A Quick Taste of Matroid Theory

Alan Yan
DRP Advisor: Noah Kravitz

April 26, 2022

Abstract

In this paper, we present the basics of matroid theory. We begin by presenting the basic definitions for matroids and proving that the matroid-like objects that we define are all equivalent. We then present some of the classical examples of matroids which come from linear algebra and graph theory. We conclude with applications and connections of matroids to combinatorial optimization and convex geometry.

Contents

1 Introduction

Matroids can be thought as a combinatorial object which abstracts the properties of linear independence in vector spaces. Despite the seemingly limited scope of this interpretation, matroids successfully describe many structures and objects all throughout mathematics. Indeed, in later sections we will show connections and examples of matroids to graph theory, combinatorial optimization, and convex geometry. Due to the length of this paper, it will be impossible to cover all of matroid theory, or even a small part of it in large detail. For more details, we redirect the diligent reader to the wonderful monograph [4] which is the main basis for these notes.

1.1 Basic Notions

We first define the basic notion of a matroid. The axioms in Definition 1 attempt to generalize linear independence by extracting the main properties satisfied by linearly independent sets of vectors.

Definition 1. A *matroid* is an ordered pair $M = (E, \mathcal{I})$ consisting of a finite set E and a collection of subsets $\mathcal{I} \subset 2^E$ called *indepedent sets* which satisfy the following three properties:

(I1) (Non-empty) $\mathcal{I}$ is non-empty,

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

(I3) (Augmentation) If $X, Y \in \mathcal{I}$ and $|X| > |Y|$, then there exists some element $e \in X - Y$ such that $Y \cup \{e\} \in \mathcal{I}$.

Given a matroid $M = (E, \mathcal{I})$, we call a subset $X \subseteq E$ a *dependent set* if and only if $X \notin \mathcal{I}$. To maintain the analogy with linear algebra, we define a basis $B \in \mathcal{I}$ to be a maximal independent set. In vector spaces, bases are have the same cardinality. The proof of this fact in the matroid case is exactly the same as in the vector space case.

Proposition 1. *Let $M = (E, \mathcal{I})$ be a matroid and B_1, B_2 are bases. Then B_1 and B_2 have the same cardinality.*

Proof. If $|B_1| < |B_2|$, then by (I3), there is a larger set containing B_1 which is independent. But this contradicts the maximality of B_1. This suffices for the proof. $\square$

In the sequel, we define several other matroid-like combinatorial objects with their own sets of axioms. The examples we give are *cirtroids*, *basetroids*, *ranktroids*, *clotroids*, and *flatroids* which are defined via *circuits*, *bases*, *ranks*, *closures*, and *flats*. These terms will be fully defined in the sequel. These objects end up being crytomorphically equivalent to the definition of a matroid. The names we've given these objects are slight play-on-words of the word matroid depending on how the object is defined. We warn the reader that the naming convention used for these objects is not standard in the literature.

1.2 A Miscellany of Matroid-like Objects

In a matroid $M = (E, \mathcal{I})$, we say $C \subseteq E$ is a circuit if it is a minimal dependent set. By abstracting the main properties of circuits, we can cook up Definition 2.

Definition 2. A *cirtroid* is an ordered pair $M = (E, \mathcal{C})$ consisting of a finite set E and a collection of subsets $\mathcal{C} \subset 2^E$ called the *circuits* which satisfy the following three properties:

(C1) (Abundance) $\emptyset \notin \mathcal{C}$.

(C2) (Minimality) If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$.

(C3) (Circuit Elimination) If $C_1, C_2 \in \mathcal{C}$ are distinct and $e \in C_1 \cap C_2$, then there is a $C_3 \in \mathcal{C}$ such that $C_3 \subset (C_1 \cup C_2) - \{e\}$.

Recall that a basis $B \subseteq E$ is a maximal independent set. By restricting our attention to bases, it is not hard to isolate the main axioms in Definition 3.

Definition 3. A *basetroid* is an ordered pair $M = (E, \mathcal{B})$ consisting of a finite set E and a collection of subsets $\mathcal{B} \subset 2^E$ called *the bases* which satisfy the following three properties.

(B1) (Non-empty) $\mathcal{B}$ is non-empty.

(B2) (Basis-Exchange) If B_1 and B_2 are members of $\mathcal{B}$ and $x \in B_1 - B_2$, then there is an element y of $B_2 - B_1$ such that $(B_1 - x) \cup y \in \mathcal{B}$.

(B3) (Maximality) If $B_1, B_2 \in \mathcal{B}$ and $B_1 \subseteq B_2$, then $B_1 = B_2$.

One non-trivial result about basetroids is that all members of $\mathcal{B}$ have the same cardinality. Note that we've seen this property with respect to matroid bases in Proposition 1. This fits our intuition about the cardinality of a basis of a vector space as the dimension of the vector space.

Proposition 2. *Let $M = (E, \mathcal{B})$ be a basetroid. Then all elements in $\mathcal{B}$ have the same cardinality.*

Proof. For the sake of contradiction, suppose there are distinct bases $B_1, B_2 \in \mathcal{B}$ with $|B_1| > |B_2|$. Pick such bases $B_1, B_2 \in \mathcal{B}$ such that $|B_1 - B_2|$ is minimized. Then there exists an element $x \in B_1 - B_2$. From (B3), there exists an element $y \in B_2 - B_1$ such that $B' := (B_1 - x) \cup y \in \mathcal{B}$. This basis satsifies $|B'| = |B_1| > |B_2|$, so B' and B_2 are still distinct. But, now we have $|B' - B_2| < |B_1 - B_2|$, which contradicts the minimality of B_1, B_2. This suffices for the proof. $\square$

For any subset $X \subseteq E$ of a matroid, we can define $r_M(E)$ to be the size of a maximal independent set in X. This value is well-defined from (I3). We call this the rank of E and is a proxy for the dimension of the space "spanned" by matroid elements. In Definition 4, we define a combinatorial object which isolates the main properties of the rank function with respect to a matroid r_M.

Definition 4. A *ranktroid* is an ordered pair $M = (E, r)$ consisting of a finite set E and a function $r : 2^E \to \mathbb{Z}_{\geq 0}$ called the rank function satisfying the following three properties.

(R1) (Set-Boundedness) If $X \subseteq E$, then $0 \leq r(X) \leq |X|$.

(R2) (Monotonicity) If $X \subseteq Y \subseteq E$, then $r(X) \leq r(Y)$.

(R3) (Submodularity) If $X, Y \subseteq E$, then $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$.

The rank function allows us to define a "topology" on a matroid. Indeed, we can define the *closure* of a set $X \subseteq E$ to be the set

$$\mathrm{clo}_M(X) := \{x \in E : r_M(X \cup x) = r_M(X)\}.$$

That is, the closure of X is the set of elements in X such that when added to X do not change the rank. The existence of the closure operator also defines a matroid-like object.

Definition 5. A *clotroid* is an ordered pair $M = (E, \text{clo})$ consisting of a finite set E and an operator $\text{clo} : 2^E \to 2^E$ called the *closure* satisfying the following four properties.

(CL1) (Increasing) $X \subseteq \text{clo}(X)$ for all $X \subseteq E$.

(CL2) (Monotonicity) If $A \subseteq B \subseteq E$, then $\text{clo}(A) \subseteq \text{clo}(B)$.

(CL3) (Idempotency) $\text{clo}(\text{clo}(X)) = \text{clo}(X)$ for all $X \subseteq E$.

(CL4) (Mac Lane-Steinitz exchange property) Let $A \subseteq E$ and $x \in E$. If $e \in \text{clo}(A \cup x) - \text{clo}(A)$, then $x \in \text{clo}(A \cup e)$.

Property (CL4) is known as the Mac Lane-Steinitz exchange property. Motivated by our knowledge of point-set topology, we can define a subset $X \subseteq E$ to be *closed* or a *flat* if $E = \text{clo}(E)$. This also defines a matroid-like object.

Definition 6. A *flatroid* is an ordered pair $M = (E, \mathcal{F})$ consisting of a finite set E and a collection $\mathcal{F} \subseteq 2^E$ called *flats* satisfying the following three properties:

(F1) (Fullness) $E \in \mathcal{F}$.

(F2) (Closed under Finite Intersections) If $F_1, F_2 \in \mathcal{F}$, then $F_1 \cap F_2 \in \mathcal{F}$.

(F3) (Partitioning under Covering Elements) If $F \in \mathcal{F}$ and $\{F_1, \ldots, F_k\}$ is the set of flats that cover F, then $\{F_1 - F, F_2 - F, \ldots, F_k - F\}$ partition $E - F$.

In (F3), when we say *cover*, we mean in the sense of the poset structure of $\mathcal{F}$.

Definition 7. A *poset* is an ordered pair $(P, \leq)$ where P is a finite set and $\leq$ is a binary relation satisfying three properties:

(P1) (Reflexivity) $x \leq x$ for all $x \in P$.

(P2) (Antisymmetry) $x \leq y$ and $y \leq x$ imply $x = y$ for any $x, y \in P$.

(P3) (Transitivity) If $x \leq y$, and $y \leq z$, then $x \leq z$.

When we write $x < y$, we mean $x \leq y$ and $x \neq y$. When we write $x \lessdot y$, we mean $x < y$ and if $x \leq z \leq y$ then $z \in \{x, y\}$. The last relation is the covering relation.

In Definition 6, the term *cover* was used with respect to the poset structure of $(\mathcal{F}, \subseteq)$ where $M = (E, \mathcal{F})$ is a flatroid. This poset of flats enjoys many nice properties including being a geometric lattice. We do not go into detail in this part of theory, and instead redirect the reader to [4].

Besides the objects we have currently defined, there are several other classical matroid-like objects defined using notions as hyperplanes, graphoids, convex hulls, and spanning sets. We do not discuss these constructions and instead direct the reader to [4] for more details. In the sequel, we prove that all of the matroid-like objects that we've defined are all equivalent.

1.3 Equivalence of Definitions

In Definition 8, we will define the isomorphisms between our matroid-like objects.

Definition 8. Let MAT, CIR, BAS, RANK, CLO, and FLAT be the class of matroids, cirtroids, basetroids, ranktroids, and clotroids, respectively. Then, we can define the following maps between these classes:

(i) $\varphi_{MC} : \mathsf{MAT} \to \mathsf{CIR}$ is the map which sends $M = (E, \mathcal{I})$ to $\varphi_{MC}(M) = (E, \mathcal{C})$ where $\mathcal{C}$ are the minimal dependent sets of M.

