maybe add a Rug logo & put contents on sepesate page?

Cryptomorphic Descriptions of Matroids

Adriel Matei, Béla Schneider, Javier Vela Castro, Juš Kocutar

June 12, 2023

Contents

1 Introduction

1.1 (In)dependence

In english language, two peolpe, objects or concepts are dependent on each other if both in some way influence one another. Two things being independent from each other then means that they in no way can affect eachother.

In mathematics there are many concepts where we can use these two words to describe certain phenomena, most notably, linear algebra. In linear algebra, a set of vectors is linearly dependent if you can write one of its vectors as a linear combination of the others. Using the word dependent here makes sense, because if you can use all others to build that one vector, then that vertor does not really stand on its own. An equivalent and more general definition is:

$$\{v_1, v_2, \ldots, v_n\} \text{ is linearly dependent if}$$

$$\text{there exists } a_1, a_2, \ldots, a_n \in \mathbb{R} \text{ not all zero, such that } a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$$

For linear independence we have the negation, which is:

$$\{v_1, v_2, \ldots, v_n\} \text{ is linearly independent if}$$

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0 \text{ implies that } a_1 = a_2 = \cdots = a_n = 0$$

There are many more fields that have this concept of (in)dependence present in some way. To relate these with another we will abstract the concept of (in)dependence into mere sets that follow certain rules. It turns out that by doing this we can find independence in places that do not even use the terms (in)dependence, most notably, graph theory.

1.2 Matroids

A matroid is a structure that abstracts the notion of independence. To construct a matroid we first start with a ground set that is finite. We do not want to work with infinite sets, because that causes lots of problems. Next, we construct a set of subsets of the ground set, following a couple of rules. Usually, this would be the set of independent sets. However, it turns out that there are many surprisingly equivalent (cryptomorphic) ways of defining a matroid, such as:

- Independent sets
- Bases
- Circuits
- Rank function
- Closure operator

- Flats

There are many more cryptomorphic ways to define a matroid, but the ones listed will be covered in this article. Each of these mathematical objects has two to four axioms that uniquely determine it as the object characterizing a matroid. To show the cryptomorphism, we will have to prove a certain equivalence each time. All of this will help us gain a deeper insight into the concept of dependence and independence.

2 Elementary Definitions

2.1 Independent sets

We will begin with the first possible way of defining what a *matroid* is. This way is arguably the simplest one because the properties are intuitive and not hard to visualize. When speaking about matroids we will always deal with finite sets, and the way we obtain a matroid from a finite set is to select some special selection of its subsets, these special sets correspond to the *independent* sets, and should obey some distinctive properties. This idea is precisely what the following definition is about.

Definition 1. *Let E be a finite set, possibly empty, and $\mathcal{I}$ a collection of subsets of E (i.e. some subset of the power set 2^E of E). We call the ordered pair $M = (E, \mathcal{I})$ a matroid if the following three properties are satisfied*

1. We have $\emptyset \in \mathcal{I}$.

2. If $I \in \mathcal{I}$ and $J \subset I$, then $J \in \mathcal{I}$.

3. If $J, I \in \mathcal{I}$ and $|J| < |I|$, then there exists $e \in I - J$ so that $J \cup e \in \mathcal{I}$.

*We call elements of $\mathcal{I}$ **independent sets**. We will refer to these three properties as (I1), (I2) and (I3).*

There are some alternatives to property 3 that are equivalent, for example we could alternatively write

3. If $I, J \in \mathcal{I}$ and $|J| = |I| + 1$, then there exists $e \in J - I$ such that $I \cup e \in \mathcal{I}$.*

or

*3.** If $X \subseteq E$ and I_1, I_2 are maximal members of $\{I \in \mathcal{I} | I \subseteq X\}$, then $|I_1| = |I_2|$.*

Below you find a representation of a matroid by writing all subsets of the ground set $\{1, 2, 3, 4\}$ and coloring them accordingly. The independent sets are the ones colored in orange. You can clearly see that the empty set is independent and that all subsets of independent sets are independent. The dependent sets, colored in cyan, are the sets that are not independent.

The definition of a matroid is designed to extract out the property that makes a subset of elements 'independent'. This leads us to our first examples, namely the so-called *representable*

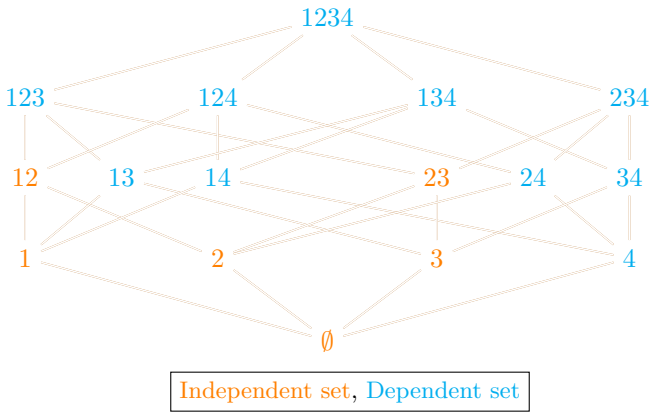


Figure 1: Diagram showing independent and dependent sets of a 4-element matroid.

matroids arising from linear algebra. We would that a subset of vectors is *independent* in a matroid, if and only if it is are *linearly independent* in the usual sense.

Let $A \in \mathrm{Mat}_{m\times n}(\mathbb{F})$ where $\mathbb{F}$ is a field. In the article we will not just be interested with $\mathbb{F} = \mathbb{C}$ or $\mathbb{F} = \mathbb{R}$ but also in finite fields [1].

Example 2.1. We will pick a concrete example of $A \in \mathrm{Mat}_{3\times 4}(\mathbb{R})$ to illustrate that the set of columns of a matrix has a natural matroid structure. Suppose

$$A = \begin{pmatrix} 2 & 0 & 2 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 3 & 3 & 0 \end{pmatrix}.$$

We would like to consider *the set of labels of columns of the matrix* A and form a matroid on it. This means we start with $E = \{1, 2, 3, 4\}$ so a finite set where the number 1 corresponds to the column $\begin{pmatrix} 2 & 1 & 0 \end{pmatrix}^T$, the number 2 corresponds to $\begin{pmatrix} 0 & -1 & 3 \end{pmatrix}^T$ and so forth. We now declare that a subset of E is called independent if and only if the corresponding set of column vectors is linearly independent as a set of vectors in $\mathbb{R}^3$. We can explicitly check what this means in our example. The sets $\{1\}$, $\{2\}$, $\{3\}$ are all independent because they correspond to non-zero vectors. For the two-element subsets we see that $\{1, 2\}$, $\{1, 3\}$ and $\{2, 3\}$ are all independent, while any two element subsets containing the last column are not. Finally, the 3-element subset $\{1, 2, 3\}$ is not independent because as vectors, the first and the second column sum up to the third. So to conclude, the collection of all independent sets is

$$\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\},$$

[1] In particular we are interested in $\mathbb{Z}/p\mathbb{Z}$ by which me mean integers modulo p where p is a prime number and will denote it by $\mathbb{F}_p$

which indeed satisfies the properties of collection of independent sets of a matroid. This is not a coincidence, we will prove that a collection of subsets formed from a matrix in the above way is always a matroid.

Theorem 1. *Let $A \in \mathrm{Mat}_{m\times n}(\mathbb{F})$ and $E = \{1, 2, \cdots, n\}$ be a finite set of n elements where the element i corresponds to the i-th column of the matrix A. We call a subset $I \subset E$ independent if and only if the column vectors that the members of I correspond to form a linearly independent set as members of $\mathbb{F}^n$, and denote the collection of all independent subsets as $\mathcal{I}$. Then $M = (M, \mathcal{I})$ is a matroid, and we denote it by $M[A]$.*

Proof. We need to check that the collection $\mathcal{I}$ satisfies the three properties for the collection of independent sets given in the definition.

1. First, $\emptyset$ is trivially in $\mathcal{I}$.

2. The second property is also satisfied because if $J \subset I$ and $I \in \mathcal{I}$ this means that the vectors corresponding to I form a linearly independent set. In particular, let $v_1, v_2, \cdots v_j, v_{j+1}, \cdots v_i$ be the column vectors corresponding to I, and that first j are also in J, that means $|I| = i$, $|J| = j$ and $j \leq i$. Then if for some linear combination we have $a_1v_1 + \cdots + a_jv_j = 0$, where $a_i \in \mathbb{F}$ then it is also true that $a_1v_1 + \cdots + a_jv_j + 0 \cdot a_{j+1} + \cdots + 0 \cdot a_i = 0$. Since the vectors of I are linearly independent it now follows that $a_1 = a_2 = \cdots a_j = 0$ as well. So the vectors corresponding to the elements of J are also linearly independent, which means by definition $J \in \mathcal{I}$.

3. Finally, we have to check third property. We assume that $J, I \in \mathcal{I}$ and $|J| < |I|$. We denote by V_J and V_I the vector subspaces of $\mathbb{F}^n$ spanned by vectors corresponding to J and I respectively. Because the vectors corresponding to J and I respectively are linearly independent, they also form a basis for V_J and V_I respectively. For any $e \in I - J$ we denote by $v(e) \in \mathbb{F}^n$ the column vector of A corresponding to e. Suppose some $e \in I - J$ has the property adding it to J does not change the dimension of the subspace spanned by J, i.e. $\dim(V_J \cup v(e)) = \dim(V_J) = |J|$. Then $v(e)$ is already in $V(J)$ because the vectors corresponding to J are linearly independent and if we do not increase the dimension, this means that $v(e)$ can be expressed as a linear combination of vectors corresponding to J. However, this cannot hold true for *every* $e \in I - J$. If it would then for every $e \in I - J$, the vector $v(e)$ would already lie in V_J, and because for all elements $i \in I \cap J$ we trivially have $v(i) \in V_J$ by definition, we would then have $V_I \subseteq V_J$. But this would mean that

$$|I| = \dim(V_I) = \dim(V_J) = |J| < |I|$$

which is a contradiction. So there is at least one $e \in I - J$ so that $\dim(V_J \cup v(e)) = \dim(V_J) + 1$, which means the vectors corresponding to $J \cup e$ form a linearly independent subset. Finally, this means that $J \cup e \in \mathcal{I}$ which proves the third property.

