. There exists some hyperplane $H \in \mathcal{H}(M)$ such that $X = H \cap Y$.

Proof. Fix a basis B_X of X. By Proposition 34, we have that $\mathrm{cl}(B_X) = \mathrm{cl}(X) = X$. Fix any $y \in Y \setminus X$; $y \notin X$, therefore $y \notin \mathrm{cl}(B_X)$, and so $r(B_X \cup \{y\}) = r(B_X) + 1 = r(X) + 1 = r(Y)$. Furthermore, $B_X \cup \{y\} \subseteq Y$, and so $B_X \cup \{y\}$ is a basis of Y.

Augment $B_X \cup \{y\}$ to a basis B of M. Since B is a basis of M, we have that B is independent and $r(B) = k$; it follows that $r(B \setminus \{y\}) = k - 1$. Let $H = \mathrm{cl}(B \setminus \{y\})$. First of all, note that $B_X \subseteq B \setminus \{y\}$, and so $X = \mathrm{cl}(B_X) \subseteq \mathrm{cl}(B \setminus \{y\}) = H$. Equivalently, we have $H \cap X = X$.

First of all, note that $y \notin \mathrm{cl}(B \setminus \{y\})$; if y were an element of $\mathrm{cl}(B \setminus \{y\})$, then Proposition 34 would tell us $\mathrm{cl}(B) = \mathrm{cl}(B \setminus \{y\} \cup \{y\}) = \mathrm{cl}(B \setminus \{y\})$, which is impossible since $r(B) \neq r(B \setminus \{y\})$. Suppose there exists $e \in Y \setminus X$ such that $e \neq y$. Then we have that $e \in \mathrm{cl}(B_X \cup \{y\})$ but $e \notin \mathrm{cl}(B_X)$; by Proposition 20, this means $y \in \mathrm{cl}(B_X \cup \{e\})$. Now, suppose $e \in \mathrm{cl}(B \setminus \{y\})$. Proposition 34 implies $\mathrm{cl}(B \cup \{e\} \setminus \{y\}) = \mathrm{cl}(B \setminus \{y\})$, and since $B_X \cup \{e\} \subseteq (B \setminus \{y\}) \cup \{e\}$, we have $\mathrm{cl}(B_X \cup \{e\}) \subseteq \mathrm{cl}(B \setminus \{y\})$. But this is a contradiction, since $y \in \mathrm{cl}(B_X \cup \{e\})$ but $y \notin \mathrm{cl}(B \setminus \{y\})$. As such, such an e either does not exist or $e \notin \mathrm{cl}(B \setminus \{y\})$; in either case, we have $H \cap (Y \setminus X) = \varnothing$.

Finally, we have

$$\begin{aligned} H \cap Y &= H \cap (X \cup (Y \setminus X)) \\ &= (H \cap X) \cup (H \cap (Y \setminus X)) \\ &= X \cup \varnothing = X \end{aligned}$$

as desired. □

Proposition 36. Let $M = (E, r)$ be a matroid and let $F \in \mathcal{F}(M)$ be a flat of rank $r(F) = k - t$. Then F can be written as the intersection of exactly t hyperplanes.

Proof. Denote $F_0 = F$. Fix any $e_1 \in E \setminus F_0$ and denote $F_1 = \mathrm{cl}(F_0 \cup \{e_1\})$. F_1 is then a flat of rank $k - t + 1$. We continue this process of adding an element and closing the set to obtain flats F_i of rank $r(F_i) = k - t + i$ until we finally

obtain the flat F_{t-1} of rank $r(F_{t-1}) = k - 1$. Note that F_{t-1} is a hyperplane; denote $H_1 = F_{t-1}$. We can apply Proposition 35 to deduce the existence of a hyperplane H_2 such that $F_{t-2} = H_2 \cap H_1$. Applying this repeatedly, we find a collection of hyperplanes $H_1, H_2, \ldots, H_t$ such that

$$F = \bigcap_{i=1}^{t} H_i$$

as desired. □

We can now combine the results of this section into the following important theorem on matroid duality.

Theorem 1. Let $M = (E, r)$ be a matroid and let $M^* = (E, r^*)$ be its dual. Let $C, H, U, F, Z, Z^* \subseteq E$ such that $C \cup H = U \cup F = Z \cup Z^* = E$. We have

(1) C is a circuit of $M \iff H$ is a hyperplane of M^*;

(2) U is a cyclic set of $M \iff F$ is a flat of M^*;

(3) Z is a cyclic flat of $M \iff Z^*$ is a cyclic flat of M^*.

3.5 Cyclic flats under restriction and contraction

For our main result in the upcoming chapter, it is crucial to develop an understanding of the relationship between the cyclic sets and flats of a matroid and its minors.

Proposition 37. Let $M = (E, r)$ be a matroid, let $S \subseteq E$ and consider the restricted matroid $M|S = (S, \rho)$. Then $U \subseteq S$ is a cyclic set of M if and only if U is a cyclic set of $M|S$.

Proof. Let $U \subseteq S$ be a cyclic set of M, i.e. $r(U \setminus \{u\}) = r(U)$ for all $u \in U$. Recall from Proposition 17 that we have

$$\rho(X) = r(X)$$

for all $X \subseteq S$. Now, fix any $u \in U$. We have

$$\rho(U \setminus \{u\}) = r(U \setminus \{u\}) = r(U) = \rho(U)$$

and as such, U is a cyclic set of $M|S$. The reverse direction follows analogously. □

Proposition 38. Let $M = (E, r)$ be a matroid, let $T \subseteq E$ and consider the contracted matroid $M/T = (E \setminus T, \rho)$. Then $F \cup T$ is a flat of M if and only if F is a flat of M/T.

Proof. Let $F \cup T$ be a flat of M, i.e. $r(F \cup T \cup \{e\}) = r(F \cup T) + 1$ for all $e \in E \setminus (F \cup T)$. Recall from Proposition 18 that we have

$$\rho(X) = r(X \cup T) - r(T)$$

for all $X \in E \setminus T$. Next, fix any $e \in (E \setminus T) \setminus F = E \setminus (F \cup T)$. We have

$$\begin{aligned}\rho(F \cup \{e\}) &= r(F \cup T \cup \{e\}) - r(T) = r(F \cup T) + 1 - r(T) \\ &= r(F \cup T) - r(T) + 1 \\ &= \rho(F) + 1\end{aligned}$$

and as such, F is a flat of M/T. As before, the reverse direction follows analogously. □

These propositions show that restriction naturally preserves cyclicity, and that contraction naturally preserves flatness. It would be ideal if restriction also preserved flatness and contraction also preserved cyclicity; luckily, we can make this happen by only adding two minor conditions.

Proposition 39. Let $M = (E, r)$ be a matroid, let $G \in \mathcal{F}(M)$ and consider the restricted matroid $M|G = (G, \rho)$. Then $F \subseteq G$ is a flat of M if and only if F is a flat of $M|G$.