(ii) $\varphi_{CM} : \mathsf{CIR} \to \mathsf{MAT}$ is the map which sends $M = (E, \mathcal{C})$ to $\varphi_{CM}(M) = (E, \mathcal{I})$ where $\mathcal{I}$ are the subsets which contain no element of $\mathcal{C}$.

(iii) $\varphi_{MB} : \mathsf{MAT} \to \mathsf{BAS}$ is the map which sends $M = (E, \mathcal{I})$ to $\varphi_{MB}(M) = (E, \mathcal{B})$ where $\mathcal{B}$ are the maximal subsets of $\mathcal{I}$.

(iv) $\varphi_{BM} : \mathsf{BAS} \to \mathsf{MAT}$ is the map which sends $M = (E, \mathcal{B})$ to $\varphi_{BM}(M) = (E, \mathcal{I})$ where $\mathcal{I}$ are the subsets which are contained in some subset in $\mathcal{B}$.

(v) $\varphi_{MR} : \mathsf{MAT} \to \mathsf{RANK}$ is the map which sends $M = (E, \mathcal{I})$ to $\varphi_{MR}(M) = (E, r)$ where $r : 2^E \to \mathbb{Z}_{\geq 0}$ where $r(X)$ is the size of the maximal independent set in X for any $X \subseteq E$.

(vi) $\varphi_{RM} : \mathsf{RANK} \to \mathsf{MAT}$ is the map which sends $M = (E, r)$ to $\varphi_{RM}(M) = (E, \mathcal{I})$ where $\mathcal{I}$ is the collection of subsets $X \subseteq E$ satisfying $|X| = r(X)$.

(vii) $\varphi_{MG} : \mathsf{MAT} \to \mathsf{CLO}$ is the map which sends $M = (E, \mathcal{I})$ to $\varphi_{MG}(M) = (E, \mathrm{clo})$ where we define $\mathrm{clo}(X) := \{x \in E : r_M(X \cup x) = r_M(X)\}$ for all $X \subseteq E$.

(viii) $\varphi_{GM} : \mathsf{CLO} \to \mathsf{MAT}$ is the map which sends $M = (E, \mathrm{clo})$ to $\varphi_{GM}(M) = (E, \mathcal{I})$ where $\mathcal{I} := \{X \subseteq E : x \notin \mathrm{clo}(X - x) \text{ for all } x \in X\}$.

(ix) $\varphi_{GF} : \mathsf{CLO} \to \mathsf{FLAT}$ is the map which sends $M = (E, \mathrm{clo})$ to $\varphi_{CF}(M) = (E, \mathcal{F})$ where $\mathcal{F}$ is the collection of subsets which are equal to its closure.

(x) $\varphi_{FG} : \mathsf{FLAT} \to \mathsf{CLO}$ is the map which sends $M = (E, \mathcal{F})$ to $\phi_{FC}(M) = (E, \mathrm{clo})$ where $\mathrm{clo}(X)$ is the intersection of all elements in $\mathcal{F}$ containing X.

$$\begin{tikzcd}
 & & \mathsf{BASE} \arrow[d, bend right, "\varphi_{BM}"'] & \\
\mathsf{FLAT} \arrow[r, bend right, "\varphi_{FG}"'] & \mathsf{CLO} \arrow[l, bend right, "\varphi_{GF}"'] \arrow[r, bend left, "\varphi_{GM}"] & \mathsf{MAT} \arrow[l, bend left, "\varphi_{MG}"] \arrow[u, bend right, "\varphi_{MB}"'] \arrow[r, bend right, "\varphi_{MR}"'] \arrow[d, bend left, "\varphi_{MC}"] & \mathsf{RANK} \arrow[l, bend right, "\varphi_{RM}"'] \\
 & & \mathsf{CIR} \arrow[u, bend left, "\varphi_{CM}"] &
\end{tikzcd}$$

Note that it is not immediate obvious that the maps we defined in Definition 8 are well-defined. In order to prove that they provide one-to-one correspondences, we will prove that they are well defined and the diagram commutes. Clearly, to prove the diagram commutes, it suffices to prove that the minimal loops are inverses.

Proposition 3 (Equivalence of Matroids and Cirtroids). *The maps φ_{MC} and φ_{CM} are well-defined and inverses.*

Proof. We first prove that for $M \in \mathsf{MAT}$, the object $\varphi_{MC}(M) = (E, \mathcal{C})$ is a cirtroid.

(C1) Since $\emptyset \in \mathcal{I}$, we have that $\emptyset \notin \mathcal{C}$. This proves (C1)

(C2) Since $\mathcal{C}$ are minimal elements by construction, we immediately get (C2).

(C3) Suppose for the sake of contradiction that there are distinct $C_1, C_2 \in \mathcal{C}$ and $e \in C_1 \cap C_2$ such that $C_1 \cup C_2 - \{e\}$ contains no circuit. This implies that $C_1 \cup C_2 - \{e\} \in \mathcal{I}$. Since C_1, C_2 are distinct, without loss of generality there exists some element $f \in C_2 - C_1$ be an element in C_2 but not in C_1. The set $C_2 - \{f\}$ is independent as a proper subset of C_2. From (I3), we can keep appending elements from $C_1 \cup C_2 - e$ to $C_2 - \{f\}$ until it is an independent set of the same magnitude. However, this independent set cannot contain f since then it would contain C_2. This implies that this independent set is contained in $(C_1 \cup C_2) - \{e, f\}$ which has less elements than $(C_1 \cup C_2) - e$. This is a contradiction and (C3) must hold as well.

Now, we prove that for $M \in \mathsf{CIR}$ the object $\varphi_{CM}(M) = (E, \mathcal{I})$ is a matroid.

(I1) (I1) holds because $\emptyset$ is a proper subset of all circuits.

(I2) (I2) holds taking a subset only makes it harder to contain elements from $\mathcal{C}$.

(I3) For the sake of contradiction, suppose that there are $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$ such that for every $e \in I_2 - I_1$, we have $I_1 \cup e \notin \mathcal{I}$. Consider the subcollection of elements $I \in \mathcal{I}$ contained in $I_1 \cup I_2$ and having more elements than I_1. This collection is non-empty since I_2 is in this collection. Let I_3 be an element of the collection which minimizes $|I_1 - I_3|$. By our assumption, we have that $I_1 - I_3$ is not empty. Pick some element $e \in I_1 - I_3$. For any $f \in I_3 - I_1$ we define $T_f := (I_3 \cup e) - f$. Note that $I_1 \subset T_f \subset I_1 \cup I_2$ and $|I_1 - T_f| < |I_1 - I_3|$. By minimality, this implies that $T_f \notin \mathcal{I}$. Thus there is $C_f \in \mathcal{C}$ such that $C_f \subset T_f$. The circuit C_f satisfies $f \notin C_f$ since $f \notin T_f$. We also have $e \in C_f$ since otherwise $C_f \subset I_3 - f$ making $C_f \in \mathcal{I}$ since we've proved (I2). If $C_f \cap (I_3 - I_1) = \emptyset$, then

$$C_f \subset I_1 \cap (I_3 \cup e - f) \subset I_1$$

which is a contradiction. Thus, there is some $g \in C_f \cap (I_3 - I_1)$. The corresponding circuit C_g is distinct from C_f because $g \notin C_g$. Thus, from (C3), there is a $C \in \mathcal{C}$ with $C \subset (C_f \cup C_g) - e$. But $C_f, C_g \subset I_3 \cup \{e\}$ which implies that $C \subset I_3$, which is a contradiction. This proves that (I3) holds.

It suffices to prove that φ_{MC} and φ_{CM} are inverses. We first prove that $\varphi_{CM} \circ \varphi_{MC} = \mathrm{id}_{\mathsf{MAT}}$. Let $M \in \mathsf{M}$ and $\varphi_{MC}(M) = (E, \mathcal{C})$. We want to show that

$$\mathcal{I} = \text{subsets of } E \text{ which contain no member of } \mathcal{C}.$$

Every member of $\mathcal{I}$ contains no member of $\mathcal{C}$ since $\mathcal{C}$ are all dependent. Consider some subset $I \subset E$ that contains no member of $\mathcal{C}$. Then I cannot be dependent, or else it would contain a minimal dependent set (a circuit). Hence $I \in \mathcal{I}$ which proves that $\psi \circ \phi$ is the identity.

Now we only need to show that $\varphi_{MC} \circ \varphi_{CM} = \mathrm{id}_{\mathsf{CLO}}$. Suppose we start with a cirtroid $M = (E, \mathcal{C}) \in \mathsf{CIR}$. Let $\varphi_{CM}(M) = (E, \mathcal{I})$ be the corresponding matroid. We want to prove that the minimal subsets in $2^E - \mathcal{I}$ are exactly $\mathcal{C}$. Consider $C \in \mathcal{C}$. Then $C \notin \mathcal{I}$ since it contains itself. Moreover, it is a minimal element in this set because any proper subset will be in $\mathcal{I}$. Now consider an arbitrary minimal element of $2^E \backslash \mathcal{I}$. It cannot contain a circuit or else it wouldn't be minimal. However, this implies that it is independent, which is a contradiction. This suffices for the proof. $\square$

Proposition 4 (Matroids and Basetroids)**.** *The maps φ_{MB} and φ_{BM} are well-defined and inverses.*

Proof. Let $M = (E, \mathcal{I})$ be a matroid. We first prove that $\varphi_{MB}(M) = (E, \mathcal{B})$ is a basetroid.

(B1) Since $\emptyset \in \mathcal{I}$, there exists a maximal element of $\mathcal{I}$. Hence $\mathcal{B}$ is also non-empty.

(B2) Let $B_1, B_2 \in \mathcal{B}$. Then $B_1, B_2 \in \mathcal{I}$ and by Proposition 2, $|B_1| = |B_2|$. Let $x \in B_1 - B_2$ be an arbitrary element. Then $B_1 - x, B_2 \in \mathcal{I}$ with $|B_1 - x| < |B_2|$. (R3) implies that there is some $y \in B_2 - (B_1 - x) = B_2 - B_1$ such that $(B_1 - x) \cup y \in \mathcal{I}$. Note that $y \in B_2 - B_1$ since $x \notin B_2$. Thus, $(B_1 - x) \cup y$ has the same size as B_1, B_2. Proposition 2 implies that this must be a maximal independent set, and hence in $\mathcal{B}$. This completes the proof of (B2).

(B3) (B3) follows immediately from the construction of $\mathcal{B}$ as the maximal independent sets.

Let $M = (E, \mathcal{B})$ be a basetroid. We want to prove that $\varphi_{BM}(M) = (E, \mathcal{I})$ is a matroid.