□

In order to talk about any classification of matroids we have to say when the two matroids are equivalent - representing the same structure of independent sets. Intuitively, it is nothing deep, the definition will just rephrase that the two are *equal* if it is possible to relabel the elements of the first matroid to the elements of the second without changing the independent sets.

Definition 2. *We call two matroids $M = (E, \mathcal{I})$ and $N = (F, \mathcal{J})$ isomorphic and denote it by $M \sim N$ if there exists a bijection $f : E \to F$ so that a subset $K \subset F$ is independent if and only if $K = f(L)$ for some independent set $L \in \mathcal{I}$.*

Definition 3. *We call a matroid M representable, if M is isomorphic to a matrix matroid $N[A]$ for some $A \in Mat_{m\times n}(\mathbb{F})$ over some field $\mathbb{F}$ and we call it $\mathbb{F}$-representable if it is representable over specific field $\mathbb{F}$.*

We will now define another important class of matroids. Due to its simplicity it will be suitable as an example in many of the notions defined in the proceeding text.

Definition 4. *Let $E = \{1, 2, \cdots, n\}$ and $\mathcal{I} = \{L \subset E \text{ such that } |L| \leq m\}$. Then $(E, \mathcal{I})$ is a matroid which we denote by $U_{m,n}$ and call it a uniform matroid of rank m on a n element set.*

Theorem 2. *The ordered pair $U_{m,n} = (E, \mathcal{I})$ is a matroid*

Proof. It is easy to check that $U_{m,n}$ is indeed a matroid.

1. For any $m \geq 0$ we have $\emptyset \in \mathcal{I}$ since $|\emptyset| = 0$.
2. If $I \in \mathcal{I}$ and $J \subset I$ then $|J| \leq |I|$ so $|J| \leq |I| \leq m$ implying $J \in \mathcal{I}$ by definition.
3. Finally, if $I, J \in \mathcal{I}$ and $|J| < |I|$ then for any $e \in I - J$ we will have $|J \cup e| = |J| + 1 \leq |I| \leq m$ so $J \cup e \in \mathcal{I}$ by definition for any $e \in I - J$.

□

2.2 Bases

Let $M = (E, \mathcal{I})$ be a matroid. We call a subset $B \subset E$ a *basis* if it is a *maximal independent set*. That means that B is an independent set and B is not properly contained inside any other independent set. It turns out that bases for matroids and bases in vector subspaces have some similarities in their properties. In particular the third property of independent sets immedietly guarantees us that all matroid bases have the same size, just like vector bases for finite-dimensional vector spaces.

Theorem 3. *Let $M = (E, \mathcal{I})$ be a matroid. All bases of M have the same size.*

Proof. Suppose for contradiction that the theorem does not hold and, without loss of generality, let B and S be two bases with $|B| < |S|$ - different size. By the third property of independent sets we know there exists $e \in S - B$ such that $B \cup e \in \mathcal{I}$. However, then B is properly contained inside $B \cup e$, another independent set, which contradicts its maximality. So the initial assumption that there exist two bases with different size is false. □

The concept of a basis is important because it allows us to define a *rank function* of a matroid which is the size of the maximal independent subset inside a given subset of a matroid. Because the sizes of all of such sets - bases - are equal, this will be a well-defined notion.

Similar to the set of independent sets, we can characterize the set of bases of M using these two properties:

Definition 5. *Let E be a non-empty finite set, and $\mathcal{B}$ be a collection of subsets of E, called bases, with the following properties:*

1. $\mathcal{B}$ is non-empty

2. If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 - B_2$, then there exists a $y \in B_2 - B_1$ such that $(B_1 - x) \cup y \in \mathcal{B}$.

We will refer to these two properties as (B1) and (B2).

Here below, you find a depiction of the matroid we have seen in chapter 2.1. This time, he have added the bases of the matroid, colored red. Two properties can be observed, first the bases are the maximal independent sets and both bases have two elements - the same size.

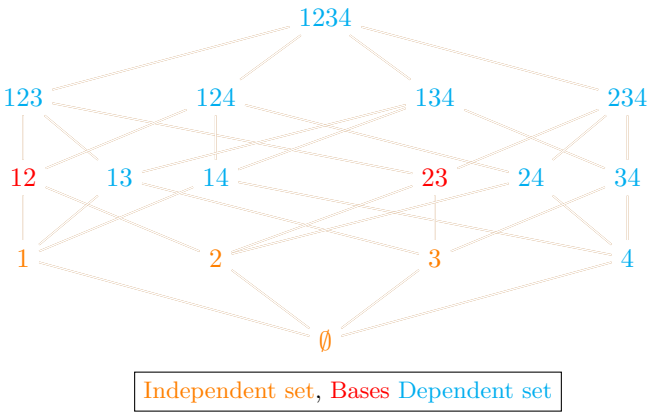


Figure 2: Diagram of a 4-element matroid

Let us prove that the set of bases of a matroid satisfy these conditions:

Proof. To prove the first property observe that by defintion $\emptyset$ is always in $\mathcal{I}$ so the collection of independent sets is nonempty. This directly implies that the collection of bases is nonempty, for

instance, an independent set with largest number of elements (there is at least one independent set! so we can talk about the largest one satisfying some properties) will be a basis, since it cannot be contained inside other independent set.

For the second property let $x \in B_2 - B_1$. We first note that (I2) implies that $B_1 - x$ is independent, since it is a subset of B_1. Since $|B_1 - x| < |B_2|$, we can apply (I3) on independent sets $B_1 - x$ and B_2 to get that there exists a $y \in B_2 - (B_1 - x)$ such that $(B_1 - x) \cup y \in \mathcal{I}$. Since $|(B_1 - x) \cup y| = |B_1|$ and that all maximal independent sets have the same cardinality, $(B_1 - x) \cup y$ must be a basis. Because y is also in $B_2 - B_1$, the property is fulfilled. □

Now that we have a new way to describe $\mathcal{B}$ with (B1) and (B2), we again need to prove that all elements in it are equicardinal. So let's do that.

Proof. Suppose that $\mathcal{B}$ is not equicardinal, that is, we have $|B_1| < |B_2|$ for some $B_1, B_2 \in \mathcal{B}$. From all B_1, B_2 where that holds, choose the pair that minimizes $|B_1 - B_2|$. Since B_1 is bigger, choose an element $b \in B_1 - B_2$ and apply (B2) to see that there exists a $d \in B_2 - B_1$ such that $(B_1 - b) \cup d \in \mathcal{B}$. With our choices of b and d, we can see that $|((B_1 - b) \cup d) - B_2| = |(B_1 - b) - B_2| < |B_1 - B_2|$. This, combined with that $|(B_1 - b) \cup d| = |B_1| < |B_2|$, tells us that B_1 and B_2 are actually not the minimal choice. This contradiction proves that $\mathcal{B}$ is equicardinal. □

To prove that the two properties are sufficient to describe the bases of M, we will that if $\mathcal{B}$ is any collection of subsets satisfying the bases axioms, then the independent sets should be all of the possible subsets of the the elements of $\mathcal{B}$:

Theorem 4. *Let $\mathcal{B}$ be a collection of subsets of a non-empty finite set E, satisfying (B1) and (B2). Let $\mathcal{I} = \{I \subset B : B \in \mathcal{B}\}$. Then $(E, \mathcal{I})$ is a matroid with $\mathcal{B}$ as its set of bases.*

Proof. Our goal is of course to show that $\mathcal{I}$ satisfies the conditions of independent sets. If we manage to do that we will have that $(E, \mathcal{I})$ is a matroid having $\mathcal{B}$ as its collection of bases.

1. Since (B1) tells us that $\mathcal{B}$ is nonempty and because $\emptyset$ is a subset of any set, in particular $\emptyset \subset B$ where B is some member of $\mathcal{B}$, we by definition have that $\emptyset \in \mathcal{I}$.

2. If $I \in \mathcal{I}$ and $J \subset I$, then by construction, $J \subset I \subset B$ for some $B \in \mathcal{B}$, which means that $J \in \mathcal{I}$. So $\mathcal{I}$ satisfies (I2).

3. Suppose (I3) fails for some $I, J \in \mathcal{I}$ with $|I| < |J|$. That means for all elements $x \in J - I$, $I \cup x \notin \mathcal{I}$. Let B_I and B_J be the elements of $\mathcal{B}$ that contain I and J, respectively, and choose the B_J so that $|B_J - (J \cup B_I)|$ is minimal.

   With our choice of I and J, it turns out that $J - B_I = J - I$. If this would not be the case, then there would be an element e in $B_I - I$ that is also in J. However, then $I \cup e \notin \mathcal{I}$, which contradicts $I \cup e \subset B_I$.

   Suppose now that $B_J - (J \cup B_I)$ is non-empty. Letting j be an element from this set, (B2) tells us that there is an element $i \in B_I - B_J$ such that $(B_J - j) \cup i \in \mathcal{B}$. However, then

$|((B_J - j) \cup i) - (J \cup B_I)| = |(B_J - j) - (J \cup B_I)| < |(B_J - (J \cup B_I)|$, which contradicts the minimality of our choice of B_J. Thus, $B_J - (J \cup B_I) = \emptyset$. This now implies that $B_J \subset J \cup B_I$, which implies that $B_J - B_I \subset (J \cup B_I) - B_I = J - B_I$. Since $J - B_I \subset B_J - B_I$, this proves equality between $B_J - B_I$ and $J - B_I$.