Proof. ($\Longrightarrow$) Let $F \subseteq G$ be a flat of M, i.e. $r(F \cup \{e\}) = r(F) + 1$ for all $e \in E \setminus F$. Fix any $e \in G \setminus F$ and note that $G \setminus F \subseteq E \setminus F$. We have

$$\rho(F \cup \{e\}) = r(F \cup \{e\}) = r(F) + 1 = \rho(F) + 1$$

and as such, F is a flat of $M|G$.

($\Longleftarrow$) Let F be a flat of $M|G$. By construction, this means $F \subseteq G$, and by Proposition 20, we have $\mathrm{cl}(F) \subseteq \mathrm{cl}(G) = G$ in M, and therefore $\mathrm{cl}(F) \setminus F \subseteq G \setminus F$. But F is a flat of $M|G$, so for any $e \in G \setminus F$, we have that $\rho(F \cup \{e\}) = \rho(F) + 1$. But then we also have, for any $e \in G \setminus F$,

$$r(F \cup \{e\}) = \rho(F \cup \{e\}) = \rho(F) + 1 = r(F) + 1$$

and so F is also a flat of M. □

Proposition 40. Let $M = (E, r)$ be a matroid, let $W \in \mathcal{U}(M)$ and consider the contracted matroid $M/W = (E \setminus W, \rho)$. Then $U \cup W$ is a cyclic set of M if and only if U is a cyclic set of M/W.

Proof. ($\Longrightarrow$) Let $U \cup W$ be a cyclic set of M, i.e. $r(U \cup W \setminus \{e\}) = r(U \cup W)$ for any $e \in U \cup W$. Now, fix any $u \in U$. We have

$$\begin{aligned}\rho(U \setminus \{u\}) &= r(U \cup W \setminus \{u\}) - r(W) \\ &= r(U \cup W) - r(W) \\ &= \rho(U)\end{aligned}$$

and therefore U is a cyclic set of M/W.

($\Longleftarrow$) Let U be a cyclic set of M/W. For any $u \in U$, we have

$$\begin{aligned} r(U \cup W \setminus \{e\}) &= \rho(U \setminus \{e\}) + r(W) \\ &= \rho(U) + r(W) \\ &= r(U \cup W) \end{aligned}$$

and as such, $U \subseteq \text{cyc}(U \cup W)$ in M. Secondly, as W is a cyclic set of M and $W \subseteq U \cup W$, we have $W = \text{cyc}(W) \subseteq \text{cyc}(U \cup W)$. Since $U \subseteq \text{cyc}(U \cup W)$ and $W \subseteq \text{cyc}(U \cup W)$, we have $U \cup W \subseteq \text{cyc}(U \cup W)$, and therefore $U \cup W$ is a cyclic set of M. □

We have seen that restriction also preserves flatness so long as we restrict to a flat, and contraction also preserves cyclicity so long as we contract by a cyclic set. We now combine these results.

Proposition 41. Let $M = (E, r)$ be a matroid, let $F \in \mathcal{F}(M)$ and let $U \in \mathcal{U}(M)$. Then $Z \cup U$ is a cyclic flat of M if and only if Z is a cyclic flat of $M|F/U$.

Proof. This follows from straightforward application of Propositions 37-40. □

This allows us to formulate the following major result.

Theorem 2. Let $M = (E, r)$ be a matroid and let $Z_1, Z_2 \in \mathcal{Z}(M)$ such that Z_2 covers Z_1. The matroid $M|Z_2/Z_1 = (Z_2 \setminus Z_1, \rho)$ is the uniform matroid on $|Z_2| - |Z_1|$ elements of rank $r(Z_2) - r(Z_1)$.

Proof. Note that Z_1, Z_2 and $M|Z_2/Z_1$ meet the conditions of Proposition 41, so we know that $Z_2 \setminus Z_1$ and $Z_1 \setminus Z_1 = \varnothing$ are cyclic flats of $M|Z_2/Z_1$. Furthermore, since Z_2 covers Z_1, these are the only cyclic flats of $M|Z_2/Z_1$. This allows us to invoke Proposition 4 of Freij-Hollanti et al. [8], which states that any matroid with a two-element lattice of cyclic flats is a uniform matroid $U_{n,k}$. Finally, $n = |Z_2 \setminus Z_1| = |Z_2| - |Z_1|$ and

$$\begin{aligned} k &= \rho(Z_2 \setminus Z_1) \\ &= r(Z_2 \setminus Z_1 \cup Z_1) - r(Z_1) \\ &= r(Z_2) - r(Z_1). \end{aligned}$$

□

4 Connections with coding theory

In the previous chapters, we have provided an extensive introduction to matroid theory. Before we present our main results in Chapter 5, we want to illustrate the usefulness of matroid theory by diving into a research area in which matroid theory finds important applications: coding theory.

4.1 Preliminaries on coding theory

Definition 16. Let q be some prime power and let $\mathbb{F}_q^n$ denote the vector space of dimension n over the finite field $\mathbb{F}_q$. A *linear block code* $\mathcal{C}$ is a collection of vectors that form an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$.

Suppose a linear block code $\mathcal{C}$ has dimension k, i.e. it is a k-dimensional subspace of $\mathbb{F}_q^n$. This implies we can choose k vectors in $\mathbb{F}_q^n$ such that their span is exactly the subspace $\mathcal{C}$. We can put these vectors as the rows of a $k \times n$ matrix, and we say that this matrix is a generator matrix of the code $\mathcal{C}$.

Definition 17. A matrix G with entries in $\mathbb{F}_q$ is a *generator matrix* for a linear block code $\mathcal{C}$ if it has full rank and its rows generate $\mathcal{C}$ over $\mathbb{F}_q$. Moreover, we have

$$\mathcal{C} = \{x \cdot G : x \in \mathbb{F}_q^k\}.$$

Remark. It is clear from this definition that a k-dimensional linear block code $\mathcal{C} \leq \mathbb{F}_q^n$ consists of precisely q^k *codewords*. This is because G having full rank implies every choice of x generates a unique codeword, and there are exactly q^k choices for x. These codewords all have n entries, which is why we refer to n as the *length* of the code.

Evidently, we can choose many different generator matrices that would all generate the same linear block code $\mathcal{C}$. We can obtain a canonical generator matrix by considering the unique reduced row-echelon form of these matrices. This canonical matrix G is known as the *standard generating matrix* of $\mathcal{C}$ and is of the form

$$G = \left[I_k \mid A\right].$$

Definition 18. A matrix H with entries in $\mathbb{F}_q$ is a *parity-check matrix* for a linear block code $\mathcal{C}$ if it has full rank and $\mathcal{C}$ is the left kernel of H^T, i.e.

$$\mathcal{C} = \{x \in \mathbb{F}_q^n : x \cdot H^T = 0\}.$$

Since H^T has left kernel of dimension k, this suggests H is of rank $n - k$. Consequently, we can state H is a matrix of dimension $(n - k) \times n$. Related to the canonical form of the generator matrix, there is also a canonical form of the parity-check matrix. If we take a standard generator matrix G, i.e.