(I1) (B1) implies that there is some $B \in \mathcal{B}$. Since $\emptyset \subseteq B$, we must have $\emptyset \in \mathcal{I}$, which proves (I1).

(I2) Suppose $I_1 \subseteq I_2 \in \mathcal{I}$. Then $I_2 \subseteq B_2$ for some $B_2 \in \mathcal{B}$. Then $I_1 \subseteq B_2$ as well. Thus $I1 \in \mathcal{I}$, proving (I2).

(I3) Consider $I_1, I_2 \in \mathcal{I}$ with $|I_1| + 1 = |I_2|$. Then there are subsets $E_1, E_2 \subseteq E$ such that $I_1 \sqcup E_1, I_2 \sqcup E_2 \in \mathcal{B}$. From Lemma 2, we must have $|E_1| = |E_2| + 1$. Now from $I_1 \sqcup E_1$, keep removing elements of E_1 until (B3) puts an element of I_2 into the set to keep it a basis. This has to happen eventually since $|E_1| > |E_2|$, and so E_2 will be exhausted before E_1 is exhausted. Taking the subset with this element and I_1 will be independent from (I2). This proves (I3).

In this case, the proof that the maps are inverses are more or less definitional, so we omit the proof. $\square$

Proposition 5 (Matroids and Ranktroids)**.** *The maps φ_{MR} and φ_{RM} are inverses.*

Proof. Let $M = (E, \mathcal{I})$ be a matroid. We will first prove that $\varphi_{MR}(M) = (E, r)$ is a ranktroid.

(R1) Any subset $X \subseteq E$, trivially contains the independent set $\emptyset$. Moreover, any independent set contained in X will have cardinality at most $|X|$. Hence $0 = |\emptyset| \leq r(X) \leq |X|$. This completes the proof of (R1).

(R2) Suppose $X \subseteq Y \subseteq E$. Then any independent set $I \in \mathcal{I}$ contained in X will also be contained in Y. Thus $r(X) \leq r(Y)$ which proves (R3).

(R3) Let $B_{X \cap Y}$ be a basis of $X \cap Y$. Since this is an independent set in $X \cup Y$, we can extend it to a basis of $B_{X \cup Y}$ of $X \cup Y$. Then, we have

$$\begin{aligned} r(X) + r(Y) &\geq |B_{X \cup Y} \cap X| + |B_{X \cup Y} \cap Y| \\ &= |B_{X \cup Y} \cap (X \cup Y)| + |B_{X \cup Y} \cap (X \cap Y)| \\ &= |B_{X \cup Y}| + |B_{X \cap Y}| \\ &= r(X \cup Y) + r(X \cap Y), \end{aligned}$$

which is exactly the statement of (R3).

Now, let $M = (E, r)$ be a ranktroid and let $\varphi_{RM}(M) = (E, \mathcal{I})$. We wish to prove that $(E, \mathcal{I})$ is a matroid. However, we need to prove Lemma 1 first.

Lemma 1 (Lemma 1.3.3 in [4])**.** *Let E be a set and r be a function on 2^E satisfying (R2) and (R3). If X and Y are subsets of E such that $r(X \cup y) = r(X)$ for all $y \in Y - X$, then*

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

Proof. Without loss of generality, we can assume that X and Y are disjoint and $Y = \{y_1, \ldots, y_k\}$. We induct on k. If $k = 1$, then the claim is clearly true. Now, suppose the claim is true for $k - 1$. By (R3), we have

$$2r(X) = r(X \cup \{y_1, \ldots, y_{n-1}\}) + r(X \cup \{y_n\}) \geq r(X) + r(X \cup \{y_1, \ldots, y_n\}) \geq 2r(X).$$

Then $r(X \cup \{y_1, \ldots, y_n\}) = r(X)$ which proves the lemma. □

Now, we prove that φ_{RM} satisfies (I1), (I2), and (I3).

(I1) Note that $0 \leq r(\emptyset) \leq |\emptyset| = 0$ from (R1). Hence $r(\emptyset) = |\emptyset|$ and $\emptyset \in \mathcal{I}$. This proves (I1).

(I2) Now suppose that $I_1 \subseteq I_2$ and $I_2 \in \mathcal{I}$. From (R3), we have

$$r(I_2) = r(I_1 \cap (I_2 - I_1)) + r(I_1 \cup (I_2 - I_1)) \leq r(I_1) + r(I_2 - I_1).$$

We can further bound $r(I_2 - I_1) \leq |I_2 - I_1|$ from (R1). Thus, we have that

$$r(I_2) \leq r(I_1) + |I_2 - I_1| \implies |I_1| \leq r(I_1).$$

From (R1) again, this implies that $r(I_1) = |I_1|$ and $I_1 \in \mathcal{I}$. This proves (I2).

(I3) For the sake of contradiction, suppose that there are members I_1 and I_2 of $\mathcal{I}$ such that $|I_1| < |I_2|$ and for all $e \in I_2 - I_1$, we have $I_1 \cup \{e\} \notin \mathcal{I}$. Equivalently, for all $e \in I_2 - I_1$, the inequality $r(I_1 \cup \{e\}) < |I_1 \cup e|$ holds. This implies that

$$|I_1| = r(I_1) \leq r(I_1 \cup e) < |I_1 \cup e| = |I_1| + 1 \implies r(I_1 \cup e) = |I_1| = r(I_1).$$

From Lemma 1, we have that $r(I_1) = r(I_2) = |I_2|$. But we have $|I_2| = r(I_1) \leq |I_1| < |I_2|$, which is a contradiction. Hence (I3) must hold.

To finish the proof, we just to show that φ_{RM} and φ_{MR} are inverses. We first prove that $\varphi_{RM} \circ \varphi_{MR} = \mathrm{id}_{\mathsf{MAT}}$. Let $M = (E, \mathcal{I})$ be a matroid and $\varphi_{MR}(M) = (E, r)$ be the corresponding ranktroid. The rank function in this case coincides with the rank function r_M with respect to the matroid M that we defined in the prequel. We want to prove that

$$\mathcal{I} = \{X \subseteq E : r(X) = |X|\}.$$

It is clear that $\mathcal{I}$ is included in the right hand side because the largest independent subset of an independent set is the whole set. To prove the other inclusion, consider an arbitrary subset $X \subseteq E$ which satisfies $|X| = r(X)$. But this implies that the largest independent subset of X has cardinality $|X|$, which forces X to be independent. This completes the proof of $\varphi_{MR} \circ \varphi_{RM} = \mathrm{id}_{\mathsf{MAT}}$.

What is left to show is that $\varphi_{MR} \circ \varphi_{RM} = \mathrm{id}_{\mathsf{RANK}}$. Let $M = (E, r)$ be a ranktroid and $\varphi_{RM}(M) = (E, \mathcal{I})$. We want to prove that

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

for all $X \subseteq E$. Suppose $X \in \mathcal{I}$, then by definition $r(X) = |X|$. This clearly is the same as the definition. Now, suppose that $X \notin \mathcal{I}$. Then consider the maximal $B \subset X$ such that $B \in \mathcal{I}$. It suffices to prove that $r(X) = |B|$. For any $x \in X - B$, we have $B \cup x \notin \mathcal{I}$ from maximality. Thus $|B| = r(B) \leq r(B \cup x) < |B \cup x| = |B| + 1$ or $r(B \cup x) = r(B)$. From Lemma 1, we have that $r(X) = r(B) = |B|$, which suffices for the proof. $\square$

Proposition 6 (Ranktroids and Clotroids)**.** *The maps φ_{MG} and φ_{GM} are well-defined and inverses.*

Proof. We first prove that $\varphi_{MG} : \mathsf{MAT} \to \mathsf{CLO}$ is well-defined. It suffices to prove that if $M = (E, \mathcal{I})$ is a matroid, then $\varphi_{MG}(M) = (E, \mathrm{clo})$ where $\mathrm{clo}(X) := \{x \in E : r_M(X \cup x) = r_M(X)\}$ is a clotroid.

- (CL1) If $x \in X$, then $X = X \cup x$. Since the sets are equal, the ranks $r_M(X) = r_M(X \cup x)$ must also be equal. Hence $X \subseteq \mathrm{clo}(X)$. This proves (CL1).
- (CL2) Consider $X \subseteq Y \subseteq E$ and an arbitrary element $x \in \mathrm{clo}(X) - X$. It suffices to prove that $x \in \mathrm{clo}(Y)$. We have that $r_M(X \cup x) = r_M(X)$ from $x \in \mathrm{clo}(X)$. Let $B \subseteq X$ be a basis. Then it is also a basis of $X \cup x$. Then we can extend it to a basis $B' \subseteq Y \cup x$. Note that B' cannot contain x or else $B \cup x$ would've been a larger basis of $X \cup x$. Then B' is also a basis of Y. This proves that $r_M(Y) = |B'| = r_M(Y \cup x)$, completing the proof of (CL2).
- (CL3) From (CL1), we have the inclusion $\mathrm{clo}(X) \subseteq \mathrm{clo}(\mathrm{clo}(X))$. It suffices to prove the opposite inclusion. Let $x \in \mathrm{clo}(\mathrm{clo}(X))$ be an arbitrary element. Then $r_M(\mathrm{clo}(X) \cup x) = r_M(\mathrm{clo}(X)) = r_M(X)$ where the last equality follows from Lemma 1. Then, we have that

  $$r_M(X) = r_M(\mathrm{clo}(X) \cup x) \geq r_M(X \cup x) \geq r_M(X) \implies r_M(X) = r_M(X \cup x).$$

  This shows that $x \in \mathrm{clo}(X)$ and proves (CL3).
- (CL4) For $x \in E$, pick an arbitrary element $y \in \mathrm{clo}(X \cup x) - \mathrm{clo}(X)$. By definition of clo, we have $r_M(X \cup x \cup y) = r_M(X \cup x)$ and $r_M(X \cup y) \neq r_M(X)$. From submodularity and monotonicity, $r_M(X) \leq r_M(X \cup y) \leq r_M(X) + 1$. This implies that $r_M(X \cup y) = r_M(X) + 1$. This gives us the inequality

  $$r_M(X) + 1 = r_M(X \cup y) \leq r_M(X \cup x \cup y) = r_M(X \cup x) \leq r_M(X) + 1.$$

  Thus, $r_M(X \cup y) = r_M(X \cup y \cup x)$, or $x \in \mathrm{clo}(X \cup y)$. This proves (CL4).