Next up we do the same thing, but this time proving that $B_I - (I \cup B_J$ is empty. Assuming the opposite by letting i be a part the set, (B2) tells us that there exists a $j \in B_J - B_I = J - B_I = J - I$ such that $(B_I - i) \cup j \in \mathcal{B}$. Since our choice of i tell us that $I \cup j \subset (B_I - i) \cup j$, it means $I \cup j \in \mathcal{I}$. This gives us precicely (I3), which contradicts our originil assumption. Thus, $B_I - (I \cup B_J) = \emptyset$. By the same logic we used in the previous paragraph, $B_I - B_J = I - B_J \subset I - J$.

We can use the fact that $\mathcal{B}$ is equicardinal to see that $|B_I - B_J| = |B_J - B_I|$. At last, we use all of our knowledge to get the following:

$$|I - J| \geq |B_I - B_J| = |B_J - B_I| = |J - B_I| = |J - I|$$

This inequality tells us that $|I| \geq |J|$, which is a contradiction with another one of our assumptions. Thus, $\mathcal{I}$ satisfies (I3). And thus, $(E, \mathcal{I})$ is a matroid.

The fact that $\mathcal{B}$ is now the set of bases of the matroid $(E, \mathcal{I})$ follows from the fact that all elements in $\mathcal{B}$ are maximal in $\mathcal{I}$. $\square$

2.3 Circuits

As mentioned before we can define a matroid in different forms, one of this other definitions is in terms of circuits. Before the definition, we need to introduce an additional concept. That is, a minimal dependent set, these are dependent sets whose all proper subsets are independent.

Now, we can state the following:

Definition 6. *Let $M = (E, \mathcal{I})$ be a matroid. Any subset $D \in \mathcal{I}$ which is not independent is called dependent. Circuit will be a minimal dependent set of an arbitrary matroid M. The collection will be denoted by C or $\mathcal{C}(M)$. Additionally, we define a circuit of a matroid M, that has n elements, as an n-circuit.*

The name is a reference to matroid circuits corresponding to circuits of the underlying graph when talking about graphic matroids.

Similarly, as with the independent sets, we can use the circuits to formulate a definition for a given matroid. And moreover, in the same way we can use the independent sets of a matroid to determine its circuits, we can use the circuits of a matroid to determine its independent sets.

So, we can characterize the concept of a matroid in the following way:

Definition 7. *Let E be a non-empty finite set, and $\mathcal{C}$ a collection of subsets of E, called circuits, such that:*

1. *$\emptyset \notin \mathcal{C}$*
2. *If C_1 and C_2 are members of $\mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$.*
3. *If C_1 and C_2 are distinct members of $\mathcal{C}$ and there exist an $e \in C_1 \cap C_2$, then there is a member C_3 of $\mathcal{C}$, such that $C_3 \subseteq (C_1 \cup C_2) - e$*

We will refer to these three properties as (C1), (C2) and (C3)

Again, we will use the same matroid example as before, this time adding circuits to the drawing (in blue). As you can see, the circuits are minimal dependent sets where everything above it is a dependent set. Also note how all independent sets do not contain any circuit.

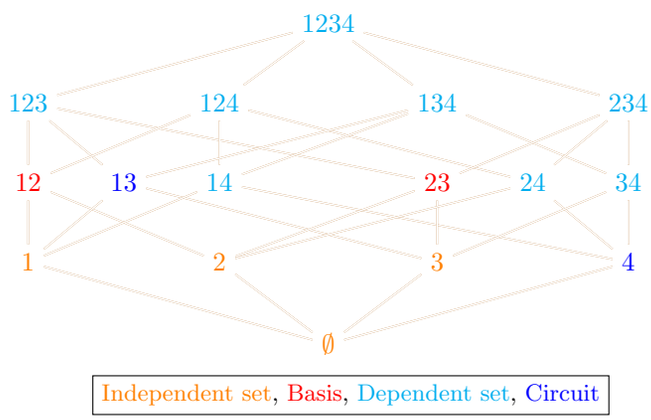
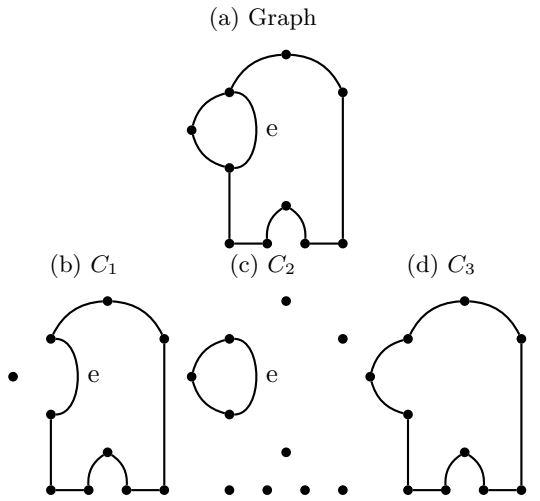


Figure 3: A graph of suspicious shape, having three cycles.



To get an intuition behind (C3), let us consider the matroid induced by the graph above. We will discuss graphic matroid later, but just know that a circuit is a cycle in the graph. Here, we have two circuits, C_1 and C_2, that share an edge, e. If you take the union of both circuits and remove the edge e from it, then that subgraph contains another cycle, circuit C_3.

We can say that a set $X \subseteq E$ is independent if and only if, it does not contain any circuit.

The concept of circuits points towards the direction of something similar to a complement of the independent sets, but not completely, since it is only the minimal dependent, and not all dependet subsets. We now have the following theorem.

Theorem 5. *Let E be a set and $\mathcal{C}$ be a collection of subsets of E which satisfies the conditions outlined above. Let $\mathcal{I}$ be the collection of subsets of E that contain no member of $\mathcal{C}$, that is*

$$\mathcal{I} = \{I \in 2^E | \text{ for all } C \in \mathcal{C} \text{ we have } C \not\subset I\} \tag{2.1}$$

The pair $(E, \mathcal{I})$ is a matroid having $\mathcal{C}$ as its collection of circuits.

Proof. We start by showing that $\mathcal{I}$ satisfies the necessary conditions for $(E, \mathcal{I})$ to be a matroid:

1. The only subset of $\emptyset$ is $\emptyset$, but $\emptyset \notin \mathcal{C}$, so $\emptyset$ satisfies (2.1), hence $\emptyset \in \mathcal{I}$.

2. Assume we have $X \subseteq Y \in \mathcal{I}$. Assume that $X \notin I$, i.e. there exists some $C \in \mathcal{C}$ such that $C \subseteq X$. We recall that $\subseteq$ is transitive, thus $C \subseteq Y$ and $Y \notin I$, hence a contradiction.

3. Given $X, Y \in \mathcal{I}$ with $|X| < |Y|$ we must show there exists some $e \in Y \setminus X$ such that $X \cup \{e\} \in \mathcal{I}$. Assume that such an e does not exist, i.e. for all $e \in Y \setminus X$ we have some circuit $C_e \in \mathcal{C}$ such that $C_e \subseteq X \cup \{e\}$. We obviously have $e \in C_e$, because otherwise $C_e \subseteq X$ and $X \notin \mathcal{I}$.

Let $X' = X \setminus Y$ and $Y' = Y \setminus X$. We will prove the statement by induction: given some set $S \subseteq X'$, a set of circuits $D \subseteq \mathcal{C}$ with $\forall C \in D, C \subseteq S \cup Y$ and a surjective but not injective function $f : D \to S$ such that $f(D)$ is maximal in size and $\forall C \in D, f(C) \in C$, our statement is proven. We will use induction on the size of S:

(a) If $S = \{e\}$ only has one element, we know that f is not injective, so we must have distinct $C_1, C_2 \in D$ such that $e = f(C_1) = f(C_2)$. We can use the 3-rd circuit axiom to generate some circuit $C_3 \subseteq C_1 \cup C_2 - e$. We recall that $C_1, C_2 \subseteq S \cup Y$, so $C_3 \subseteq S \cup Y - e$ which implies $C_3 \subseteq Y$, which is a contradiction.

(b) Inductive step. Assuming the statement is true for all choices of S with k elements, we will attempt to prove it is also true when S has $k+1$ elements. Recalling that f is not injective, we must have distinct $C_1, C_2 \in D$ such that $f(C_1) = f(C_2)$. Let $g = f(C_1)$. We have $g \in C_1, C_2$, so by the 3-rd circuit axiom we must have some circuit $C_3 \subseteq C_1 \cup C_2 - g$. Let $S' = C_3 \cap X'$.

For all $e \in S'$, we claim there must exist some $C_e \in D$ such that $e = f(C_e)$. Assume this is not the case, i.e. there is some $e \in S'$ such that no valid choice of C_e exists. Given that $e \in S'$, we know that either $e \in C_1$ or $e \in C_2$. After a potential swap, we assume that $e \in C_1$. We can now define $f'(C) = e$ when $C = C_1$ and $f'(C) = f(C)$. Because no choice of C_e exists, we know that $e \notin f(D)$. Because $f(C_1) = f(C_2)$ we have $f(D) = f(D - C_1)$ which lets us compute $f'(D) = f(D) \cup \{e\}$, which means $f(D)$ was not maximal, hence a contradiction. Our claim is then true.