$G = \left[I_k \mid A \right]$, then it is easy to check that a *standard parity-check matrix* exists of the following form:

$$H = \left[-A^T \mid I_{n-k} \right].$$

Moreover, we have by construction that $GH^T = 0$, and so we come to the realisation that H is actually a generator matrix for the orthogonal complement of $\mathcal{C}$. As we would expect the orthogonal complement to be of dimension $n - k$, this matches what we know about the rank of H. Formally, we have the following:

Definition 19. Let $\mathcal{C} \leq \mathbb{F}_q^n$ be a linear block code with $k \times n$ generator matrix G and $(n-k) \times n$ parity-check matrix H. Its orthogonal complement $\mathcal{C}^\perp$ is also a linear block code with generator matrix H and parity-check matrix G and consists of all codewords $x \in \mathbb{F}_q^n$ with the property that

$$\langle x, v \rangle = \sum_{i=1}^{n} x_i v_i = 0$$

for all $v \in \mathcal{C}$.

Example 10. Let $\mathcal{C} \leq \mathbb{F}_2^5$ be a 3-dimensional linear block code generated by the vectors $(1,0,0,1,1)$, $(0,1,0,0,1)$ and $(0,0,1,1,1)$. $\mathcal{C}$ should contain $q^k = 2^3 = 8$ codewords, which are:

$$\mathcal{C} = \left\{ \begin{array}{c} (0,0,0,0,0) \\ (1,0,0,1,1) \\ (0,1,0,0,1) \\ (0,0,1,1,1) \\ (1,1,0,1,0) \\ (1,0,1,0,0) \\ (0,1,1,1,0) \\ (1,1,1,0,1) \end{array} \right\}.$$

Moreover, we can express a generator and parity-check matrix in canonical form as

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

Using our perspective of H as the generator matrix for $\mathcal{C}^\perp$, we find

$$\mathcal{C}^\perp = \left\{ \begin{array}{c} (0,0,0,0,0) \\ (1,0,1,1,0) \\ (1,1,1,0,1) \\ (0,1,0,1,1) \end{array} \right\}.$$

We will end this section with some basic properties of codes and their codewords.

Definition 20. Let $\mathcal{C} \leq \mathbb{F}_q^n$ and let $v \in \mathcal{C}$ be a codeword. We define its *(Hamming) weight* $\omega(v)$ to be the number of non-zero coordinates of v, and its *(Hamming) support* $\sigma(v)$ to be the set of indices of its non-zero coordinates, i.e.

$$\sigma(v) = \{i \in [n] : v_i \neq 0\}.$$

Remark. Note that $\omega(v) = |\sigma(v)|$.

Definition 21. Let $\mathcal{C} \leq \mathbb{F}_q^n$ and let $v \in \mathcal{C} \setminus \{0\}$ be a codeword. We say v is a *minimal* codeword if there does not exist another codeword $w \in \mathcal{C} \setminus \{0\}$ such that $\sigma(w) \subset \sigma(v)$, i.e. there does not exist a codeword with support strictly contained in the support of v.

Definition 22. Let $\mathcal{C} \leq \mathbb{F}_q^n$. $\mathcal{C}$ is called *non-degenerate* if

$$\bigcup_{v \in \mathcal{V}} \sigma(V) = [n].$$

Definition 23. Let $\mathcal{C} \leq \mathbb{F}_q^n$. The *minimum weight* or *minimum distance* of $\mathcal{C}$ is denoted $\mathrm{d}(\mathcal{C})$ and is precisely

$$\mathrm{d}(\mathcal{C}) = \min_{v \in \mathcal{C}} \{\omega(v)\}$$

Proposition 42. Let $\mathcal{C} \leq \mathbb{F}_q^n$. We have

$$\mathcal{C} \text{ is non-degenerate } \iff \mathrm{d}(\mathcal{C}^\perp) \neq 1.$$

Proof. ($\Longrightarrow$) Suppose $\mathrm{d}(\mathcal{C}^\perp) = 1$. Then there exists a codeword $c \in \mathcal{C}^\perp$ and $j \in [n]$ such that $c_i = 0$ for all $i \in [n] \setminus \{j\}$ and $c_j \neq 0$. Now $c \in \mathcal{C}^\perp$, which means

$$\langle v, c \rangle = \sum_{i=1}^{n} v_i c_i = v_j c_j = 0$$

for all $v \in \mathcal{C}$. Since $c_j \neq 0$, we must have that $v_j = 0$ for all $v \in \mathcal{C}$, and so

$$j \notin \bigcup_{v \in \mathcal{C}} \sigma_H(v).$$

As such, $\mathcal{C}$ is degenerate. This shows $\mathrm{d}(\mathcal{C}^\perp) \geq 2$ is necessary.

($\Longleftarrow$) Suppose that a code $\mathcal{C} \leq \mathbb{F}_q^n$ is degenerate. That means

$$\bigcup_{v \in \mathcal{C}} \sigma_H(v) \neq [n]$$

so there must exist some $j \in [n]$ with

$$j \notin \bigcup_{v \in \mathcal{C}} \sigma_H(v).$$

As such, $v_j = 0$ for all $v \in \mathcal{C}$, and so $e_j \in \mathcal{C}^\perp$. As such, $\mathrm{d}(\mathcal{C}^\perp) = 1$. This shows $\mathrm{d}(\mathcal{C}^\perp) \geq 2$ is sufficient. $\square$

4.2 Operations on codes

As with matroids, there are many ways to take a code and use it to create other codes. In this section, we will explore some of these operations and provide a series of propositions that relate the resulting codes and their dimensions.

Definition 24. Let $\mathcal{C} \leq \mathbb{F}_q^n$ and let $S \subseteq [n]$. We define the following operations:

$$\begin{aligned} \mathcal{C}(S) &= \{v \in \mathcal{C} : \sigma(v) \subseteq S\}, \\ \pi_S(\mathcal{C}) &= \{\pi_S(v) : v \in \mathcal{C}\}, \\ \pi_S(\mathcal{C}(S)) &= \{\pi_S(V) : v \in \mathcal{C}(S)\}. \end{aligned}$$

where $\pi_S(v)$ denotes the projection of v onto the coordinates indexed by S.

Proposition 43. Let $\mathcal{C} \leq \mathbb{F}_q^n$. We have $\mathcal{C}(S) \leq \mathbb{F}_q^n$, $\pi_S(\mathcal{C}) \leq \mathbb{F}_q^{|S|}$ and $\pi_S(\mathcal{C}(S)) \leq \mathbb{F}_q^{|S|}$.