We haven proven that $\varphi_{MG}(M)$ is a clotroid and φ_{MG} is well-defined. The next step is to prove that $\varphi_{GM} : \mathsf{CLO} \to \mathsf{MAT}$ is well-defined. It suffices to prove that if $M = (E, \mathrm{clo})$ is a clotroid, then $\varphi_{GM}(M) = (E, \mathcal{I})$ where

$$\mathcal{I} = \{X \subseteq E : x \notin \mathrm{clo}(X - x) \text{ for all } x \in X\}$$

is a matroid. Before proving (I1), (I2), (I3), we first prove the following characterization of $\mathcal{I}$.

Lemma 2 (Lemma 1.4.6 in [4])**.** *Suppose $X \subseteq E$ and $x \in E$. If $X \in \mathcal{I}$ and $X \cup x \notin \mathcal{I}$, then $x \in \mathrm{clo}(X)$.*

Proof. Since $X \cup x \notin \mathcal{I}$, there is some $y \in X \cup x$ such that $y \in \mathrm{clo}((X \cup x) - y)$. If $y = x$, then immediately we have that $x \in \mathrm{clo}(X)$. Now suppose that $y \neq x$. Then $y \in \mathrm{clo}((X - y) \cup x)$ and $y \notin \mathrm{clo}(X - y)$ since $X \in \mathcal{I}$. Thus $y \in \mathrm{clo}((X - y) \cup x) - \mathrm{clo}(X - y)$ and (CL4) implies that $x \in \mathrm{clo}((X - y) \cup y) = \mathrm{clo}(X)$. This proves the lemma. $\square$

We now prove that $(E, \mathcal{I})$ satisfies (I1), (I2), and (I3).

(I1) Vacuously, $\emptyset \in \mathcal{I}$. This proves (I1).

(I2) Suppose that $X \in \mathcal{I}$ and $Y \subseteq X$. Consider an arbitrary element $y \in Y$. Then $y \in X$, so $y \notin \mathrm{clo}(X - y)$. From (CL2), we get $y \notin \mathrm{clo}(Y - y)$. Since y was arbitrary, we get that $Y \in \mathcal{I}$. This proves (I2).

(I3) For the sake of contradiction, suppose that there are $X, Y \in \mathcal{I}$ with $|X| < |Y|$ and (I3) fails for X, Y. We can pick X and Y such that $|X \cap Y|$ is maximal. Then there is an element $y \in Y - X$. I claim that $X \not\subseteq \mathrm{clo}(Y - y)$. Indeed, if we had $X \subseteq \mathrm{clo}(Y - y)$, since $y \notin \mathrm{clo}(Y - y)$ from $Y \in \mathcal{I}$, we also have $y \notin \mathrm{clo}(X)$. Lemma 2 implies that $X \cup y \in \mathcal{I}$. But this contradicts the assumption that X, Y fails (I3). Thus, our assumption $X \subseteq \mathrm{clo}(Y - y)$ must be wrong. This allows us to pick some $x \in X - \mathrm{clo}(Y - y)$. Note that

$$X - \mathrm{clo}(Y - y) \subseteq X - (Y - y) = X - Y.$$

This gives us $x \notin Y$. From (I1), we have $Y - y \in \mathcal{I}$. Since $x \notin \mathrm{clo}(Y - y)$, Lemma 2 implies that $(Y - y) \cup x \in \mathcal{I}$. But then $|(Y - y) \cup x| = |Y| > |X| \implies (Y - y) \cup x \neq X$ and

$$|\{(Y - y) \cup x\} \cap X| = |\{X \cap (Y - y)\} \cup x| = |(X \cap Y) \cup x| = |X \cap Y| + 1 > |X \cap Y|.$$

But this contradicts the maximality of $|X \cap Y|$. This proves (I3).

Now, we want to prove that φ_{MG} and φ_{GM} are inverses. We first prove that $\varphi_{GM} \circ \varphi_{MG} = \mathrm{id}_{\mathsf{MAT}}$. Let $M = (E, \mathcal{I})$ be a matroid. It suffices to prove that

$$\mathcal{I} = \{X \subseteq E : x \notin \mathrm{clo}_M(X - x) \text{ for all } x \in X\}$$

where clo_M is the closure operator of the matroid M which returns the size of a maximal independent set contained in the argument. Let $I \in \mathcal{I}$ be an arbitrary independent set. Then $x \notin \mathrm{clo}_M(I - x)$ for all $x \in X$ since $r_M(I - x) = |I - x| = |I| - 1$ and $r_M((I - x) \cup x) = r_M(I) = |I|$. Thus $\mathcal{I} \subseteq \{X \subseteq E : x \notin \mathrm{clo}_M(X - x) \text{ for all } x \in X\}$. To prove the opposite inclusion, consider $X \subseteq E$ such that $x \notin \mathrm{clo}_M(X - x)$ for all $x \in X$. For any $x \in X$, let $B_x \subseteq X - x$ be a basis of $X - x$. Since $r_M(X) > r_M(X - x)$, we can extend B_x to a basis of X. From the maximality of B_x in $X - x$, the only way we can extend the basis is by adding on x. Thus $B_x \cup x$ is a basis of X. Now suppose that $B_x \cup x \neq X$. Then there is some $y \in X - (B_x \cup x)$. Then $|B_y \cup y| = |B_x \cup x|$ as bases of X. This gives $|B_x| = |B_y|$ since bases all have the same cardinality. But then $B_x \cup x$ is an independent set contained in $X - y$ which is larger than B_y. This contradicts the maximality of B_y, and proves that $B_x \cup x = X$. In particular $X \in \mathcal{I}$. Since X was arbitrary, we have proven the opposite inclusion.

Now, we prove that $\varphi_{MG} \circ \varphi_{GM} = \mathrm{id}_{\mathsf{CLO}}$. Let $M = (E, \mathrm{clo})$ be a clotroid and

$$\mathcal{I} := \{X \subseteq E : x \notin \mathrm{clo}(X - x) \text{ for all } x \in X\}.$$

Then, we want to prove that $\mathrm{clo}_N \equiv \mathrm{clo}$ where $N = (E, \mathcal{I})$ is the matroid $\varphi_{GM}(M)$. Let $X \subseteq E$ be an arbitrary subset. For any $x \in \mathrm{clo}_N(X) - X$, we have that $r_N(X \cup x) = r_N(X)$. Let $B \subseteq X$

be a basis of X with respect to N. This set is also a basis of $X \cup x$ with respect to N. Hence, $B \cup x \notin \mathcal{I}$ and $B \in \mathcal{I}$. Lemma 2 implies that $x \in \mathrm{clo}(B) \subseteq \mathrm{clo}(X)$. Since x was arbitrary, we have that $\mathrm{clo}_N(X) \subseteq \mathrm{clo}(X)$. Now, consider an arbitrary $x \in \mathrm{clo}(X) - X$. Let $B' \subseteq X$ be a basis of X with respect to N. Then $B' \cup y \notin \mathcal{I}$ and $B' \in \mathcal{I}$ for all $y \in X - B'$. Lemma 2 implies that $X \subseteq \mathrm{clo}(B') \implies \mathrm{clo}(X) \subseteq \mathrm{clo}(B')$. Then $x \in \mathrm{clo}(B') \implies x \in \mathrm{clo}((B' \cup x) - x)$, giving us $B' \cup x \notin \mathcal{I}$. In particular, B' is a basis of $X \cup x$ and $r_N(X \cup x) = |B'| = r_N(X)$. This is exactly the statement $x \in \mathrm{clo}_N(X)$. Since x was arbitrary, we get $\mathrm{clo}(X) \subseteq \mathrm{clo}_N(X)$. Hence, $\mathrm{clo}(X) = \mathrm{clo}_N(X)$ for all $X \subseteq E$, which suffices for the proof. □

Proposition 7 (Clotroids and Flatroids)**.** *The maps φ_{GF} and φ_{FG} are well-defined and inverses.*

Proof. We first prove that $\varphi_{GF} : \mathsf{CLO} \to \mathsf{FLAT}$ is well-defined. It suffices to prove that if $M = (E, \mathrm{clo})$ is a clotroid, then $\varphi_{GF}(M) = (E, \mathcal{F})$ where $\mathcal{F} = \{X \subseteq E : X = \mathrm{clo}(X)\}$ is a flatroid.

(F1) We have $E \subseteq \mathrm{clo}(E) \subseteq E \implies \mathrm{clo}(E) = E$. This proves (F1).

(F2) Let $F_1, F_2 \in \mathcal{F}$. Then $F_1 \cap F_2 \subseteq \mathrm{clo}(F_1 \cap F_2)$. We also have $\mathrm{clo}(F_1 \cap F_2) \subseteq \mathrm{clo}(F_i) = F_i$ for $i = 1, 2$. Thus, $\mathrm{clo}(F_1 \cap F_2) \subseteq F_1 \cap F_2$. Both inclusions imply that $\mathrm{clo}(F_1 \cap F_2) = F_1 \cap F_2$ or $F_1 \cap F_2 \in \mathcal{F}$. This proves (F2).

(F3) Let $F \in \mathcal{F}$ and $\{F_1, \ldots, F_k\}$ be the flats which cover F according to the poset structure of $\mathcal{F}$. We first prove that the union of the F_i's cover E. It suffices to prove that an arbitrary element $x \in E - F$ is covered by a flat which covers F. Consider $F_x := \mathrm{clo}(F \cup x)$. Then this is a flat which contains both F, x. Let F_0 be a flat satisfying $F \subseteq F_0 \subseteq F_x$. Suppose that there is an element $y \in F_0 - F$. Then

$$y \in F_0 - F \subseteq \mathrm{clo}(F \cup x) - \mathrm{clo}(F) \implies x \in \mathrm{clo}(F \cup y)$$

from (CL4). Since $\mathrm{clo}(F \cup y) \subseteq \mathrm{clo}(F_0) = F_0$, we get that $x \in F_0$. But then $F \cup x \subseteq F_0$. Taking closures, we get $F_0 = \mathrm{clo}(F \cup x)$. If there is no element $y \in F_0 - F$, then $F_0 = F$. This proves that $\mathrm{clo}(F \cup x)$ covers F and contains both F and x. Hence, we must have

$$\bigcup_{i=1}^{k} F_i = E.$$

Next, we want to prove that $F_i \cap F_j = F$ whenever $i \neq j$. Suppose that there is some element $z \in F_i \cap F_j - F$. Then

$$F \subsetneq F \cup z \subseteq F_i \cap F_j.$$

Taking closures and using (F2), we get

$$F \subsetneq \mathrm{clo}(F \cup z) \subseteq F_i \cap F_j.$$

From the covering relation, we get $F_i = F_j = \mathrm{clo}(F \cup z)$, which is a contradiction. Hence, we must have that $F_i \cap F_j = F$. This proves (F3).