Define $D' = \{C_e | e \in S'\} \cup \{C_3\}$. We've essentially proven in the last paragraph that $f : \{C_e | e \in S'\} \to S'$ is still a surjective function. It then follows that $h = f : D' \to S'$ is surjective as well. By the Pigeonhole principle, we know h cannot be injective, because $|D'| = |S'| + 1$. We are now almost ready to apply the induction hypothesis to (S', D', h). We've shown a choice for h exist. If this choice is not maximal, swap it with a maximal choice (we had to show that at least one choice exists for a maximal choice to exist). We can now apply the induction hypothesis, proving the statement.

We notice that X can be partitioned into X' and $X \cap Y$, hence $|X| = |X'| + |X \cap Y|$. We can follow a similar process for Y. Combining the two together with the fact that $|X| < |Y|$ yields that $|X'| < |Y'|$. We know that $Y \in \mathcal{I}$ so $\forall e \in Y', C_e \not\subseteq Y$, but $C_e \subseteq X \cup \{e\}$ therefore there must exist some $c_e \in C_e \cap X'$.

We define $D = \{C_e, e \in Y'\}$, $f(C_e) = c_e$ and $S = f(D)$. Furthermore, we know that f is not injective by the Pigeonhole principe (we have $|D| = |Y'| > |X'| \geq |S|$). We also know, by the definition of S, that f is surjective. We've shown a choice of f exists. If it is not maximal, swap it with a maximal choice. We can now apply the statement proven by induction to finish the proof.

this spacing looks a bit weird

It remains to prove that $\mathcal{C}$ is the set of circuits in the newly defined matroid. We start by proving

that all circuits have these properties:

1. $\emptyset \in \mathcal{I}$, therefore $\emptyset$ is not dependent (which means it cannot be a circuit)
2. A counterexample to this clause would violate the C_2 being minimal.
3. Assume a counterexample exists. Because $C_1 \cup C_2 - e$ does not contain a circuit, it must be an element of $\mathcal{I}$.

   We claim that $C_2 \setminus C_1$ is nonempty. Assume this is not the case. That would imply $C_2 \subseteq C_1$, but $C_1 \neq C_2$ by (C3), which means that C_1 is a proper subset of C_2. As both C_1 and C_2 are members of $\mathcal{C}$, this violates (C2), and is a contradiction. We can then assume some $f \in C_2 \setminus C_1$ exists.

   As C_2 is minimally dependent, we know that $C_2 - f$ is independent. Let I be a maximal independent subset of $C_2 \cup C_1$ which is a superset of $C_2 - f$. Clearly, $f \notin I$ (otherwise $C_2 \subseteq I \in \mathcal{I}$). Furthermore, as C_1 is a circuit, we know that $C_1 \not\subseteq I \in \mathcal{I}$ (otherwise C_1 would be independent). This means some $g \in C_1$ exists such that $g \notin I$. As $f \in C_2 \setminus C_2$, we know that $f \neq g$.

   As $I \subseteq C_1 \cup C_2$ and $f, g \in C_1 \cup C_2$ but $f, g \notin I$, we can infer that

   $$|I| \leq |C_1 \cup C_2 - f - g| = |C_1 \cup C_2| - 2.$$

   We also notice that $|C_1 \cup C_2 - e| = |C_1 \cup C_2| - 1$. We can now conclude by transitivity with $|C_1 \cup C_2| - 2 < |C_1 \cup C_2| - 1$ that $|I| < |C_1 \cup C_2 - e|$. We recall that both I and $C_1 \cup C_2 - e$ are members of $\mathcal{I}$. We can apply (I3) to generate a superset of I which contradicts it's maximallity.

It now remains to prove that having these properties is enough to be considered a circuit. Assume a subset C with these properties exists which is not a circuit. Clearly, $I \notin \mathcal{I}$ is implied by the definition of $\mathcal{I}$ seen above. This implies that C is dependent but not a circuit, which means C is not miminal. A proper subset $D \subsetneq C$ must then exists such that D is a circuit. As proven above, D satisfies the three axioms, hence $D \in \mathcal{C}$. We have now constructed a contradiction to (C2), hence our assumption that such a circuit exists is false.

We've proven that all circuits satisfy the three axioms, and that all subsets satisfying the axioms are circuits, which implies that $\mathcal{C}$ is indeed the set of circuits of the matroid we've constructed.

□

New page?

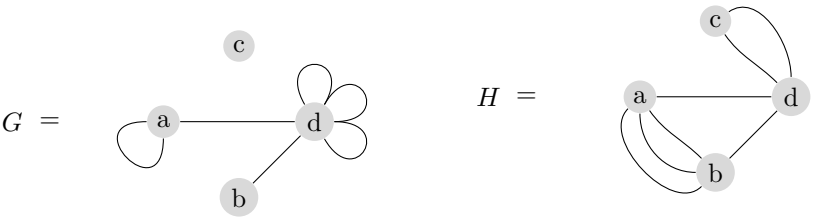
3 Graphic Matroids

rephrase sentence

First, we do not define graphs in completely the same way as in the graph theory class. We used the definition that a graph G is an ordered pair $G = (V, E)$ where V is a finite set (of vertices) and E is a collection of two-element subsets of V (of edges). We will extend the notion of edge to include

loops and *parallel edges*. For this, we will first illustrate the two notions. Intuitively a loop is an edge going from a vertex to itself, one can also have multiple loops on a single vertex.

For example, in the figure 4, we have a vertex a with a single loop and vertex d with 3 loops.



(a) Loops (b) Parallel edges

Figure 4: Graph G with loops and graph H with parallel edges

Above we see graphs G and H, one has loops and the other has parallel edges. One way to formalize both constructions, as done in [3] (for them to behave in the way we would like them to behave) is to define a graph to be an ordered pair (V, E), where V is a finite set, so unchanged, however, E is a *multiset* of edges. This allows the same two-element subset of V to appear multiple (but at most finitely many) times in E, even though it is the same set. Hence, we get parallel edges. For loops, we can get to a multiset consisting of a single element twice, and we also allow it to appear multiple times... However, the formal construction is not so important, as we will see in the future and one can usually restrict to simple graphs, which are by our terminology the ones without loops or parallel edges. However, we are interested in *properties* loops and parallel edges have. In particular, we see that by our definition of a cycle (a path (a walk (a sequence of adjacent vertices) which does not repeat vertices) which can repeat only one vertex (the ending and the starting vertex)), we have that if a loop is in a cycle, then the whole cycle consists only of that loop - we have one vertex appearing multiple times in a sequence - the beginning/ending vertex. Also, for parallel edges, at most one from a class of parallel edges connecting the same two vertices can appear in a cycle.

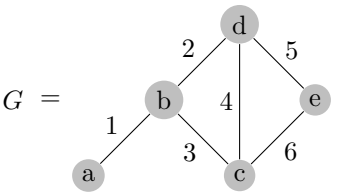


Figure 5: Simple graph on 6 edges

Consider a concrete example of a simple graph and build a matroid out of it. Let us label the set of edges $E = \{1, 2, 3, \cdots, 6\}$. We will define a collection of subsets $\mathcal{C}$ of E where $C \in \mathcal{C}$ if and only if the set of edges of C forms a cycle in G. We check that

$$\mathcal{C} = \{\{2,3,4\},\{4,5,6\},\{2,3,5,6\}\}.$$

Not surprisingly, the set E with the collection $\mathcal{C}$ being as its set of circuits is, in fact, a matroid we can check that there is no $\emptyset$ in $\mathcal{C}$, none of its members is properly contained in each other, and finally "circuit elimination axiom" works for all three possibilities of taking pairs of elements of $\mathcal{C}$. We will now prove that this works for a general graph.

Theorem 6. *Let $G = (V, E)$ be a graph and let C_1, C_2 be sets of edges of two distinct cycles with a nonempty intersection. Then for any $e \in C_1 \cap C_2$ there exists a cycle $C_3 \subset C_1 \cup C_2 - e$, making the set E of edges into a matroid with the set of circuits equal to the collection of cycles.*

Proof. Let the cycle C_1 correspond to the sequence of incident vertices $v_0, \cdots, v_n = v_0$ and let without loss of generality the special edge in the interesection be the edge $e = \{v_0, v_1\}$. Our goal is to find a cycle in the set of edges $C_1 \cup C_2 - e$, which is not difficult, the idea is that we go around C_1 until we can jump to C_2 for the first time, then we go back to e via C_2 from the "backward direction".

Let k be the smallest integer $1 < k \leq n$ such that the vertex v_k is in the cycle C_2. We know that such an integer exists because v_n is in the cycle C_2.

Let $v_k, w_{k+1}, w_{k+2}, \cdots, v_1$ be the path of vertices in the cycle C_2 which does not include the edge e. We know that such a path exists, because C_2 is a cycle, so from any two distinct vertices, in particular v_k and v_1 there are two paths going from v_k to v_1 including only the vertices of C_2 - we pick the one that does not include the edge e.

We claim that the cycle consisting of vertices $v_1, v_2, \cdots v_k, w_{k+1}, \cdots, v_1$ is the desired one and denote its set of edges by C_3. By construction the sequence of vertices $v_1, v_2, \cdots v_k, w_{k+1}, \cdots, v_1$ is a cycle, namely the neighboring vertices are incident and except v_1 there is no vertex repeating, because we have chosen $v_2, v_3, \cdots v_{k-1}$ to be disjoint from C_2. Crucially, $e \notin C_3$ because we have chosen path $v_k, w_{k+1}, \cdots v_1$ to not include the edge e and $v_1, v_2, \cdots v_k$ does not include it because $e = \{v_n = v_0, v_1\}$ and there is no v_0 in our cycle. Finally, all of the vertices of C_3 are inside the vertices of C_1 and C_2 by construction so, to conclude the set C_3 has the desired property $C_3 \subset (C_1 \cup C_2) - e$.