Proof. The fact that $\mathcal{C}(S)$, $\pi_S(\mathcal{C})$ and $\pi_S(\mathcal{C}(S))$ are $\mathbb{F}_q$-linear subspaces is inherited from $\mathcal{C}$. □

Proposition 44. Let $\mathcal{C} \leq \mathbb{F}_q^n$ and let $S \subseteq [n]$. We have

$$\dim \pi_S(\mathcal{C}(S)) = \dim \mathcal{C}(S).$$

Proof. $\mathcal{C}(S)$ contains precisely all codewords $v \in \mathcal{C}$ with zeroes in the coordinates indexed by $[n] \setminus S$. As such, the way π_S acts on $\mathcal{C}(S)$ is by only removing coordinates in which all codewords in $\mathcal{C}(S)$ are zero, and therefore the dimension does not change. □

Proposition 45. Let $\mathcal{C} \leq \mathbb{F}_q^n$ and let $S \subseteq [n]$. We have

$$\dim \mathcal{C}(S) + \dim \pi_{E\setminus S}(\mathcal{C}) = \dim \mathcal{C}$$

Proof. Consider the linear transformation $f : \mathcal{C} \to \pi_{E\setminus S}(\mathcal{C})$, i.e. f takes as input a codeword $v \in \mathcal{C}$ and maps it to its projection $\pi_{E\setminus S}(v)$. The kernel of f is then all codewords with support contained in S, i.e. we have

$$\ker(f) = \mathcal{C}(S)$$

and by definition

$$\mathrm{im}(f) = \pi_{E\setminus S}(\mathcal{C}).$$

Recall the classical dimension theorem for linear transformations $T : V \to W$:

$$\dim \ker(T) + \dim \mathrm{im}(T) = \dim V$$

We can simply substitute our findings to obtain

$$\dim \mathcal{C}(S) + \dim \pi_{E\setminus S}(\mathcal{C}) = \dim \mathcal{C}$$

as desired. □

Proposition 46. Let $\mathcal{C} \leq \mathbb{F}_q^n$ and let $S \subseteq [n]$. We have

$$\pi_S(\mathcal{C}(S))^\perp = \pi_S(\mathcal{C}^\perp)$$

Proof. ($\subseteq$) Instead of the inclusion in question, we will prove the following inclusion:

$$\pi_S(\mathcal{C}^\perp)^\perp \subseteq \pi_S(\mathcal{C}(S)).$$

Since $A \subseteq B \implies B^\perp \subseteq A^\perp$, this will imply the desired inclusion if we have that $(\pi_S(\mathcal{C}^\perp)^\perp)^\perp = \pi_S(\mathcal{C}^\perp)$, which is true if and only if $\pi_S(\mathcal{C}^\perp)$ is a subspace of $\mathbb{F}_q^{|S|}$. This is equivalent to π_S being a linear map, and it is fairly trivial to see that this is the case.

Next, we define an extension map $\tau_S : \pi_S(\mathbb{F}_q^n) \to \mathbb{F}_q^n$ as follows: for any input $w \in \pi_S(\mathbb{F}_q^n)$, $\tau_S(w)$ will be the unique vector with the entries of w, in order, as the entries indexed by S, and zeroes in entries indexed by $[n] \setminus S$. For example, if $n = 4$ and $S = \{2, 4\}$, then $\tau_S((w_1, w_2)) = (0, w_1, 0, w_2)$. Importantly, τ_S is injective and $\pi_S(\tau_S(w)) = w$ for any $w \in \pi_S(\mathbb{F}_q^n)$.

Now, take any $w \in \pi_S(\mathcal{C}^\perp)^\perp$. For all $y \in \pi_S(\mathcal{C}^\perp)$, we have

$$\sum_{i=1}^{|S|} y_i w_i = 0.$$

Take $v = \tau_S(w)$. We have for all $x \in \mathcal{C}^\perp$ that

$$\sum_{i=1}^{n} x_i v_i = \sum_{i \in S} x_i v_i + \sum_{i \notin S} x_i \cdot 0 = \sum_{i=1}^{|S|} \pi_S(x)_i w_i = 0.$$

and so $v \in \mathcal{C}$. Since $v_i = 0$ for all $i \in [n] \setminus S$, we have $v \in \mathcal{C}(S)$, and so $w = \pi_S(v) \in \pi_S(\mathcal{C}(S))$.

($\supseteq$) Take any $w \in \pi_S(\mathcal{C}^\perp)$ and an arbitrary representative $v \in \mathcal{C}^\perp$ of w, i.e. $\pi_S(v) = w$. We know $\langle c, v \rangle = 0$ for all $c \in \mathcal{C}$. In particular, this is true for all $x \in \mathcal{C}(S)$, i.e.

$$\sum_{i \in S} x_i v_i = 0$$

which implies

$$\sum_{i=1}^{|S|} \pi_S(x)_i \pi_S(v)_i = \sum_{i=1}^{|S|} \pi_S(x)_i w_i = 0$$

for all $x \in \mathcal{C}(S)$. Since $\pi_S(\mathcal{C}(S)) = \{\pi_S(x) : x \in \mathcal{C}(S)\}$, this implies $\langle y, w \rangle = 0$ for all $y \in \pi_S(\mathcal{C}(S))$, and so $w \in \pi_S(\mathcal{C}(S))^\perp$. □

Proposition 47. Let $\mathcal{C} \leq \mathbb{F}_q^n$ with generator matrix G and let $S \subseteq [n]$. We have

$$\dim \pi_S(\mathcal{C}) = |S| - \dim \mathcal{C}^\perp(S).$$

Proof. First of all, basic knowledge of the orthogonal complement tells us that

$$\begin{aligned} &\dim \pi_S(\mathcal{C}) + \dim \pi_S(\mathcal{C})^\perp = |S| \\ \Longrightarrow &\dim \pi_S(\mathcal{C}) = |S| - \dim \pi_S(\mathcal{C})^\perp. \end{aligned}$$

Applying Proposition 46 to $\mathcal{C}^\perp$ and taking the orthogonal complement on both sides of the resulting equation, we find

$$\pi_S(\mathcal{C}^\perp(S)) = \pi_S(\mathcal{C})^\perp$$

and so also their dimensions are equal:

$$\dim \pi_S(\mathcal{C}^\perp(S)) = \dim \pi_S(\mathcal{C})^\perp.$$

By Proposition 44, we have

$$\dim \mathcal{C}^\perp(S) = \dim \pi_S(\mathcal{C})^\perp$$

and we find

$$\dim \pi_S(\mathcal{C}) = |S| - \dim \mathcal{C}^\perp(S)$$

as desired. □

4.3 Matroid associated with a code

In order to make a connection between matroid theory and coding theory, we need to look at matroids that are in some sense associated with codes. Recall Example 1 and Definition 1; given a linear block code $\mathcal{C}$ with generator matrix G and parity-check matrix H, it is standard to associate with this code the matroid M generated by the columns of G.

Definition 25. Let $\mathcal{C} \leq \mathbb{F}_q^n$ with generator matrix G. The matroid $M(\mathcal{C}) = ([n], r)$ associated with $\mathcal{C}$ is the matroid generated by the columns of G.