We have proven that φ_{GF} is a well-defined map. Now, we prove that φ_{FG} is a well-defined map. It suffices to prove that if $M = (E, \mathcal{F})$ is a flatroid, then $\varphi_{FG}(M) = (E, \mathrm{clo})$ where

$$\mathrm{clo}(X) := \bigcap_{F \in \mathcal{F} : X \subseteq F} F$$

is a clotroid. Before proving the axioms for clotroids, we first prove Lemma 3

Lemma 3. *Let $F \in \mathcal{F}$ be a flat and $x \notin F$ be an arbitrary element. Then, the flat $F_x = \operatorname{clo}(F \cup x)$ is the unique flat which contains x and covers F.*

Proof. Uniqueness and existence of such a flat is guarenteed by (F3) and it is clear that F_x contains both x and F. It suffices to prove that F_x covers F. Let F_0 be an arbitrary flat which contains both F and x. Then $F \subseteq F \cup x \subseteq F_0$. Taking closures, we get

$$F \subseteq \operatorname{clo}(F \cup x) \subseteq F_0 \implies F \subseteq F_x \subseteq F_0.$$

This completes the proof of the lemma. $\square$

(CL1) This follows because $\operatorname{clo}(X)$ is the intersection of flats which all contain X.

(CL2) Let $A \subseteq B \subseteq E$. (CL2) follows from the fact that any flat which contains B will also contain A.

(CL3) For any $X \subseteq \mathcal{F}$ we have that $\operatorname{clo}(X) \in \mathcal{F}$ from (F2). The closure of a flat is clearer itself, hence $\operatorname{clo}(\operatorname{clo}(X)) = \operatorname{clo}(X)$. This gives (CL3).

(CL4) Let $X \subseteq E$ and $y \in E$. Suppose that $y \in \operatorname{clo}(X \cup x) - \operatorname{clo}(X)$. Let $F_x = \operatorname{clo}(\operatorname{clo}(X) \cup x)$ be the unique flat containing $\operatorname{clo}(X) \cup x$ which covers $\operatorname{clo}(X)$ from Lemma 3. Then

$$X \subseteq X \cup x \subseteq \operatorname{clo}(X) \cup x.$$

Taking closures, we get $\operatorname{clo}(X) \subseteq \operatorname{clo}(X \cup x) \subseteq F_x$. From the covering relation of F_x, we get $\operatorname{clo}(X \cup x) = F_x$. Thus $y \in F_x$. This implies that F_x is the unique flat which covers $\operatorname{clo}(X)$ and contains y. Hence $F_x = F_y \implies x \in F_y$ and $x \in \operatorname{clo}(\operatorname{clo}(X) \cup y)$. By the same reasoning, we get that this last set is equal to $\operatorname{clo}(X \cup y)$. This proves (CL4).

Now we want to prove that φ_{GF} and φ_{FG} are inverses. We first prove that $\varphi_{FG} \circ \varphi_{GF} = \mathrm{id}_{\mathsf{CLO}}$. Let $M = (E, \operatorname{clo})$ be a clotroid. It suffices to prove that the operator clo' defined by

$$\operatorname{clo}'(X) := \bigcap_{F \subseteq E : X \subseteq F, \operatorname{clo}(F) = F} F$$

is the same as clo. Whenever $F \subseteq E$ satisfies $X \subseteq F$ and $\operatorname{clo}(F) = F$, we have that $\operatorname{clo}(X) \subseteq \operatorname{clo}(F) = F$. Hence, $\operatorname{clo}(X) \subseteq \operatorname{clo}'(X)$. To prove the other inclusion, note that $\operatorname{clo}(\operatorname{clo}(X)) = \operatorname{clo}(X)$ from (CL3). Thus, in the intersection we can let $F = \operatorname{clo}(X)$. This gives the inclusion $\operatorname{clo}'(X) \subseteq \operatorname{clo}(X)$. This proves the desired relation.

Now, we want to prove that $\varphi_{GF} \circ \varphi_{FG} = \mathrm{id}_{\mathsf{FLAT}}$. Let $M = (E, \mathcal{F})$ be flatroid. It suffices to prove that

$$\mathcal{F} = \left\{ X \subseteq E : X = \bigcap_{F \in \mathcal{F} : X \subseteq F} F \right\}.$$

Let $F \in \mathcal{F}$ be an arbitrary flat. Then F is included among the flats which contain it, proving that F is an element of the right hand set. This proves one inclusion. To prove the other inclusion, let $X \subseteq E$ be an arbitrary subsets satisfying the property that it is the intersection of all of the flats containing it. From (F2), X is a flat, giving the other inclusion. This suffices for the proof. $\square$

2 Examples of Matroids

In this section, we give examples of matroids which manifest naturally throughout mathematics. The examples which we provide will come from linear algebra and graphs. Before giving the examples, we first define a notion of matroid isomorphism.

Definition 9. We say a map $f : (E_1, \mathcal{I}_1) \to (E_2, \mathcal{I}_2)$ is a *isomorphism* if $f : E_1 \to E_2$ is a bijection and $X \in \mathcal{I}_1$ if and only if $f(X) \in \mathcal{I}_2$.

We call two matroids *isomorphic* if and only if there is an isomorphism between them. Note that isomorphism preserves not only independent sets, but also circuits, bases, rank functions, flats, closures, etc. The notion of isomorphism will be useful as we consider examples of matroids and try to classify general matroids. One reasonable question to ask about a matroid is whether or not it is isomorphic to one of our canonical examples. In the sequel, we consider our first example which manifests through linear algebra.

2.1 Linear Algebra

The first example comes from linear algebra and linear independence of vectors.

Proposition 8. *Let $\mathbb{F}$ be a field and V be a $\mathbb{F}$-vector space. Let $M = (E, \mathcal{I})$ where $E = \{v_1, \ldots, v_n\} \subset V$ and $\mathcal{I}$ are all subsets of E which are linearly independent. Then M is a matroid.*

Proof. (I1) and (I2) follow trivially. Now suppose $\{w_1, \ldots, w_k\}$ and $\{u_1, \ldots, u_{k+1}\}$ are both linearly independent. It suffices to prove that there exists i, $1 \le i \le k+1$ such that $\{w_1, \ldots, w_k, u_i\}$ is linearly independent. For the sake of contradiction, suppose this is not true. This implies that $u_i \in \mathbb{F}\langle w_1, \ldots, w_k \rangle$ for all i. But then

$$\mathbb{F}\langle u_1, \ldots, u_{k+1} \rangle \subseteq \mathbb{F}\langle w_1, \ldots, w_k \rangle.$$

But this clearly false since the left hand side has dimension $k+1$ and the right hand side has dimension k. $\square$

We say a matroid is $\mathbb{F}$-*representable* if it is isomorphic to a matroid constructed as in Proposition 8. If a matroid is $\mathbb{F}$-representable for some field $\mathbb{F}$, we call it *algebraic*. Equivalently, we say that a matroid $M = (E, \mathcal{I})$ is $\mathbb{F}$-representable if there is a $\mathbb{F}$-vector space V and a map $\phi : E \to V$ such that $\phi(I)$ is linearly independent if and only if $I \in \mathcal{I}$. There are many interesting questions in matroid theory about representability.

Question 1. *Are all matroids algebraic?*

The answer is no. In [2], Ingleton and Main prove that the Vamos matroid, defined on the set of 8 elements $S = \{a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4\}$ having as independent sets all subsets of cardinality at most 4 except for the sets

$$\{a_1, b_1, a_2, b_2\}, \{a_1, b_1, a_3, b_3\}, \{a_1, b_1, a_4, b_4\}, \{a_2, b_2, a_3, b_3\}, \{a_2, b_2, a_4, b_4\}$$

is not algebraic. This example is small, but it is difficult to prove that it is not algebraic over any field. For an easier example, we need the notion of the direct sum of two matroids.

Definition 10. Let $M_1 = (E_1, \mathcal{I}_1)$ and $M_2 = (E_2, \mathcal{I}_2)$ be two matroids. Then we define their direct sum $M_1 \oplus M_2 := (E_1 \sqcup E_2, \mathcal{I})$ to be the matroid on the disjoint union of E_1 and E_2 with independent sets of the form $I_1 \sqcup I_2$ with $I_1 \in \mathcal{I}_1$ and $I_2 \in \mathcal{I}_2$.

It is not difficult to show that the direct sum of two matroids is indeed a matroid. In Example 1, we show that the matroid $U_{2,4}$ is representable over every field except $\mathbb{F}_2$. Now, consider the Fano matroid F_7 whose construction comes from the Fano plane (Figure 1) where the ground set are the points and the bases are the non-collinear three-element subsets.

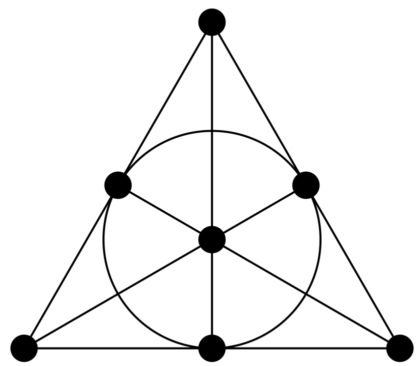

Figure 1: The Fano Plane

The Fano matroid turns out to be representable over $\mathbb{F}_2$, but not over any other field. Thus, the matroid $U_{2,4} \oplus F_7$ will not be representable over any other field since any representation would induce representations on both $U_{2,4}$ and F_7.

Question 2. *If M is representable over one field, is it representable over all fields?*

The answer is still no. This follows from the following Example 1.

Example 1. *Let $U_{m,n}$ be the matroid with ground set $[n]$ and independent sets all subsets of size at most m. Matroids of these types are called uniform matroids. The matroid $U_{2,4}$ is not $\mathbb{F}_2$-representable, but it is $\mathbb{F}_3$-representable.*

Proof. We first prove that $U_{2,4}$ is $\mathbb{F}_3$-representable. Indeed, consider the matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{bmatrix}.$$

The matroid with the ground set as the column vectors and independent sets corresponding to linearly independence is isomorphic to $U_{2,4}$. To prove that $U_{2,4}$ is not $\mathbb{F}_2$-representable, suppose for the sake of contradiction there is a $\mathbb{F}_2$ vector space V and vectors $v_1, v_2, v_3, v_4 \in V$ such that every pair is linearly indepent and every triple of them are linearly independent. In particular, this implies that the sum of every three is 0. But then, we have

$$0 \neq v_1 + v_4 = (v_1 + v_2 + v_3) + (v_2 + v_3 + v_4) = 0$$

which is a contradiction. □

There are two interesting operations that you can do to matroids: deletion and contraction.