We have to check to check the possibility that e might be a loop or a parallel edge as well, the above argument works assuming G is a simple graph. If e is a parallel edge than the above argument does still hold since we only now that there is more than one edge between v_0 and v_1 which does not change anything. However, if e is a loop then by our convention, a cycle consisting of a loop can just be that loop and nothing else, heuristically, because it begins and ends at a single vertex. So $C_1 = C_2 = \{e\}$ which is a contradiction, since we have assumed C_1 and C_2 are distinct.

To show that the set E is a matroid with the collection $\mathcal{C}$ of cycles as circuits we only have to verify the first two circuit axioms. The empty set is by our defintion not a cycle, because by our defintion a cycle always includes a nonempty set of vertices it is build upon. If there are at least

two vertices, than we have incident edges inside, and the only cycle on one vertex is a loop, which is still an edge.

The show the first property suppose we have two sets of edges of cycles such that $C_1 \subset C_2$ and assume for contradiction there is some $e \in C_2 - C_1$. Then (we are assuming neither of the cycles are loops, that case is obvious) the set of edges $C_2 - e$ corresponds to a path from the vertices which e connects. However there is a cycle $C_1 \subset C_2 - e$ which is a subset of a path - a contradiction. So if $C_1 \subset C_2$ then $C_2 - C_1$ is empty, in particular then $C_2 = C1$ and all three circuit axioms are satisfied. □

Definition 8. *We call a matroid M graphic if it is isomporphic to $(E, \mathcal{I})$ where E is the set of edges of some graph and the set of circuits is given by the set of all edge cycles.*

We thus know that given any graph G we have natural matroid structure on its set of edges, by declaring graph cycles to be circuits. Because we know other equivalent descriptions of matroids it is natural to ask what are the independent sets or bases in the case of graphic matroids.

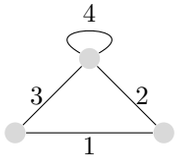
Suppose that the set of edges B is a base of a graphic matroid. We know that this means that B is independent (interpretation of which in the case of graphic matroids we do not yet know) however, adding any element of $E - B$ to B, i.e. any edge not in B to B, we get a *dependent set*, which means it contains a circuit. By our defintion this means that it has to contain an edge cycle. Combining all we see that the set of edges B has the property that it does not contain any cycles, however adding any edge makes a cycle - this is the precisely one of the equivalent characterizations of *spanning forrests*. we cannot say spanning trees because the graph might not be connencted.

Any independent set is a subset of some basis, so in graphic matroids the set of edges that is independent has to be a subset of some spanning forrest, which means it is just a forrest.

As an example we will show that many matroids shown until now are, in fact, graphic.

$$\mathrm{A} = \begin{pmatrix} 2 & 0 & 2 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 3 & 3 & 0 \end{pmatrix}$$

(a) Matrix A

$H =$ 

(b) Graph H

Figure 6: Matroid $M[A]$ is graphic; it is isomprphic to the graphic matroid G

In 7 we see that the graph H exactly to corresponds to the vector matroid formed on matrix A. Edge 4 is a loop, so a dependent set, corresponding to the fact that the fourth column is a zero vector. Similarly, any two element sets of nonzero vector are independent, corresponding to the fact that any two non-loop edges do not form a cycle in the graph. Finally, any set of three or more edges in dependent, which is easily seen in the graph because we have 3 vertices so the size of a spanning forrest is at most 3 - 1 = 2.

4 Rank Function

The rank function is a function $r : 2^E \to \mathbb{Z}_{\geq 0}$ that, when given a $X \subset E(M)$, gives you the cardinality of the maximal independent set contained in X. In other words:

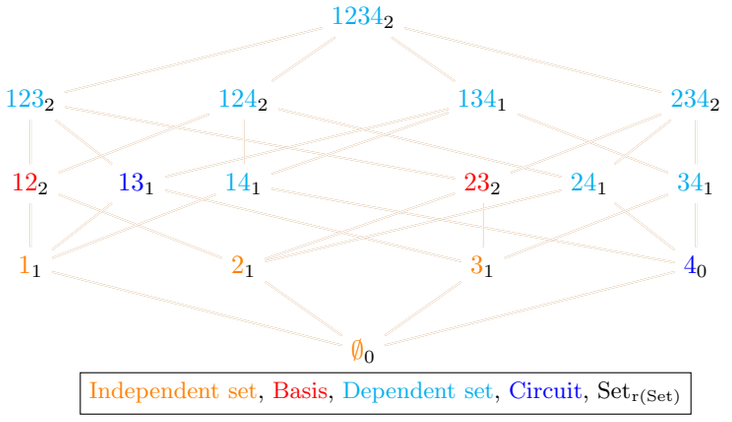
$$r(X) = \max\{\, |I| : I \in \mathcal{I} \text{ and } I \subset X\}$$

For example, $r(M) := r(E(M)) = |B|$ for some $B \in \mathcal{B}(M)$. Like all the previous times, we can characterize the rank function with the following properties:

Definition 9. *Let E be a non-empty finite set, and let $r : 2^E \to \mathbb{Z}_{\geq 0}$ be a function satisfying:*

1. *If $X \subset E$, then $0 \leq r(X) \leq |X|$*
2. *If $X \subset Y \subset E$, then $r(X) \leq r(Y)$*
3. *If $X, Y \subset E$, then $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$*

Below, we again find our example matroid drawing. This time, instead of using a new color, we will denote the rank of each set by writing it in subscript below the set. We can see that the rank of any set is atmost its cardinality and each subset of some set has at most the rank of that set. As always it takes a bit more effort to show that the last property holds for a given matroid.



Now, let us prove that the rank function of a matroid satirfy these properties:

Proof.

1. Since the co-domain is $\mathbb{Z}_{\geq 0}$, $0 \leq \text{r}(X)$. Since the maximal independent set contained in X is... contained in X, the cardinality of that set must be smaller or equal to $|X|$. Thus, $0 \leq \text{r}(X) \leq |X|$.

2. Let I_X be a minimal independent set contained in X, so $\mathrm{r}(X) = |I_X|$. $I_X \subset X \subset Y$ implies that I_X is an independent set contained in Y. Since I_X may or may not be a maximal independent set contained in Y, $\mathrm{r}(X) = |I_X| \leq \mathrm{r}(Y)$.

3. We assume that $A \subset B \subset E$. Let $I_{A\cap B}$ be a maximal independent set contained in $A \cap B$. Since $A \cap B \subset A \cup B$, $I_{A\cap B}$ must be an independent set contained in $A \cup B$. Let $I_{A\cup B}$ be $I_{A\cap B}$ extended to be a **maximal** independent set contained in $A \cup B$.

   Now let us take a look at $I_{A\cup B} \cap A$. Since the set is contained in A, (I2) tells us that $I_{A\cup B} \cap A$ is in independent set contained in A. Since the set may or may not be maximal in that regard, $|I_{A\cup B} \cap A| \leq \mathrm{r}(A)$. Similarly, $|I_{A\cup B} \cap B| \leq \mathrm{r}(B)$.

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

   Since $I_{A\cup B} \subset A \cup B$, $I_{A\cup B} \cap (A \cup B) = I_{A\cup B}$.

   Since $I_{A\cap B} \subset I_{A\cup B}$, $I_{A\cup B} \cap (A \cap B) \supset I_{A\cap B} \cap (A \cap B) = I_{A\cap B}$. Let $e \in I_{A\cup B} \cap (A \cap B)$. Aiming for contradiction, suppose $e \notin I_{A\cap B}$. Since $I_{A\cap B} \cup e \subset I_{A\cup B}$, $I_{A\cap B} \cup e$ must be an independent set conained in $A \cap B$. This contradicts the fact that $I_{A\cap B}$ is a maximal in that regard. Thus, $e \in I_{A\cap B}$. This proves that $I_{A\cup B} \cap (A \cap B) \subset I_{A\cap B}$, which implies equality between the two sets.

   Thus,

$$\mathrm{r}(X) + \mathrm{r}(Y) \geq |I_{A\cup B}| + |I_{A\cap B}| = \mathrm{r}(A \cup B) + \mathrm{r}(A \cap B)$$

□

One might observe that the rank of an independent set is the cardinality of the set itself. This is because the largest independent set that is contained in this independent set is ofcourse the independent set itself. With this property, we can define the set of independent sets with the three properties of the rank function.

Theorem 7. *Let E be a finite set, and let $r : 2^E \to \mathbb{Z}_{\geq 0}$ be a function satisfying (R1)-(R3). Let $\mathcal{I} = \{I \subset E : r(I) = |I|\}$. Then $(E, \mathcal{I})$ is a matroid with r as its rank function.*

Before we prove this, let's prove this small theorem first:

Theorem 8. *Let E be a finite set and $r : 2^E \to \mathbb{Z}_{\geq 0}$ be a function satisfying (R2) and (R3). Let $X, Y \subset E$. Then if for all $y \in Y - X$, $r(X \cup y) = r(X)$, then $r(X \cup Y) = r(Y)$.*

Proof. We will prove that the statement holds with $Y - X = \{a_1, a_2, \ldots, a_k\}$ holds for all itegers k.

1. Base case: $k = 1$

   If $\mathrm{r}(X \cup a_1) = \mathrm{r}(X)$, then $\mathrm{r}(X \cup Y) = \mathrm{r}(X \cup (Y - X)) = \mathrm{r}(X \cup a_1) = \mathrm{r}(X)$.