Remark. Although a code can be generated by different generator matrices, the associated matroid is the same no matter the choice of the generator matrix. However, one can start with non-equivalent codes but obtain the same associated matroid.

The matroid associated with a linear block code $\mathcal{C}$ turns out to be an interesting object to study; many invariants from the code can be retrieved from its associated matroid. A number of such results, such as the ability to retrieve a code's weight distribution from its associated matroid, are discussed by Jurrius [3]. Later in this section, we will explicitly show one such connection between a code $\mathcal{C}$ and its associated matroid, however we will discuss some examples first.

Example 11. Let $\mathcal{C} \leq \mathbb{F}_q^n$ be an MDS code of dimension k with generator matrix G. A well-known property of MDS codes is that any selection of k or fewer columns of the generator matrix is linearly independent; this implies the corresponding matroid is precisely the uniform matroid $U_{n,k}$.

Example 12. Let us return to Example 10, where we discussed the code $\mathcal{C}$ generated by the matrix

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

We will index the columns of G by the numbers $\{1, 2, 3, 4, 5\}$. We could now list a number of objects that have been introduced in previous chapters. For example, its collection of bases would be

$$\mathcal{B}(M(\mathcal{C})) = \{123, 124, 125, 135, 145, 234, 235, 345\}$$

and its collection of circuits would be

$$\mathcal{C}(M(\mathcal{C})) = \{134, 245, 1235\}.$$

Let us now consider the code $\mathcal{C}^\perp$. The associated matroid $M(\mathcal{C}^\perp)$ is generated by the parity-check matrix

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

Again, we can identify its collection of bases as

$$\mathcal{B}(M(\mathcal{C}^\perp)) = \{45, 35, 34, 24, 23, 15, 14, 12\}$$

and its collection of circuits as

$$\mathcal{C}(M(\mathcal{C}^\perp) = \{13, 25, 124, 145, 234, 345\}.$$

In this example, one might notice two peculiarities.

- The bases of $M(\mathcal{C}^\perp)$ are the complements of the bases of $M(\mathcal{C})$, suggesting that these matroids are dual.
- More subtly, the circuits of $M(\mathcal{C})$ are precisely the supports of the minimal codewords of $\mathcal{C}^\perp$; the same holds reversely as well.

These peculiarities turn out to be true in general and are the subject of the remainder of this section.

Proposition 48. Let $\mathcal{C} \leq \mathbb{F}_q^n$ with generator matrix G and consider the matroid $M(\mathcal{C}) = ([n], r)$. Let $S \subseteq [n]$. We have

$$r(S) = \dim \pi_S(C).$$

Proof. $\pi_S(\mathcal{C})$ is a code by Proposition 43. Denote by G_S the matrix containing the columns of G indexed by S; it is easy to see that G_S is a generator matrix for $\pi_S(\mathcal{C})$. Then the dimension of $\pi_S(\mathcal{C})$ is the rank of G_S, which is precisely $r(S)$ by Definition 6. □

Proposition 49. Let $C \leq \mathbb{F}_q^n$ be a linear block code with associated matroid $M(\mathcal{C})$. We have that $M(\mathcal{C}^\perp) = M(\mathcal{C})^*$, i.e. the matroids generated by the generator matrix G and the parity-check matrix H are dual matroids.

Proof. For brevity, we will denote $M = M(\mathcal{C})$ and $M^* = M(\mathcal{C}^\perp)$. These matroids both have ground set $E = [n]$, and their rank functions will be denoted by r and r^* respectively. Denote $\dim \mathcal{C} = k$; this implies $\dim \mathcal{C}^\perp = n - k$, and Proposition 48 tells us that $r(M) = k$ and $r^*(M^*) = n - k$.

To prove that M and M^* are dual matroids, we will show their rank functions correspond as in Proposition 15. In particular, we will leverage the dimensionality results of the previous section to show that the following equality holds:

$$r^*(E \setminus S) = |E \setminus S| + r(S) - r(M).$$

By Proposition 48, we have

$$r^*(E \setminus S) = \dim \pi_{E \setminus S}(\mathcal{C}^\perp).$$

Proposition 45 allows us to rewrite the right hand side as follows:

$$r^*(E \setminus S) = \dim \mathcal{C}^\perp - \dim \mathcal{C}^\perp(S)$$

The quantity $\dim \mathcal{C}^\perp(S)$ appears in Proposition 47 and can be rewritten as $|S| - \dim \pi_S(\mathcal{C})$; recognising the latter term as $-r(S)$ by Proposition 48, this finally gives

$$r^*(E \setminus S) = \dim \mathcal{C}^\perp - (|S| - r(S)).$$

Note that $\dim \mathcal{C}^\perp = n - k = |E| - r(M)$. As such, we have

$$\begin{aligned} r^*(E \setminus S) &= |E| - r(M) - |S| + r(S) \\ &= |E \setminus S| + r(S) - r(M) \end{aligned}$$

as desired. □

Proposition 50. Let $C \leq \mathbb{F}_q^n$ be a linear block code with generator matrix G and parity-check matrix H. Denote its associated matroid and the dual matroid by $M = ([n], r)$ and $M^* = ([n], r^*)$ respectively. We have that $v \in \mathcal{C}$ is a minimal codeword of $\mathcal{C}$ if and only if $\sigma(v)$ is a circuit of M^*.

Proof. ($\Longrightarrow$) Let $v \in \mathcal{C}$ be minimal, i.e. there is no codeword w such that $\sigma(w) \subset \sigma(v)$. Then we know $vH^T = 0$, i.e. the columns of H indexed by $\sigma(v)$ are dependent. Furthermore, no proper subset of these columns is dependent, otherwise there would be a codeword with support properly contained in $\sigma(v)$.

As such, the columns of H indexed by $\sigma(v)$ are a minimal dependent set, so $\sigma(v)$ is a circuit of M^*.

($\Longleftarrow$) Let C be some circuit of M^*. That means the columns of H indexed by C are linearly dependent, and we can write this dependence relation in the form $vH^T = 0$ for some vector v. This vector v will have non-zero coordinates in the entries indexed by C and zeroes everywhere else. In particular, v is a codeword. Since C is minimal, there exists no dependence relation in any set of columns indexed by a proper subset of C, so there exists no codeword with support properly contained in $\sigma(v) = C$. That is, v is a minimal codeword. $\square$

Remark. Recall from Section 3.4 that circuits of M^* are exactly the complements of hyperplanes of M. As such, any minimal codeword of $\mathcal{C}$ has support precisely $E \setminus H$, where H is some hyperplane of M. Now, let $H_1.H_2, \ldots, H_m$ denote a collection of hyperplanes of M, and let v^i be the codewords with support $\sigma(v^i) = E \setminus H_i$. For the flat F that appears as the intersection of the hyperplanes $H_1, \ldots, H_m$, we have

$$\begin{aligned} E \setminus F &= E \setminus \left(\bigcap_{i=1}^{m} H_i \right) \\ &= \bigcup_{i=1}^{m} E \setminus H_i \\ &= \bigcup_{i=1}^{m} \sigma(v^i), \end{aligned}$$

i.e. the space supported on the complement of F is generated by the minimal codewords $v^1, \ldots, v^m$.