Definition 11. Let $M = (E, \mathcal{I})$ be a matroid and let $e \in E$ be an element of E. Let $\mathcal{I}' = \{I \subseteq E - \{e\} : I \in \mathcal{I}\}$. Then we define $M \backslash e = (E - e, \mathcal{I}')$ to be the *deletion* of e from M. If e is a loop, then we define $M/e = M \backslash e$. If e is not a loop, then we define

$$M/e = (E - e, \mathcal{I}''), \quad \mathcal{I}'' = \{I \subset E - e : I \cup e \in \mathcal{I}\}.$$

We call M/e the *contraction* of e from M.

The operations of deletion and contraction are related to those in graph theory, which we will explain in a later section. Any matroid which can be achieved via deletions and contractions from another one is called a *minor*. In [5], Rota made the following conjecture.

Conjecture 1 (Rota, 1971)**.** *For every finite field $\mathbb{F}$, can all $\mathbb{F}$-representable matroids be characterized by a finite set of forbidden minors?*

In [11], Vamos showed that the conjecture is false when $\mathbb{F}$ is an infinite field. This problem is still open, and has been proven only for $\mathbb{F}_2, \mathbb{F}_3$ and $\mathbb{F}_4$. In particular, we have the following characterization of $\mathbb{F}_2$-representable matroids proven by Tutte in [10].

Theorem 1. *A matroid is $\mathbb{F}_2$-representable if and only if it does not have $U_{2,4}$ as a minor.*

2.2 Graph Theory

We begin with the classic example of a matroid coming from graphs where independent sets are subsets of the edges which do not contain any cycle.

Definition 12. Let $G = (V, E)$ be an undirected graph. Then $\mathcal{I} \subseteq 2^E$ be the subsets of the edges which contain no cycles. Then we call $M[G] = (E, \mathcal{I})$ the *graphic matroid* with respect to G.

It is not immediately obvious why graphic matroids are matroids. This can proved directly by checking (I1), (I2), and (I3). However, Theorem 2 provides a nice indirect method which also proves that graphic matroids are algebraic.

Theorem 2. *Let $G = (V, E)$ be an undirected graph. Let A be the $|V| \times |E|$ matrix where the columns are indexed by the edges, the rows are indexed by the vertices, and the column corresponding to an edge $e \in E$ has 1 in the entry corresponding to one of its incident vertices and -1 in the other incident vertex. Then a subset $X \subseteq E$ of edges contains a cycle if and only if the corresponding columns in A are linearly dependent. In particular, $M[G]$ is a matroid which is isomorphic to the matroid $M[A]$.*

Proof. Suppose $X \subseteq E$ contains a cycle. Then, there are edges $e_1, \ldots, e_k \in X$ that are a cyclic in this order with vertices $v_1, \ldots, v_k$. Let $c_1, \ldots, c_k$ be the columns in A corresponding to $e_1, \ldots, e_k$. We can pick $\varepsilon_i \in \{\pm 1\}$ such that $\varepsilon_i c_i = u_{v_i} - u_{v_{i+1}}$ for all $1 \leq i \leq k$ and $v_{k+1} := v_1$. Then

$$\sum_{i=1}^{k} \varepsilon_i c_i = \sum_{i=1}^{n} u_{v_i} - u_{v_{i+1}} = 0.$$

This proves that $c_1, \ldots, c_k$ are linearly dependent. Conversely, suppose that the corresponding columns of X in A are linearly dependent. Then, there is a linear combination

$$\sum_{i=1}^{k} \lambda_i c_i = 0$$

where $\lambda_i \neq 0$ for $1 \leq i \leq k$. Consider the vector c_1. This vector has two non-zero entry. Since we have a non-trivial linear relation, there must be another vector which has a non-zero entry in one of these two locations. Now consider this vector and consider the other non-zero entry. By the same reasoning, there is another vector which has a non-zero entry in this same entry. Repeating this process, we eventually have to pick a column that we picked before. This creates a cycle. This suffices for the proof. $\square$

Theorem 2 proves that graphic matroids are matroids. If we consider our matroid notions in the graph setting, we find that independent sets are exactly the edges which forests, bases are spanning forests, and circuits are minimal cycles. Then, many problems in graph theory can be translated to the language of matroids in a more general setting. For example, if we wanted to count the number of spanning forests of a graph, this is a subcase of enumerating the number of bases for a matroid. We end this section with an example that comes from transversals and the vertices of the graph.

Theorem 3. *Let $G = (V, E)$ be a bipartite graph with bipartitions A, B. Let $\mathcal{I} \subseteq 2^A$ be the collection of subsets of A that can be matched with vertices in B. Then $(A, \mathcal{I})$ is a matroid.*

Proof. This prove follows Theorem 4.1 in [3]. (I1) holds because the empty set can be matched since we do not need to match any vertices. (I2) holds because if we match a subset $X \subseteq A$, then we can match any $Y \subseteq X$ by restricting to Y in the matching of X. It suffices to prove (I3). Let $X, Y \in \mathcal{I}$ with $|X| = |Y| + 1$ and corresponding matchings M_X and M_Y. Now, color the edges M_X red and the edges of M_Y blue. Any edge which is colored both red and blue will be considered to be colored purple. Then $|M_X| = |M_Y| + 1$ and there are exactly $|M_X - M_Y|$ red edges and $|M_Y - M_X|$ blue edges. Moreover, we have that $|M_X - M_Y| = 1 + |M_Y - M_X|$. Now, focus on only the red and blue edges. On this subgraph, every vertex has degree at most 2 since every vertex can be incident to at most 1 red edge and 1 blue edge. Hence, the subgraph must be some disjoint collection of paths and cycles where the edges alternate in color. Since every cycle has an equal number of red and blue edges, there must be at least one connected component which is a path. Moreover, we can find such a path where the number of red edges is one greater than the number of blue edges. Now, swap the colors in this path and the edges which are colored blue and purple now form a matching. This corresponds to $Y \cup \{x\}$ where $x \in X - Y$. This suffices for the proof. $\square$

2.3 Regular Matroids

In this section, we revisit the question of classifying matroids which are representable over every field.

Definition 13. We say a matroid M is *regular* if it is representable over every field.

From Example 1, we know that there exist matroids which are not regular. If we do consider regular matroids, we find that they satisfy several nice properties. To illustrate, we include the statement of Theorem 4.

Theorem 4 (Theorem 5.16 in [3])**.** *The following statements are equivalent for a matroid M.*

(i) M is regular.

(ii) M is $\mathbb{F}_2$ and $\mathbb{F}_3$ representable.

(iii) M is representable over $\mathbb{F}_2$ and $\mathbb{F}$ where $\mathbb{F}$ is a field of characteristic other than 2.

(iv) M is representable over $\mathbb{R}$ by a unimodular matrix.

We will not prove Theorem 4 and instead refer the interested reader to [4]. We will be particularly interested in (iv) in Theorem 4 which uses the term "unimodular", a term that we have not defined yet.

Definition 14. We call a matrix $A \in \mathbb{R}^{d \times n}$ *unimodular* if every minor lies in the set $\{0, \pm 1\}$.

Since every individual entry of a matrix is a 1×1 minor, every entry of a unimodular matrix must lie in the set $\{0, \pm 1\}$. In our previous examples, we have already dealt with unimodular matrices.

Proposition 9. *Let $G = (V, E)$ be a graph and $M = M[G]$ the corresponding graphic matroid. Then $M \cong M[A]$ where A is matrix defined in Theorem 2. The matrix A is unimodular.*

Proof. We want to prove that the determinant of any square submatrix is in $\{0, \pm 1\}$. To prove this, we induct on the size of the square submatrix. If the submatrix is 1×1, then the determinant is in $\{0, \pm 1\}$ since the entries of A are in $\{0, \pm 1\}$. Now consider an arbitrary square submatrix A_0 of A and suppose square submatrices of smaller size have determinant in $\{0, \pm 1\}$. If there exists a 0 column in A_0, then the determinant is 0. If there exists a column with only one non-zero entry (which is either 1 or -1), then the determinant is then ± 1 multiplied the determinant of a smaller square submatrix. By the inductive hypothesis, this value is in $\{0, \pm 1\}$. Finally, suppose that all columns have two non-zero entries. Then the two non-zero entries must be 1 and -1 in each column. Summing all of the rows together, we get the zero matrix. This implies that the matrix has linearly dependent rows, implying that the determinant is zero. This completes the induction. $\square$

From Theorem 4 and Proposition 9, we get the fact that all graphic matroids are regular. We will see that regularity, through the unimodular representation, allows us to optimize the dimensionality of our matroid. To see why our current representations are not optimal, consider a graph $G = (V, E)$ and the matrix A defined in Theorem 2. Since A is a $|V| \times |E|$ matrix, the matroid $M[A]$ isomorphic to $M[G]$ consist of $|E|$ vectors in $\mathbb{R}^{|V|}$. However, the rank of our matroid $M[G]$ is very unlikely to large enough to fill up the whole space $\mathbb{R}^{|V|}$. Indeed, in the best case scenario, our graph G is connected and the rank of the matroid is $|V| - 1$. If we have a matroid of rank r which is representable over $\mathbb{R}$, it is not unreasonable to ask for a representation by vectors in $\mathbb{R}^r$. Theorem 5 implies that such a representation is possible for regular matroids.

Theorem 5. *Let $M = (E, \mathcal{I})$ be a regular matroid of rank r. Then M can be represented by a unimodular matroid of dimension $r \times |E|$.*

Proof. Since M is regular, it can be represented by some unimodular matrix U of dimension $n \times |E|$ where $n \geq r$. We can first permute the columns of U such that the first r columns are linearly independent. Note that after performing any invertible row operations on U, the matrix U will still represent M. I claim that we can perform a series of row operations preserving unimoduarlity such that the first r columns are $e_1, \ldots, e_r$ where $e_1, \ldots, e_n$ is the standard basis of $\mathbb{R}^n$. Suppose that we have already transformed the first $k-1$ columns into $e_1, \ldots, e_{k-1}$ where $k \leq r$. Then, perform the following two steps.

1. In the kth column, one of the entries in the $k, k+1, \ldots, n$ place is non-zero. Otherwise, the column would be in the span of the previous $k-1$ columns, which contradicts the fact that the first r columns are linearly independent. Hence, we can permute the rows $k, \ldots, n$ such that the entry $[U]_{kk}$ is non-zero.