2. Induction Step: Assume the statement holds for $k = n$.

3. Let $k = n+1$: Assume that $Y - X = \{a_1, \ldots, a_{n+1}\}$ for all $i \in \{1, \ldots, n+1\}$ $\mathrm{r}(X \cup a_i) = \mathrm{r}(X)$. Then, using the assumption and our induction assumption,

$$\mathrm{r}(X) + \mathrm{r}(X) = \mathrm{r}(X \cup \{a_1, \ldots, a_n\}) + \mathrm{r}(X \cup a_{n+1})$$

Using (R3), we get

$$\geq \mathrm{r}([X \cup \{a_1, \ldots, a_n\}] \cup [X \cup a_{n+1}]) + \mathrm{r}([X \cup \{a_1, \ldots, a_n\}] \cap [X \cup a_{n+1}])$$

$$= \mathrm{r}(X \cup \{a_1, \ldots, a_{n+1}\}) + \mathrm{r}(X)$$

Using (R2), we get

$$\geq \mathrm{r}(X) + \mathrm{r}(X)$$

Since $\mathrm{r}(X) + \mathrm{r}(X)$ is on both sides, equality holds throughout. Thus, $\mathrm{r}(X \cup \{a_1, \ldots, a_{n+1}\}) = \mathrm{r}(X \cup Y) = \mathrm{r}(X)$. And thus, the statement holds for $k = n + 1$.

Thus, by mathematical induction, the statement holds for all integers k. □

Finally, we can prove Theorem 5:

Proof. To prove that $(E, \mathcal{I})$ is a matroid, we will check if $\mathcal{I}$ satisfies (I1)-(I3).

1. (R1) tells us that $0 \leq \mathrm{r}(\emptyset) \leq |\emptyset| = 0$, which implies that $\mathrm{r}(\emptyset) = 0 = |\emptyset|$, which means that $\emptyset \in \mathcal{I}$, so (I1) is satisfied.

2. Assume we have $J \subset I \in \mathcal{I}$. Then, using (R3),

$$\mathrm{r}(J) + \mathrm{r}(I - J) \geq \mathrm{r}(J \cup [I - J]) + \mathrm{r}(J \cap [I - J]) = \mathrm{r}(I) + \mathrm{r}(\emptyset) = |I|$$

Using (R2), we also get that

$$\mathrm{r}(J) + \mathrm{r}(I - J) \leq |J| + \mathrm{r}(I - J) \leq |J| + |I - J| = |I|$$

This implies that equality must hold throughout. At last, we show that

$$\mathrm{r}(J) + \mathrm{r}(I - J) = |J| + \mathrm{r}(I - J) \Rightarrow \mathrm{r}(J) = |J|$$

Thus, $J \in \mathcal{I}$, so I2 is satisfied.

3. Suppose (I3) does not hold for some $I, J \in \mathcal{I}$ with $|I| > |J|$. Then for all $e \in I - J$, $J \cup e \notin \mathcal{I}$. Also, remember that $I, J \in \mathcal{I}$ means that $\mathrm{r}(I) = |I|$ and $\mathrm{r}(J) = |J|$.

   Since $J \subset J \cup e$, we can use (R1) and (R2) to see that

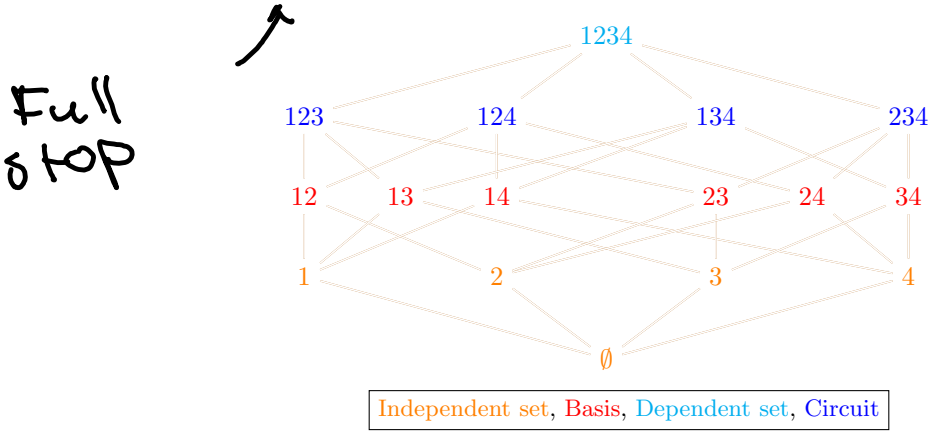
$$|J| = \mathrm{r}(J) \leq \mathrm{r}(J \cup e)| \leq |J \cup e| = |J| + 1$$

   $J \cup e \notin \mathcal{I}$ tells us that $\mathrm{r}(J \cup e) \neq |J \cup e|$, so that must mean that $\mathrm{r}(J \cup e)$ is equal to what's on the left hand side, so $\mathrm{r}(J)$.

   This gives us that for all $e \in I - J$, $\mathrm{r}(J \cup e) = \mathrm{r}(J)$, which, according to Theorem 6, implies that $\mathrm{r}(J \cup I) = \mathrm{r}(J) = |J|$. However, since $I \subset J \cup I$, (R2) tells us that $\mathrm{r}(J \cup I) \geq \mathrm{r}(I) = |I|$, which means that $|J| \geq |I|$. This contradicts our assumption that $|J| < |I|$. Thus, (I3) is satisfied.

Thus, $(E, \mathcal{I})$ is a matroid. □

Example 4.1. We will consider the uniform matroid $U_{2,4}$ and show that it is $\mathbb{F}_3$-representable, while it is not $\mathbb{F}_2$-representable. First, $U_{2,4} = (\{1, 2, 3, 4\}, \mathcal{I})$ where the bases are all of the two element subsets of $\{1, 2, 3, 4\}$, so the matroid looks like:



Suppose $U_{2,4}$ were $\mathbb{F}_2$-representable. Then there is some $A = \mathrm{Mat}_{m \times 4}(\mathbb{F}_2)$,

$$A = \begin{pmatrix} v_1 & v_2 & v_3 & v_4 \end{pmatrix}$$

so that $U_{2,4} \sim M[A]$. We have the following observation.

Lemma 1. *Suppose a set of vectors $A = \{w_1, w_2, \cdots, w_r\} \subset \mathbb{F}_2^n$ is minimaly linarly dependent, that means that it is linarly dependent but any proper subset of it is linearly independent. Then $w_1 + w_2 + \cdots + w_r = 0$.*

Proof. Because A is linearly dependent, there exists a set of scalars $\{a_1, a_2, \cdots, a_r\} \in \mathbb{F}_2$ not all zero such that

$$\sum_{i=1}^{r} a_i v_i = 0.$$

If for some $1 \leq j \leq r$ we have $a_j = 0$ then we also have

$$\sum_{\substack{i=1 \\ i \neq j}}^{r} a_i v_i = 0$$

but not all out of $a_1, \cdots a_{j-1}, a_{j+1}, \cdots a_r$ are 0. This means that $v_1, \cdots, v_{j-1}, v_{j+1}, \cdots, v_r$ is linearly dependent, which is not true by assumption. Therefore, for all $1 \leq j \leq r$ we have $a_j \neq 0$. But since the field is $\mathbb{F}_2$ this forces $a_j = 1$ for all j. Hence, we obtained what we want, namely

$$\sum_{i=1}^{r} a_i v_i = 0 = \sum_{i=1}^{r} 1 \cdot v_i = 0.$$

□

If the matroid $U_{2,4} \sim M[A]$ for the above A then we would have all of the three element subsets of vectors to be minimally linearly dependent. This means by 1 that $v_1+v_2+v_3 = 0$ and $v_1+v_2+v_3 = 0$. However, we are in $\mathbb{F}_2$ so

$$v_1 + v_2 + v_3 = 0 \iff v_1 + v_2 + (v_3 + v_3) = v_3 \iff v_1 + v_2 = v_3$$

And in the same way $v_1 + v_2 = v_4$. This implies that

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

so the set $\{v_3, v_4\}$ is linearly dependent, which is a contradiction. So $U_{2,4}$ is not $\mathbb{F}_2$-representable. However, $U_{2,4}$ is $\mathbb{F}_3$-representable, for instance the following matrix taken from [3, 20] works

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

since we see that no vector is 0, so all singletons are independent. No vector is a scalar multiple of each other, so two element subsets are independent. Finally, no 3-element subsets can be independent, since the dimension of the $\mathbb{F}_3^2$ is 2, so the dimension of any subspace is at most 2.

We will also show that $U_{2,4}$ has an interesting property that it is not a graphic matroid. In other words, we can show that there is no graph G such that $U_{2,4} \sim M$ where M is the matroid formed by the set of edgs of G with the usual rules.

We will show $U_{2,4}$ is not graphic by contradiction, that is assume $U_{2,4}$ is graphic and let G be the graph it represents. Then G has four edges and since all two-element subsets of $U_{2,4}$ are independent we see that G has no loops or parallel edges. In particular, all three element subsets of $U_{2,4}$ are

circuits, so in the graph the edges they correspond to form a cycle. Both if both sets $\{1, 2, 3, \}$ and $\{1, 2, 4\}$ corresonds to edge cycles without parallel edegs it immediatly follows that 3 and 4 connect the same vertices, i.e. are parallel edges, which is a contradiction. $\not\in$ $U_{2,4}$ is not graphic.

5 Closure Operator

We will introduce one more important notion, the one of closure operator. As the name suggests, it is a map between objects of the same type. Our objects are, of course, the subsets of the ground set of a matroid. The idea of the closure operator is that it adds to any subset $X \subset E$, whatever is left in E that does not change the rank when added to X. In doing so it will produce *closed sets* which are in matroid theory called flats, another collection of subsets with distinctive properties.