Proposition 50 can be generalised neatly.

Proposition 51. Let $\mathcal{C} \leq \mathbb{F}_q^n$. Denote its associated matroid and the dual matroid by $M = ([n], r)$ and $M^* = ([n], r^*)$ respectively. Let $U \subseteq [n]$. We have

$$U \text{ is a cyclic set of } M \iff \pi_U(\mathcal{C}^\perp(U)) \text{ is non-degenerate.}$$

Furthermore, $\dim \pi_U(\mathcal{C}^\perp(U)) = |U| - r(U)$.

Proof. ($\Longrightarrow$) Let U be a cyclic set of $M(\mathcal{C})$. Proposition 23 tells us that U is a union of circuits, i.e.

$$U = \bigcup_{i=1}^{m} C_i$$

for some collection of circuits $C_1, \ldots, C_m$. By Proposition 50, $\mathcal{C}^\perp$ contains a codeword v^i with the property that $\sigma(v^i) = C_i$. This means $v^i \in \pi_U(\mathcal{C}^\perp(U))$

and

$$U = \bigcup_{i=1}^{m} \sigma(v^i) \subseteq \bigcup_{v \in \pi_U(\mathcal{C}^\perp(U))} \sigma(v) \subseteq U,$$

i.e. $\pi_U(\mathcal{C}^\perp(U))$ is non-degenerate.

($\Longleftarrow$) We will show the contrapositive statement. To that end, let X be a non-cyclic set of $M(\mathcal{C})$. That means there exists some $x \in X$ such that $r(X \setminus \{x\}) = r(X) - 1$. Propositions 47 and 48 allow us to rewrite this equality as

$$\begin{aligned} r(X \setminus \{x\}) &= r(X) - 1 \\ \dim \pi_{X\setminus\{x\}}(\mathcal{C}) &= \dim \pi_X(\mathcal{C}) - 1 \\ |X \setminus \{x\}| - \dim \mathcal{C}^\perp(X \setminus \{x\}) &= |X| - \dim \mathcal{C}^\perp(X) - 1 \\ |X| - 1 - \dim \mathcal{C}^\perp(X \setminus \{x\}) &= |X| - \dim \mathcal{C}^\perp(X) - 1 \\ \dim \mathcal{C}^\perp(X \setminus \{x\}) &= \dim \mathcal{C}^\perp(X). \end{aligned}$$

Note that $\mathcal{C}^\perp(X \setminus \{x\})$ is a subspace of $\mathcal{C}^\perp(X)$; equality of their dimensions implies they are the same space, i.e. $\mathcal{C}^\perp(X \setminus \{x\}) = \mathcal{C}^\perp(X)$. But this means that $v_x = 0$ for all $v \in \mathcal{C}^\perp(X)$, which implies that $\pi_X(\mathcal{C}^\perp(X))$ is degenerate.

Finally, we can apply Propositions 15, 44 and 45 to find

$$\begin{aligned} \dim \pi_U(\mathcal{C}^\perp(U)) &= \dim \mathcal{C}^\perp(U) \\ &= \dim \mathcal{C}^\perp - \dim \pi_{E\setminus U}(\mathcal{C}^\perp) \\ &= n - r(M) - r^*(E \setminus U) \\ &= n - r(M) - (|E \setminus U| + r(U) - r(M)) \\ &= n - r(M) - n + |U| - r(U) + r(M) \\ &= |U| - r(U) \end{aligned}$$

as desired. □

We can use Theorem 1 to obtain a dual result for flats of $M(\mathcal{C})$.

Proposition 52. Let $\mathcal{C} \leq \mathbb{F}_q^n$. Denote its associated matroid and the dual matroid by $M = ([n], r)$ and $M^* = ([n], r^*)$ respectively. Let $F \subseteq [n]$. We have

$$F \text{ is a flat of } M \iff \pi_{E\setminus F}(\mathcal{C}(E \setminus F)) \text{ is non-degenerate.}$$

Furthermore, $\dim \pi_{E\setminus F}(\mathcal{C}(E \setminus F)) = r(M) - r(F)$.

Proof. Theorem 1 states that F is a flat of M if and only if $E \setminus F$ is a cyclic set of M^*. As such, the main claim follows from applying Proposition 51 to the

cyclic set $E \setminus F$ of M^*. For its dimension, we apply Proposition 15 to find

$$\begin{aligned}\dim \pi_{E\setminus F}(\mathcal{C}(E \setminus F)) &= |E \setminus F| - r^*(E \setminus F) \\ &= |E \setminus F| - (|E \setminus F| + r(F) - r(M)) \\ &= r(M) - r(F)\end{aligned}$$

as desired. □

Finally, we can combine Propositions 51 and 52 to obtain a result that describes the relationship between the cyclic flats of a code's associated matroid and the non-degeneracy of certain subcodes.

Theorem 3. Let $\mathcal{C} \leq \mathbb{F}_q^n$ and denote its associated matroid by $M = ([n], r)$. Let $Z \subseteq [n]$. We have that Z is a cyclic flat of M if and only if $\pi_Z(\mathcal{C}^\perp(Z))$ and $\pi_{E\setminus Z}(\mathcal{C}(E\setminus Z))$ are non-degenerate and of dimension $|Z|-r(Z)$ and $r(M)-r(Z)$ respectively.

5 Constructing flats from cyclic flats

In this chapter, we will be presenting our main result: the ability to construct the lattice of flats of a matroid from its lattice of cyclic flats. This is technically not a new result, as this has been done before; see [8]. We have discovered a novel approach, using the framework of contraction, that allows us to formulate a more straightforward and simple construction.

However, one might wonder why such a construction is interesting. As noted in Section 4.3, a code's associated matroid can be used to retrieve invariants of said code. One such application is that a code's weight distribution can be retrieved from a certain polynomial invariant of its associated matroid that can be determined through the flats of said matroid. However, in Section 3.3, we included a cryptomorphic axiom system for matroids purely based on its lattice of cyclic flats; as such, one could expect the same to be possible by only considering the matroid's cyclic flats. This has served as motivation to find a way to reconstruct the flats of a matroid from its cyclic flats. We should note that constructing one class of sets from a second, different class of sets should generally not be expected to be a trivial endeavour. We attempted to illustrate this in Section 2.2, where we introduced the term *cryptomorphic* axiom systems exactly for those situations where it is possible to change between perspectives, even though the equivalence between these perspectives is non-obvious.

For most results contained in this section, we will require the assumption that $\varnothing$ and E are cyclic flats of the matroid $M = (E, r)$; following Proposition 30, this means we are only considering matroids that have no loops or coloops.

Definition 26. Let $M = (E, r)$ be a matroid and let $X \subseteq E$. The set $X \backslash \mathrm{cyc}(X)$ is called the *free part* of X and denoted $\mathrm{free}(X)$.