2. Multiply the kth row by $1/[U]_{kk}$. Thus, we now have $[U]_{kk} = 1$.

3. For every $j \in \{1, \ldots n\} \backslash \{k\}$, subtract $[U]_{jk}$ times the kth row from the jth row.

After this operation, the first $k-1$ columns remain $e_1, \ldots, e_k$ and the kth column is not e_{k+1}. It suffices to prove that this operation preserves unimodularity. Let X be a square submatrix before the operation and Y the same submatrix after the operation. Assuming $\det X \in \{0, \pm 1\}$, we want to prove that $\det Y \in \{0, \pm 1\}$. The only step that could break unimodularity is (3). Let R be the row set of X and C the column set of X. We consider three cases.

(i) (Case 1: $k \in R$) In this case, Y differs from X by row operations within the submatrix. Hence $\det Y = \det X \in \{0, \pm 1\}$.

(ii) (Case 2: $k \notin R, k \in C$) In this case, the column corresponding to k in Y is the zero column. Then $\det Y = 0 \in \{0, \pm 1\}$.

(iii) (Case 3: $k \notin R, k \notin C$) Consider the submatrix corresponding the rows and columns $R \cup k$ and $C \cup k$. The result of this matrix after the operation in column k is the zero vector besides for the (k, k) entry which is 1. From our previous cases, the determinant of this matrix is in $\{0, \pm 1\}$. The determinant of this matrix is equal to the determinant of Y. This proves that $\det Y \in \{0, \pm 1\}$.

Thus, through a series of row operations, we can transform U into a matrix U^* where U^* is unimodular, represents M, and the first r rows are $e_1, \ldots, e_r$. This implies that the rows $r+1, \ldots, n$ are all zero since the space spanned by $e_1, \ldots e_r$ has full rank. Removing these rows, we get a representation of M by a $r \times |E|$ unimodular matrix. This suffices for the proof. $\square$

3 Applications

In the final section, we discuss two applications of matroids. The first is in combinatorial optimization while the second is in convex geometry.

3.1 The Greedy Algorithm

Suppose we have a set E, a family of subsets $\mathcal{I} \subset 2^E$, and a weight function $w : E \to \mathbb{R}_{>0}$. With this weight function, we can define the weight of any subset $X \subset E$ as

$$w(X) := \sum_{e \in X} w(e).$$

Oftentimes, we are interested in finding an element of $\mathcal{I}$ which maximizes the weight. Moreover, we want to do it efficiently (without computing the weights of all of our subsets and then picking the largest one). If we have a quick way to check if a certain subset is in $\mathcal{I}$, then the following algorithm is more efficient and in some cases will output the correct answer.

Definition 15. Let $(E, \mathcal{I})$ be a set family and $w : E \to \mathbb{R}_{>0}$ a positive weight function. The following algorithm is called the *greedy algorithm* associated to $(E, \mathcal{I}, w)$.

1. Let $B = \emptyset$ be our current independent set. Our algorithm will add elements to B.

2. If there exists $e \in E \backslash B$ such that $B \cup e \in \mathcal{I}$, pick such a $e \in E$ with maximum weight and add it to B.

3. If there is no such $e \in E \backslash B$ with $B \cup e \in \mathcal{I}$, then we output B.

It turns out that the greedy algorithm outputs a weight maximizing element of $\mathcal{I}$ if $M = (E, \mathcal{I})$ is a matroid. More surprisingly, for any set family $(E, \mathcal{I})$ satisfying (I1), (I2) for which the greedy algorithm works for all positive weight functions has to be a matroid.

Theorem 6 (Theorem 1.8.5 in [4]). *Let $\mathcal{I}$ be a collection of subsets of a finite set E. Then $(E, \mathcal{I})$ is a matroid if and only if $\mathcal{I}$ satisfies (I1), (I2), and (G): for all positive real weight functions w on E, the Greedy Algorithm produces a maximum-weight member of $\mathcal{I}$.*

Proof. Suppose $M = (E, \mathcal{I})$ is a matroid and let $w : E \to \mathbb{R}_{>0}$ be an arbitrary weight function. Let B be the output of the greedy algorithm. Since the weight function is positive, B must be a basis. Let $B = \{e_1, \ldots, e_r\}$ where $e_1, \ldots, e_r$ were chosen in this order and let $B' = \{f_1, \ldots, f_r\}$ be another basis with $w(f_1) \geq \ldots \geq w(f_r)$. I claim that for all i, $w(e_i) \geq w(f_i)$, which proves that B is indeed weight maximizing. The base case $w(e_1) \geq w(f_1)$ is clear since at first we pick the element with highest weight which is in some independent set. Now, suppose that we know $w(e_i) \geq w(f_i)$ for $i < k$. For the sake of contradiction, suppose that $w(e_k) < w(f_k)$. Then consider $\{e_1, \ldots, e_{k-1}\}$ and $\{f_1, \ldots, f_{k-1}, f_k\}$. Both of these are independent, so there is some f_i such that

$$\{e_1, \ldots, e_{k-1}, f_i\} \in \mathcal{I}.$$

But $w(f_i) \geq w(f_k) > w(e_k)$, which contradicts the maximality of e_k. Thus B must maximize the weight.

Now suppose that $(E, \mathcal{I})$ satisfies (I1), (I2), and (G). It suffices to prove that it satisfies (I3). For the sake of contradiction, suppose that there are $I_1, I_2 \in \mathcal{I}$ with $|I_2| = |I_1| + 1$ and for all $e \in I_2 - I_1$ we have $I_1 \cup e \notin \mathcal{I}$. We now construct a special weight function which will give our contradiction. Note that $|I_2 - I_1| = |I_1 - I_2| + 1$. Since (I2) holds, we have $I_1 - I_2 \neq \emptyset$. Thus, there is a sufficiently small number $\varepsilon > 0$ such that

$$0 < (1 + 2\varepsilon)|I_1 - I_2| < |I_2 - I_1|.$$

Consider the weight function

$$w(e) := 2 \cdot \mathbb{1}_{I_1 \cap I_2} + \frac{1}{|I_1 - I_2|} \cdot \mathbb{1}_{I_1 - I_2} + \frac{1 + 2\varepsilon}{|I_2 - I_1|} \cdot \mathbb{1}_{I_2 - I_1} + \frac{\varepsilon}{|I_2 - I_1| \cdot |E - (I_1 \cup I_2)|} \cdot \mathbb{1}_{E - (I_1 \cup I_2)}.$$

We first prove that this is well-defined. The only part of the definition which threatens well-definedness is that we are possibly dividing by 0 in the expression

$$\frac{\varepsilon}{|I_2 - I_1| \cdot |E - (I_1 \cup I_2)|}.$$

However, if $|E - (I_1 \cup I_2)| = 0$, the corresponding indicator variable will always be 0. In that case, it is understood that we just ignore that term. Hence the weight function is well-defined. Now consider how the greedy the algorithm picks our maximizing set B. We have that

$$2 > \frac{1}{|I_1 - I_2|} > \frac{1 + 2\varepsilon}{|I_2 - I_1|}$$

from our construction of ε. If $|E - (I_1 \cup I_2)| \neq 0$, then we have

$$\frac{1 + 2\varepsilon}{|I_2 - I_1|} > \frac{\varepsilon}{|I_2 - I_1| \cdot |E - (I_1 \cup I_2)|}.$$

Thus, we will first pick all the elements in $I_1 \cap I_2$, then pick all the elements in $I_1 - I_2$. But then, it cannot pick any elements in $I_2 - I_1$ from our assumption. Thus, the remaining elements (if they exist) must be chosen from $E - (I_1 \cup I_2)$. Thus, we have

$$\begin{aligned} w(B) &\leq 2|I_1 \cap I_2| + \frac{|I_1 - I_2|}{|I_1 - I_2|} + \left(\frac{\varepsilon \cdot |E - (I_1 \cup I_2)|}{|E - (I_1 \cup I_2)| \cdot |I_2 - I_1|} \cdot \mathbb{1}_{|E-(I_1 \cup I_2)| \neq 0} \right) \\ &= 2|I_1 \cap I_2| + 1 + \frac{\varepsilon}{|I_2 - I_1|} \\ &\leq 2|I_1 \cap I_2| + 1 + \varepsilon. \end{aligned}$$

However, we have that

$$w(I_2) = 2|I_1 \cap I_2| + 1 + 2\varepsilon > w(B).$$

But this is a contradiction.

Remark. The idea behind our choice of w was that $|I_1|$ is slightly smaller than $|I_2|$. So, we can have our greedy algorithm pick I_1 first by making the weight slightly larger than I_2. After it picks all of I_1, it cannot pick anything from I_2 anymore. However, we can make the differential small enough so that all of I_2 will be larger than this amount, giving the contradiction.

□

A classical example in graph algorithms of the greedy algorithm is Kruskal's algorithm for finding minimum spanning tree. The proof that the algorithm works is the same as the one presented here with the matroid notions replaced with the more specific language of graphs. In the sequel, we give another connection between matroids and the theory of convex bodies. Even thoug it is much more an application of convex body theory to matroid theory, the results are worth a read.

3.2 Log-concavity and the Alexandrov-Fenchel Inequality

In this section, we prove a charming result about the log-concavity of a base-counting combinatorial sequence with respect to a regular matroid. Our main tool for proving log concavity will be Theorem 8, a deep inequality which underlines all of convex geometry and Brunn-Minkowski theory. In this paper, we will not go into detail of the theory of convex bodies and Theorem 8. We redirect the interested reader to the excellent monograph [6]. The subject of Theorem 8 are about convex bodies, which are defined in Definition 16

Definition 16. We call a subset $K \subset \mathbb{R}^d$ a *convex body* if and only if it is non-empty, convex, and compact. We use K^d to denote the collection convex bodies in $\mathbb{R}^d$.

With two convex bodies $K, L \in \mathsf{K}^d$, we can define the *Minkowski sum* of K and L as $K + L = \{x + y \in \mathbb{R}^d : x \in K, y \in L\}$. The Minkowski sum of two convex bodies remains a convex body.

Example 2 (Zonotopes)**.** *For a finite set of vectors $S = \{v_1, \ldots, v_m\} \subset \mathbb{R}^d$, we define the convex polytope*

$$Z(S) := \{\alpha_1 v_1 + \ldots + \alpha_m v_m \in \mathbb{R}^d : \alpha_i \in [0, 1]\} = \sum_{i=1}^{d} [0, v_i]$$

where $[0, v] := \{\lambda v \in \mathbb{R}^d : \lambda \in [0, 1]\}$ is called the zonotope with respect to S. You can think of zonotopes as a high-dimensional generalization of the parallelepiped.