Closure will also admit desirable interpretation in the case of the prototypical examples of representable and graphic matroids. In the case of representable matroids, in will add to X all elements which are in the vector span of X and contained in E (thus it will not increase the vector rank of E). In the case of graphic matroids it will add to any set of edges, all edges that create cycles between its sets of vertices (thus will not increase the size of spanning forrest).

Definition 10. *Let $M = (E, \mathcal{I})$ be a matroid. The closure operator is a function* $\mathrm{cl} : 2^E \to 2^E$ *such that*

$$\mathrm{cl}(X) = \{x \in E \mid r(X \cup x) = r(X)\}.$$

The operator has numerour important properties and we will immediatly also prove the reverse statement. Namely, that these characteristic properties *uniquely characterize* the closure operator of a matroid.

Theorem 9. *Let $M = (E, \mathcal{I})$ be a matroid and* $\mathrm{cl} : 2^E \to 2^E$ *be a function. Then* cl *is the closure operator of M* ***if and only if***

1. *For any $X \subset E$ we have $X \subset \mathrm{cl}(X)$*
2. *If $X \subset Y \subset E$ then $\mathrm{cl}(X) \subset \mathrm{cl}(Y)$.*
3. *For all X we have $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$*
4. *Let $X \subset E$ and $b \in \mathrm{cl}(X \cup a) - \mathrm{cl}(X)$ then $a \in \mathrm{cl}(X \cup b)$*

Proof. All of the four statements in the only if direction (assuming cl is the closure operator) are pretty straightforward and we will prove them first. We first assume cl is the closure operator and would like to show the four properties.

1. If $X \subset E$ is arbitrary and we pick any element $x \in X$ then $X \cup x = X$. Consequently $r(X \cup x) = r(X)$ thus $x \in \mathrm{cl}(X)$ by defintion of the closure operator which shows the inclusion $X \subset \mathrm{cl}(X)$.

2. Let $X \subset Y \subset E$ and $x \in \mathrm{cl}(X)$. This is equivalent to saying $\mathrm{r}(X \cup x) = \mathrm{r}(X)$. Because we would like to show that $x \in \mathrm{cl}(Y)$ we would by definition like that $\mathrm{r}(Y \cup x) = \mathrm{r}(Y)$. In particular, we observe that we can without loss of generality assume $x \in \mathrm{cl}(X) - Y$ since the result trivially follows if x is already in Y.

   This immediatly incentivizes us to check some rank function inequalities containing the sets $X, Y - X$ and these sets containing x. In particular, it would be good if we would come to the inequality $\mathrm{r}(Y \cup x) \leq \mathrm{r}(Y)$. So our goal is to choose a suitable set A such that $Y \cup A = Y \cup x$ while $\mathrm{r}(Y \cap A) = \mathrm{r}(A)$ and we could use the semi-modular inequality of the rank function (R3). More specifically, what we would like is

$$\mathrm{r}(\underbrace{Y \cup A}_{=Y \cup x}) + \underbrace{\mathrm{r}(Y \cap A)}_{=\mathrm{r}(A)} \leq \mathrm{r}(Y) + \mathrm{r}(A).$$

   One A that does exactly this is $A = X \cup x$. Then we have, since $X \subset Y$ that $Y \cup A = Y \cup X \cup x = Y \cup x$, and since we are assuming $x \in \mathrm{cl}(X) - Y$ we have $Y \cap (X \cup x) = X$.

   We see that

$$\mathrm{r}(Y \cup (X \cup x)) + \mathrm{r}(X) \leq \mathrm{r}(Y) + \mathrm{r}(X \cup x)$$

   and since $\mathrm{r}(X \cup x) = \mathrm{r}(X)$ by assumption, we have $\mathrm{r}(Y \cup x) \leq \mathrm{r}(X)$ what we wanted to show. To conclude, the inequality $\mathrm{r}(Y) \leq \mathrm{r}(Y \cup x)$ follows by (R2) so we have $\mathrm{r}(Y) \leq \mathrm{r}(Y \cup x) \leq \mathrm{r}(X)$ implying $\mathrm{r}(Y \cup x) = \mathrm{r}(X)$ so by defintion $x \in \mathrm{cl}(Y)$.

   So we have shown the inclusion $\mathrm{cl}(X) \subset \mathrm{cl}(Y)$ which was our goal.

3. By combining the first and the second property already of closure we have already proven, the inclusion $\mathrm{cl}(X) \subset \mathrm{cl}(\mathrm{cl}(X))$ follows. We have to exhibit the reverse one as well, so suppose $z \in \mathrm{cl}(\mathrm{cl}(X))$. This means $\mathrm{r}(\mathrm{cl}(X) \cup z) = \mathrm{r}(\mathrm{cl}(X))) = \mathrm{r}(X)$ where the last inequality follows by the 8, namely for all $v \in \mathrm{cl}(X)$ we by definition have $\mathrm{r}(X \cup v) = \mathrm{r}(X)$ so by the 8 we have $\mathrm{r}(\mathrm{cl}(X)) = \mathrm{r}(X)$. But now we have, since $X \subset \mathrm{cl}(X)$ that

$$\mathrm{r}(X) \leq \mathrm{r}(X \cup z) \leq \mathrm{r}(\mathrm{cl}(X) \cup z) = \mathrm{r}(X)$$

   therefore the equality holds in all ineqalities above. In particular, this means that $\mathrm{r}(X \cup z) = \mathrm{r}(X)$ which by defintions means that $z \in \mathrm{cl}(X)$. So the desired inclusion $\mathrm{cl}(\mathrm{cl}(X)) \subset \mathrm{cl}(X)$ also holds, which finally implies the desired equality of sets $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$.

4. Let $X \subset E$ be arbitrary and $b \in \mathrm{cl}(X \cup a) - \mathrm{cl}(X)$. Since, $b \in \mathrm{cl}(X \cup a)$ we have $\mathrm{r}((X \cup a) \cup b) = \mathrm{r}((X \cup b) \cup a) = \mathrm{r}(X \cup a)$ by definition.

Now since $b \notin \mathrm{cl}(X)$ then by defninition $\mathrm{r}(X \cup b) \neq \mathrm{r}(X)$, and because $X \subset X \cup b$ we have by (R2) that $\mathrm{r}(X \cup b) > \mathrm{r}(X)$. In particular, since the rank function measures the size of the largest indpependent set inside of a given subset we have that $\mathrm{r}(X \cup b) = \mathrm{r}(X) + 1$.

Now since $\mathrm{r}(X \cup a \cup b) = \mathrm{r}(X \cup a)$, and by the same reason as in the previous paragraph, since $\mathrm{r}(X \cup a)$ is either $\mathrm{r}(X)$ or $\mathrm{r}(X) + 1$, we have it is in fact equal to $\mathrm{r}(X) + 1$ since $\mathrm{r}(X \cup a) = \mathrm{r}(X \cup a \cup b) \geq \mathrm{r}(X \cup b) = \mathrm{r}(X) + 1$.

So we have $r((X \cup b) \cup a) = \mathrm{r}(X \cup b)$ or in other words, $a \in \mathrm{cl}(X \cup b)$ by definition, which is precisely what we wanted to show.

more

Now we prove the complicated reverse direction. We assume we have a finite set E and an arbitrary function function $\beta : 2^E \to 2^E$ satifying the properties of the closure operator listed above.

Unlike the proofs of the reverse implication of the cryptomorphisms in terms of bases, circuits or rank function, where we had a very straightforward way to spot where the independent sets should appear (for bases they are all of the subsets of members of $\mathcal{B}$, for circuits they are all sets which contain no members of $\mathcal{C}$ and for the rank function they are sets with the property that $\mathrm{r}(X) = |X|$), this is now not the case, or is at least not immediatly appearent.

So we will not relate the function β directly to the indepedent sets, but rather some other cryptomorphic defintion of matroids we have already proven. In particular, observe that the if $\mathrm{cl}(X) = E$ holds for some subset $X \subseteq E$ this means that the rank of X is $r(E)$, or in other words the maximal indpendent set inside of X is a *basis*.

So our goal is to look at the collection of all subsets such that $\beta(X) = E$ and prove that the subcollection of its *minimal sets* satisfies the axioms for the collection of bases of a matroid. Therefore we define $\mathcal{B}' = \{X \subset E \mid \beta(X) = E\}$ and call $\mathcal{B}$ the collection of minimal members of $\mathcal{B}$, for reminder, that are sets which are in $\mathcal{B}$ but do not contain any members of $\mathcal{B}$ as their proper subsets.

1. We have to prove that $\mathcal{B}$ satisfies the two basis axioms. The first one (B1) is evident since by the first property of closure operator we have the first inclsuion in $E \subset \beta(E) \subset E$ and the second follows because β maps into 2^E. So $E \in \mathcal{B}'$ which in particular implies that $\mathcal{B}'$ and consequently $\mathcal{B}$ are nonempty.

2. For the second property (B2) assume B_1, B_2 are distinct elements of $\mathcal{B}$. Because $\mathcal{B}$ constitutes of *minimal* sets we know that if they are distinct one cannot be a subset of another. So let us pick any $x \in B_1 - B_2$. We observe two things, first, $\beta(B_1) = E$ and $\beta(B_1 - x) \neq E$ since B_1 is minimal. It is also clear that there exists $y \in B_2 - B_1$ such that $y \in E - \beta(B_1 - x)$, this is because, otherwise all of the elements of B_2 would be in $\beta(B_1 - x)$, but then we would have that $B_2 \subset \beta(B_1 - x)$ by (CL2) we would have that $E = \beta(B_2) \subset \beta(\beta(B_1 - e)) = \beta(B_1 - e) \neq E$. So by (CL4) we have that we can exchange x and y in the following inclusion.

$$y \in E - \beta(B_1 - x) = \beta((B_1 - x) \cup x) - \beta(B_1 - x)$$

which directly implies that $x \in \beta((B_1 - x) \cup y)$. Now we are done, because this means that

$$\beta((B_1 - x) \cup y) = \beta(\beta((B_1 - x) \cup y)) = \beta(\beta((B_1 - x) \cup y) \cup x) \supset \beta(B_1) = E.$$

Thus $(B_1 - x) \cup y$ is in $\mathcal{B}'$ by definition, since its β is E. We still have to show that $(B_1 - x) \cup y$ is minimal.