Proposition 53. Let $M = (E, r)$ be a matroid and let $X \subseteq E$. We have $r(\mathrm{free}(X)) = |\mathrm{free}(X)|$, i.e. the free part of X is independent.

Proof. We will argue by contradiction. Suppose $\mathrm{free}(X)$ were dependent; then it must contain some circuit C. But then $C \subseteq \mathrm{free}(X) \subseteq X$, and Proposition 23 tells us that $C \subseteq \mathrm{cyc}(X)$; a contradiction. Therefore, $\mathrm{free}(X)$ is independent. □

Corollary 2. $X \subseteq E$ is independent $\iff \mathrm{cyc}(X) = \varnothing$.

Proposition 54. Let $M = (E, r)$ be a matroid and let $X \subseteq E$. We have

$$r(X) = r(\mathrm{cyc}(X)) + |\mathrm{free}(X)|$$

Proof. $\mathrm{free}(X)$ does not contain any circuits and no subset of it forms a circuit with any subset of $\mathrm{cyc}(X)$; if this did occur, the relevant elements would be contained in $\mathrm{cyc}(X)$ by definition. Therefore, we can add the elements of $\mathrm{free}(X)$ to $\mathrm{cyc}(X)$ one-by-one, in any order, and at no point will we close a circuit; this implies the rank will increase after every addition of an element. □

Proposition 55. Let $M = (E, r)$ be a matroid without loops, and let $F \in \mathcal{F}(M)$. We have that $\text{free}(F) \in \mathcal{F}(M)$.

Proof. Note that $\text{cl}(\text{free}(F)) \subseteq \text{cl}(F) = F$. Suppose $\text{free}(F)$ is not a flat; that means there exists some $e \in F \setminus \text{free}(F) = \text{cyc}(F)$ which we can add to $\text{free}(F)$ without increasing its rank. The set $\text{free}(F) \cup \{e\}$ is contained in F and is dependent, as it was constructed by adding an element to $\text{free}(F)$ without increasing the rank. Therefore, Proposition 6 tells us we can find a fundamental circuit $C(e, \text{free}(F))$; since M has no loops, this circuit must contain at least one element from $\text{free}(F)$. But that means we have obtained a circuit $C \in F$ but $C \notin \text{cyc}(F)$, a contradiction. Therefore, $\text{free}(F)$ is a flat. □

Proposition 55 is an important result to state the direction we are about to head in. Our central idea for recognising whether or not a set is flat has to do with 'filtering out', in some sense, its cyclic core, and then checking whether or not the remaining elements form an independent flat. This does require us to be able to recognise when a set is an independent flat; this is the subject of the next proposition.

Proposition 56. Let $M = (E, r)$ be a matroid without loops or coloops. $X \subseteq E$ is an independent flat of M if and only if for every cyclic flat $Z \neq \varnothing$, it holds that

$$|X \cap Z| < r(Z).$$

Proof. Denote the lattices of (cyclic) flats of M by $\mathcal{F}$ and $\mathcal{Z}$ respectively. Our proof consists of two parts.

($\Longrightarrow$) Let $X \subseteq E$ be an independent flat of M and let $Z \neq \varnothing$ be any cyclic flat of M. Since X is independent, Corollary 2 tells us that $\text{cyc}(X) = \varnothing$; therefore, X cannot contain Z. Then, flatness of X implies $r(X) < r(X \cup Z)$. Additionally, since X is independent and $X \cap Z \subseteq X$, we have that $r(X) = |X|$ and $r(X \cap Z) = |X \cap Z|$. We can now apply submodularity to find our result:

$$\begin{aligned} r(X \cap Z) + r(X \cup Z) &\leq r(X) + r(Z) \\ |X \cap Z| + r(X) &< |X| + r(Z) \\ |X \cap Z| + |X| &< |X| + r(Z) \\ |X \cap Z| &< r(Z). \end{aligned}$$

($\Longleftarrow$) We will use Proposition 28. First of all, note that for $Z = \varnothing$, the expression $r(Z) - |X \cap Z|$ evaluates to 0. For any other cyclic flat Z, we know that $r(Z) - |X \cap Z| > 0$, and therefore

$$r(X) = |X| + \min_{Z \in \mathcal{Z}} \{r(Z) - |X \cap Z|\} = |X|$$

and as such, $|X|$ is independent. Additionally, consider Proposition 28 on the set $X \cup \{e\}$ for any $e \in E \setminus X$:

$$r(X \cup \{e\}) = |X \cup \{e\}| + \min_{Z \in \mathcal{Z}} \{r(Z) - |(X \cup \{e\}) \cap Z|\}.$$

For $Z = \varnothing$, again we would have $r(\varnothing) - |(X \cup \{e\}) \cap \varnothing| = r(\varnothing) - |\varnothing| = 0$. This means, were the minimum to be attained in $Z = \varnothing$, then $r(X \cup \{e\}) = |X \cup \{e\}| = |X| + 1$ and we would be happy. As such, we can exclude $Z = \varnothing$ and continue to rewrite

$$\begin{aligned} r(X \cup \{e\}) &= |X \cup \{e\}| + \min_{Z \neq \varnothing} \{r(Z) - |(X \cup \{e\}) \cap Z|\} \\ &\geq |X| + 1 + \min_{Z \neq \varnothing} \{r(Z) - |X \cap Z| - 1\} \\ &= |X| + \min_{Z \neq \varnothing} \{r(Z) - |X \cap Z|\} > |X| \end{aligned}$$

and as such, we have that $r(X \cup \{e\}) = |X| + 1$. Therefore, X is a flat and we are done. □

Proposition 56 gives a criterion which can be used to construct all independent flats. The required 'filtering' process, as discussed prior to the previous proposition, will be done through contraction.

Proposition 57. Let $M = (E, r)$ be a matroid. Let $Z' \in \mathcal{Z}(M)$ and consider the contracted matroid $M/Z' = (E \setminus Z', \rho)$. We have that $Z \in \mathcal{Z}(M/Z')$ if and only if $Z \cup Z' \in \mathcal{Z}(M)$. In particular, this implies that if M has no loops or coloops, then M/Z' has no loops or coloops either.

Proof. The initial statement is a special case of Proposition 41. Moreover, this statement implies the following:

- Since E is a cyclic flat of M, this means $E \setminus Z'$ is a cyclic flat of M/Z';
- Since Z' is a cyclic flat of M, this means $\varnothing = Z' \setminus Z'$ is a cyclic flat of M/Z'.