An interesting quantity to consider the volume of the Minkowski sum of a collection of convex bodies. For any convex bodies $K_1, \ldots, K_d \in \mathsf{K}^d$, there exists a quantity $\mathsf{MV}_d(K_1, \ldots, K_d) \in \mathbb{R}_{\geq 0}$ such that

$$\mathrm{Vol}_d\left(\sum_{i=1}^m \lambda_i C_i\right) = \sum_{i_1,\ldots,i_d=1}^m \mathsf{MV}_d(C_{i_1}, \ldots, C_{i_d}) \cdot \lambda_{i_1} \ldots \lambda_{i_d}, \quad \forall\, \lambda_1, \ldots, \lambda_m \in [0,\infty)$$

for any $C_1, \ldots, C_m \in \mathsf{K}^d$. The quantity $\mathsf{MV}_d(K_1, \ldots, K_d)$ is called the *mixed volume* of $K_1, \ldots, K_d$. The mixed volume satisfies many nice properties which are listed by Theorem 7.

Theorem 7 (Theorem 3.7 in [1])**.** *The mixed volume* $\mathsf{MV}_d(K_1, \ldots, K_d)$ *of* n *convex bodies* $K_1, \ldots, K_d \in \mathsf{K}^d$ *has the following properties.*

(a) Let S_d be the permutation group on d letters. For any $\pi \in S_d$, we have

$$\mathsf{MV}_d(K_1, \ldots, K_d) = \mathsf{MV}_d(K_{\pi(1)}, \ldots, K_{\pi(d)}).$$

That is, the mixed volume is symmetric in its arguments.

(b) For any linear operator $A : \mathbb{R}^d \to \mathbb{R}^d$, we have

$$\mathsf{MV}_d(AK_1, \ldots, AK_d) = |\det A| \cdot \mathsf{MV}_d(K_1, \ldots, K_d).$$

(c) If $\dim(K_1 + \ldots + K_d) \leq d-1$*, then* $\mathsf{MV}_d(K_1, \ldots, K_d) = 0$.

(d) The mixed volume is linear with respect to positive Minkowski combinations in each argument.

The symmetry of the mixed volumes also gives the following succinct interpretation of the mixed volume:

$$\mathsf{MV}_d(K_1, \ldots K_d) = \frac{1}{d!} \frac{\partial^d}{\partial x_1 \ldots \partial x_d} \mathrm{Vol}_d\left(\sum_{i=1}^d x_i K_i\right).$$

Example 3. *Let $e_1, \ldots, e_d \in \mathbb{R}^d$ be the standard basis of $\mathbb{R}^d$. Then*

$$\mathsf{MV}_d([0,e_1], \ldots, [0,e_d]) = \frac{1}{d!} \frac{\partial^d}{\partial x_1 \ldots \partial x_d} \mathrm{Vol}_d\left(\sum_{i=1}^d x_i [0,e_1]\right).$$

The Minkowski sum can be simplified as $\sum_{i=1}^d x_i[0,e_i] = \prod_{i=1}^d [0,x_i]$, the volume of which is $x_1 \ldots x_d$. This gives the mixed volume

$$\mathsf{MV}_d([0,e_1], \ldots, [0,e_d]) = \frac{1}{d!}.$$

Example 4. *Let $v_1, \ldots, v_d \in \mathbb{R}^d$ be vectors in $\mathbb{R}^d$. Then*

$$\mathsf{MV}_d([0,v_1], \ldots, [0,v_d]) = |\det[v_1, \ldots, v_d]| \mathsf{MV}_d([0,e_1], \ldots, [0,e_d]) = \frac{|\det[v_1, \ldots, v_d]|}{d!}.$$

Example 5. *Let $S = \{v_1, \ldots, v_m\} \subseteq \mathbb{R}^d$ be a finite subset of vectors in $\mathbb{R}^d$. Then, we can compute*

$$\begin{aligned} \mathrm{Vol}_d(Z(S)) &= \sum_{i_1,\ldots i_d=1}^m \mathsf{MV}_d([0,v_{i_1}], \ldots, [0,v_{i_d}]) \\ &= \frac{1}{d!} \sum_{i_1,\ldots,i_d} |\det[v_{i_1}, \ldots, v_{i_d}]| \\ &= \sum_{1 \leq i_1 < \ldots < i_d \leq m} |\det[v_{i_1}, \ldots, v_{i_d}]|. \end{aligned}$$

Mixed volumes satisfy the inequality given in Theorem 8. This inequality can be seen as a generalization of the isoperimetric inequality, Brunn-Minkowski inequality, and similar inequalities. Indeed, by substituting in suitable convex bodies into Theorem 8, we recover these famous inequalities from convex geometry. For the specific details, see [6].

Theorem 8 (Alexandrov-Fenchel Inequality)**.** *Let $\mathcal{P} = (K_1, \ldots, K_{d-2}) \in (\mathsf{K}^d)^{d-2}$ be an ordered collection of convex bodies in $\mathbb{R}^d$. Then, for any convex bodies $K, L \in \mathsf{K}^d$, we have*

$$\mathsf{MV}_d(K, L, \mathcal{P})^2 \geq \mathsf{MV}_d(K, K, \mathcal{P}) \cdot \mathsf{MV}_d(L, L, \mathcal{P}).$$

We do not prove Theorem 8 in this paper due to the technical nature of the proof. We recommend the interested reader to read the proof given in [7] which reduces the inequality to proving that a certain linear operator satisfies a hyperbolic version of the Cauchy-Schwartz inequality. In this paper, Theorem 8 will be mainly used to prove that some sequences are log-concave.

Definition 17. Let $\{a_k\}_{0 \leq k \geq n}$ be a finite sequence of non-negative real numbers. We say the sequence is *log-concave* if for all $1 \leq k \leq n-1$, we have $a_k^2 \geq a_{k+1}a_{k-1}$. We say the sequence is *ultra-log-concave* if $\{a_k/\binom{n}{k}\}_{0 \leq k \leq n}$ is *log-concave.*

Log-concave and ultra-log-concave sequences appear all throughout combinatorics. We recommend the interested reader to check out the classic paper by Stanley [9] on this topic. We now have the tools to consider the main problem in this section, which was first solved by Stanley in [8] with this very solution.

Theorem 9. *Let $M = (E, \mathcal{I})$ be a regular matroid of rank r. For a partition $E = S \sqcup T$, we can define the sequence $f_0, \ldots, f_r$ where f_i is the number of bases $B \subseteq E$ satisfying $|B \cap S| = i$ and $|B \cap T| = r - i$. For any such partition, the sequence f_i is ultra-log-concave.*

Since M is regular, Theorem 4 implies that there is a map $\phi : E \to \mathbb{R}^m$ where ϕE is unimodular and for $X \subseteq E$ we have $X \in \mathcal{I}$ if and only if ϕX is a linearly independent set of vectors. Moreover, Theorem 5 implies we can pick ϕ such that $\phi : E \to \mathbb{R}^r$. Hence, we can think of M as a collection of vectors $\{v_1, \ldots, v_m\}$ where $v_i \in \mathbb{R}^r$ for all $1 \leq i \leq m$. Since $[v_1, \ldots, v_m]$ is unimodular, we have that

$$|\det[v_{i_1}, \ldots, v_{i_d}]| = \mathbb{1}_{(v_{i_1}, \ldots, v_{i_d}) \text{ is a basis}}.$$

Thus, the determinant detects when a subset of $\{v_1, \ldots, v_m\}$ is a basis. We are now ready to prove Theorem 9.

Proof of Theorem 9. We can represent S and T by the vectors $S = \{v_1, \ldots, v_s\}$, $T = \{w_1, \ldots, w_t\}$. Consider the zonotopes $Z_S := Z(S)$ and $Z_T := Z(T)$. Then,

$$\mathrm{Vol}_d(\lambda Z_S + \mu Z_T) = \sum_{i=0}^{d} \mathsf{MV}_d(Z_S[i], Z_T[d-i]) \binom{r}{i} \cdot \lambda^i \mu^{r-i}.$$

Note that $\lambda Z_S + \mu Z_T$ is the zonotope

$$\lambda Z_S + \mu Z_T = Z(\lambda v_1, \ldots, \lambda v_s, \mu w_1, \ldots, \mu w_t).$$

Taking this view, we also have that

$$
\begin{aligned}
\mathrm{Vol}_d(\lambda Z_S + \mu Z_T) &= \sum_{k=0}^{d} \lambda^k \mu^{r-k} \sum_{\substack{1\le i_1<\ldots<i_k\le s \\ 1\le j_1<\ldots<j_{r-k}\le t}} |\det[v_{i_1},\ldots,v_{i_k},w_{j_1},\ldots,w_{j_{r-k}}]| \\
&= \sum_{k=0}^{d} f_i \lambda^k \mu^{r-k}.
\end{aligned}
$$

Matching coefficients, we get that

$$
\frac{f_i}{\binom{r}{i}} = \mathsf{MV}_d(Z_S[i], Z_T[d-i]).
$$

Finally, Theorem 8 proves that $\{f_i\}$ is ultra-log-concave. This suffices for the proof. $\square$

Acknowledgements

Many thanks to my advisor Noah Kravitz who patiently and helpfully guided me through the directed reading project. I would also like to thank Professor Ramon van Handel for introducing me to the Alexandrov-Fenchel inequality, and in particular, the last application. Finally, I would like to thank Ollie Thakar who was always eager to listen to my matroidal ramblings.

References

[1] Daniel Hug and Wolfgang Weil. *Lectures on Convex Geometry*. Springer International Publishing, 2020.

[2] A. W. Ingleton and R. A. Main. Non-Algebraic Matroids exist. *Bulletin of the London Mathematical Society*, 7(2):144–146, 07 1975.

[3] James Oxley. What is a matroid?, 2014.

[4] James G. Oxley. *Matroid Theory (Oxford Graduate Texts in Mathematics)*. Oxford University Press, Inc., USA, 2006.

[5] Gian-Carlo Rota. Combinatorial theory, old and new. In *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3*, pages 229–233. 1971.

[6] Rolf Schneider. *Convex Bodies: The Brunn–Minkowski Theory*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 2013.

[7] Yair Shenfeld and Ramon van Handel. Mixed volumes and the bochner method, 2018.

[8] Richard P. Stanley. Two combinatorial applications of the aleksandrov-fenchel inequalities. *J. Comb. Theory, Ser. A*, 31:56–65, 1981.

[9] RICHARD P. STANLEY. Log-concave and unimodal sequences in algebra, combinatorics, and geometrya. *Annals of the New York Academy of Sciences*, 576(1):500–535, 1989.

[10] W. T. Tutte. A homotopy theorem for matroids, ii. *Transactions of the American Mathematical Society*, 88(1):161–174, 1958.

[11] P. Vámos. The Missing Axiom of Matroid Theory is Lost Forever. *Journal of the London Mathematical Society*, s2-18(3):403–408, 12 1978.