Proposition 30 then implies that M/Z' has no loops or coloops. □

Proposition 57 tells us a couple of things. First of all, it is easy to construct the lattice of cyclic flats of a matroid minor obtained through contracting by a cyclic flat Z': simply take all cyclic flats containing Z' and delete all elements belonging to Z'. Additionally, Proposition 18 tells us that

$$\rho(Z) = r(Z \cup Z') - r(Z),$$

which allows us to obtain their ranks as well. Combining this knowledge and the fact that M/Z' has no loops or coloops by Proposition 57, we can apply Proposition 56 to any matroid minor obtained through contracting by a cyclic flat. This gives us the following result:

Proposition 58. Let $M = (E, r)$ be a matroid without loops or coloops. Let $Z' \in \mathcal{Z}(M)$ and consider the contracted matroid $M/Z' = (E \setminus Z', \rho)$. $X \subseteq E \setminus Z'$ is an independent flat of M/Z' if and only if for every cyclic flat $Z \in \mathcal{Z}(M/Z') \setminus \{\varnothing\}$, it holds that

$$|X \cap Z| < \rho(Z).$$

Definition 27. Let $M = (E, r)$ be a matroid and let $X \subseteq E$. Consider the collection Z_X of all cyclic flats Z contained in X, i.e.

$$Z_X = \{Z \in \mathcal{Z}(M) : Z \subseteq X\}.$$

If Z_X contains a unique cyclic flat Z of maximum cardinality, we call Z the *largest cyclic flat* contained in X and denote it by $\text{lcf}(X)$.

Proposition 59. If X is a flat, we have $\text{lcf}(X) = \text{cyc}(X)$.

Proof. The proofs of these propositions are straightforward from Propositions 23 and 56. □

In the next theorem, we will be combining everything discussed in this section so far. The resulting statement finishes our construction of the lattice of flats from the lattice of cyclic flats; remarkably, a relatively simple criterion allows us to perform a process that is difficult in general.

Theorem 4. Let $M = (E, r)$ be a matroid without loops or coloops. $X \subseteq E$ is a flat of M if and only if $\text{lcf}(X)$ exists and for every cyclic flat $Z \supset \text{lcf}(X)$, it holds that

$$|(X \setminus \text{lcf}(X)) \cap Z| < r(Z) - r(\text{lcf}(X)).$$

Proof. The existence of $\text{lcf}(X)$ is important here, as we might be trying to determine the flatness of a set X containing multiple cyclic flats of maximum cardinality. However, Proposition 59 tells us that if X is a flat, then it contains a unique cyclic flat of maximum cardinality: $\text{cyc}(X)$. As such, $\text{lcf}(X)$ not existing immediately disqualifies X from being a flat.

Next, suppose $\text{lcf}(X)$ does indeed exist uniquely. If $\text{lcf}(X) = \varnothing$, then Proposition 56 immediately gives the desired result. In case $\text{lcf}(X) \neq \varnothing$, then we can apply Proposition 58 to check if $X \setminus \text{lcf}(X)$ is an independent flat of $M/\text{lcf}(X)$; if this is true, then Proposition 38 gives us that $X \setminus \text{lcf}(X) \cup \text{lcf}(X) = X$ is a flat of M. This process is captured by our provided criterion

$$|(X \setminus \text{lcf}(X)) \cap Z| < r(Z) - r(\text{lcf}(X)),$$

which is a rewritten version of the criterion in Proposition 58 using the knowledge of a contracted matroid's rank function from Proposition 18. As expected, substituting $\text{lcf}(X) = \varnothing$ gives the same criterion as in Proposition 56. □

Remark. For every flat X, the criterion can be rewritten in the nicer form

$$|\text{free}(X) \cap Z| < r(Z) - r(\text{cyc}(X))$$

for all $Z \supseteq \text{cyc}(X)$. Finally, Proposition 54 allows us to retrieve the rank of our obtained flats X, as

$$r(X) = r(\text{cyc}(X)) + |\text{free}(X)|.$$

Finally, it is only natural to try and reincorporate loops and coloops into the construction.

Proposition 60. Let $M = (E, r)$ be a matroid. If $e \in E$ is a loop of M, then every flat $F \in \mathcal{F}(M)$ contains e.

Proof. We will argue by contradiction. Suppose there is some flat F that does not contain e. Note that we have $r(\varnothing \cup \{e\}) = r(\{e\}) = 0 = r(\varnothing)$; then, since $\varnothing \subseteq F$, Corollary 1(i) implies $r(F \cup \{e\}) = r(F)$, which means F is not a flat. □

Proposition 60 implies that all flats contain all loops, and in particular all cyclic flats contain all loops. As such, the collection of loops of a matroid M can be immediately identified from the lattice of cyclic flats as the bottom element $0_{\mathcal{Z}}$ of the lattice, i.e. $\mathcal{L}(M) = 0_{\mathcal{Z}}$. Then, it is possible to remove these loops from every cyclic flat and apply Theorem 4 to construct the flats of the restricted matroid $M|(E \setminus \mathcal{L}(M))$, and we can add $\mathcal{L}(M)$ to every constructed flat to obtain the flats of M.

Unfortunately, it is not so simple to reincorporate the coloops of M. Let us denote the collection of coloops of M by $\mathcal{L}(M^*)$, reflecting Proposition 29 where we showed that the coloops of M are precisely the loops of M^*. By this definition, coloops are precisely those elements of M that are in no circuits. Since cyclic sets, and cyclic flats in particular, are unions of circuits by Proposition 23, this means the coloops of M do not show up in any cyclic flat of M. As such, in the situation where one is only given a lattice of cyclic flats of a matroid and asked to reconstruct the flats, it is impossible to reincorporate the coloops.

6 Conclusion

In this thesis, we have provided a basic overview of codes and their associated matroids, as well as a more thorough exploration of matroid theory. This has led to a result connecting the cyclic flats of a matroid's associated code to the non-degeneracy of certain subcodes, as well as a novel way to construct the lattice of flats of a matroid without loops or coloops through its lattice of cyclic flats.

It seems there is significantly more to be understood regarding the information about a matroid one can learn from just its lattice of cyclic flats. As such, this is an interesting avenue for future research.

References

[1] R. Freij-Hollanti and O. Kuznetsova, "Information hiding using matroid theory," *Advances in Applied Mathematics*, vol. 129, p. 102205, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0196885821000439

[2] R. Freij-Hollanti, C. Hollanti, and T. Westerbäck, "Matroid theory and storage codes: Bounds and constructions," 2017.

[3] R. Jurrius, "Codes, arrangements, matroids, and their polynomial links," Ph.D. dissertation, Eindhoven University of Technology, 2012.

[4] J. Oxley, *Matroid Theory*. Oxford University Press, 2011.

[5] F. Ardila, *Matroid theory*. Lecture notes, San Francisco State University and Universidad de los Andes, 2007. [Online]. Available: https://fardila.com/Clase/Matroids/lectures.html

[6] R. J. Wilson, *Introduction to Graph Theory*. Pearson Education Limited, 2010.

[7] J. Bonin and A. de Mier, "The lattice of cyclic flats of a matroid," *Annals of Combinatorics*, vol. 12, 07 2005.

[8] R. Freij-Hollanti, M. Grezet, C. Hollanti, and T. Westerbäck, "Cyclic flats of binary matroids," *Advances in Applied Mathematics*, vol. 127, p. 102165, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0196885821000038