Therefore we will prove separatly that all of the members of $\mathcal{B}$ have the same size. Let B_{min} be a member of $\mathcal{B}$ with the smallest size and B_3 a member of $\mathcal{B}$ such that among all such possible pairs (B_{min} has the smallest number of elements and B_3 is another member of $\mathcal{B}$ not equal to B_{min}) we have that $|B_{min} \cap B_3|$ is maximal. Since both elements are minimal members of $\mathcal{B}'$ they are not subsets of each other. In particular this means we can choose $x \in B_{min} - B_3$.

We know that $\beta(B_{min} - x) \neq E$ and what is more, by the similar argument as before, there has to be $y \in B_3 - \beta(B_{min} - x)$, since otherwise $B_3 \subset \beta(B_{min} - x)$ which would mean that $E = \beta(B_3) \subset \beta(\beta(B_{min} - x)) = \beta(B_{min} - x)$ which is a contradiction.

So we have that $y \in \beta((B_{min} - x) \cup x) - \beta(B_{min} - x)$ and (CL4) we thus have $x \in \beta((B_{min} - x) \cup y)$ - we exchange x and y.

However, we see two things. First

$$\beta((B_{min} - x) \cup y) \supset \beta(B_{min}) = E$$

so $(B_{min} - x) \cup y \in \mathcal{B}'$ and $|B_{min}| = |(B_{min} - x) \cup y|$ so $(B_{min} - x) \cup y$ is a member of $\mathcal{B}'$ with the smallest possible number of elements.

Second we see that $|((B_{min} - x) \cup y) \cup B_3| = |B_{min} \cup B_3| + 1$ which contradicts the maximality of pair (B_{min}, B_3).

So all the elements of $\mathcal{B}$ have the same size, which in particular implies that $(B_1 - x) \cup y \in \mathcal{B}$ since its β is E what we wanted to show.

The last thing to check is if β is, in fact, the closure operator for the matroid with the basis set $\mathcal{B}$. We first introduce some notation, let $M = (E, \mathcal{I})$ be the matroid we are interested in, meaning the one with the basis set $\mathcal{B}$ and we denote its rank function by r' and its closure operator by cl'. Our goal is to show that for all subsets X we have that $\mathrm{cl}'(X) = \beta(X)$, i.e. the operators coincide.

We know that β and cl' already do coincide on some sets, precisely the ones that contain a basis, for such X we have $\beta(X) = \mathrm{cl}'(X) = E$.

Second thing to note is that β preserves rank, i.e., we always have $\mathrm{r}'(\beta(X)) = \mathrm{r}'(X)$ for all $X \subset E$. We will prove this by contradiction, let $\mathrm{r}'(M) = n$. Suppose there is some subset X with $k = \mathrm{r}'(X) < \mathrm{r}'(\beta(X)) = l$ (applying β to X has to increase the rank because $X \subset \beta(X)$). Then the largest indepenent set L of $\beta(X)$ has the size l. We know L is in some basis B of $\mathcal{B}$, i.e. $L \subset B$. Let us observe the set $X \cup (B - L)$. Its largest independent set has the size at most $k + (n - l) < n$,

because the largest independent set of X has size k and we added $|B - L| = n - l$ elements to it, so we increase it by at most $n - l$. The point is that because $k < l$ we have $k + (n - l) < n$, which in particular means that *there is no basis* in $X \cup (B - L)$ and that its rank is less than n.

But on the other hand, we have

$$L \subset \beta(X) \subset \beta(X \cup (B - L))$$

and

$$B - L \subset \beta(X \cup (B - L))$$

which in particular means that $B \subset \beta(X \cup (B - L)$. Finally, this would mean that $E = \beta(B) \subset \beta(\beta(X \cup (B - L))) = \beta(X \cup (B - L))$ which would imply, by definition of $\mathcal{B}$ that $X \cup (B - L) \in \mathcal{B}$ - which ultimately means it *contains a basis* of our matroid. But we have already established this is not the case so we have come upon a contradiciton. Therefore β preserves rank. The fact that β preserves rank and looking at the definition of the closure operator, namely that it puts in all of the elements which preserve rank we have thus obtained the inclusion $\beta(X) \subset \mathrm{cl}'(X)$ for all subsets X.

Finally, suppose for contradiction that for some X the latter inclusion $\beta(X) \subset \mathrm{cl}'(X)$ is proper and additionally assume that X is a maximal set with this properties (at some point this will have to stop since for $X = E$ the equality $\beta(E) = \mathrm{cl}'(E) = E$ holds.) First, we pick $x \in E - \mathrm{cl}'(X)$ such that $\mathrm{cl}'(X \cup x) - \mathrm{cl}'(X)$ is nonempty (there exists such an x because X does not contain a basis, otherwise, the equality $\beta(X) = \mathrm{cl}'(X) = E$ would hold). Because of the maximality of X we hence know that $\beta(X \cup x) = \mathrm{cl}'(X \cup x)$ holds. Also since the inclusion $\beta(X) \subset \mathrm{cl}'(X)$ is proper, we can pick $r \in \mathrm{cl}'(X) - \beta(X)$. In particular, we then have that $r \in \beta(X \cup x) - \beta(X)$ so by (CL4) we have $x \in \beta(X \cup r)$.

However, this means that $X \cup x \subset \beta(X \cup r)$ and since $X \cup r \subset \mathrm{cl}'(X)$ we have that $\mathrm{r}'(X \cup r) = \mathrm{r}'(X)$. But on the other hand

$$\mathrm{r}'(X) + 1 = \mathrm{r}'(X \cup x) = \mathrm{r}'(\beta(X \cup x)) \leq \mathrm{r}'(\beta(\beta(X \cup r))) = \mathrm{r}'(\beta(X \cup r)) = \mathrm{r}'(X \cup r) = \mathrm{r}'(X)$$

which is a contradiction. So our initial assumption that the inclusion $\beta(X) \subset \mathrm{cl}'(X)$ is proper for some X was false, which implies that $\beta(X) = \mathrm{cl}'(X)$ for all X and we are done.

□

With the definition of closure operator we can three more important family of subsets of a matroid.

Definition 11. *Let $M = (E, \mathcal{I})$ be a matroid with the rank function r closure operator* cl. *We call a subset $X \subset E$ a flat if* $\mathrm{cl}(X) = X$ *holds. We call a subset $H \subset E$ a hyperplane if H is a rank with $r(H) = r(E) - 1$. Finally, we call a subset $S \subset E$ a spanning set if* $\mathrm{cl}(S) = E$.

6 Flats

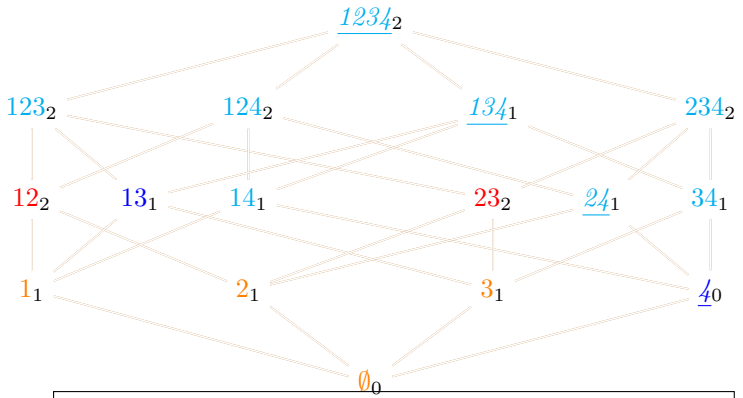
In [3, 35] we have as an excercise an alternative characterization of matroids in terms of their flats. Because we think it is a prototypical model of a statement of the form (a collection of subsets satisfies properties X) if and only if (it is some well known family of matroid subsets), we will show our proof here.

Given a matroid M with a ground set E and its collection of flats, that is all the subsets $X \subset E$ satisfying $\mathrm{cl}(X) = X$, the statement 'abstracts out' which properties of flats *make them flats*. Such statements are a common theme of our article.

Theorem 10. *Let $M = (E, \mathcal{I})$ be a matroid. A collection $\mathcal{F}$ is a collection of flats if and only if the following three conditions hold*

1. *We have $E \in \mathcal{F}$.*
2. *If $F_1, F_2 \in \mathcal{F}$ then $F_1 \cap F_2 \in \mathcal{F}$.*
3. *If $F \in \mathcal{F}$ and $\{F_1, F_2, \cdots, F_k\}$ is a collection of all minimal members of $\mathcal{F}$ properly containing F then $\{F_1 - F, F_2 - F, \cdots, F_k - F\}$ partition $E - F$.*

As an example, we can once again return to our depiction from earlier. This time, we write flats in cursive and with a line below it. As one can see, every superset of a flat has a larger rank. One can see here that the ground set is indeed a flat, and the intersection of, for example *134* and *24*, is indeed another flat, *4*. In this picture, only dependent sets are flats. However, if all supersets one larger than a certain independent set are also independent, then that independent set is a flat. We unfortunately do not have such a situation in this matroid.



Proof. Before we begin the proof, we have two notable observations. First, we see that the characterization of our collection $\mathcal{F}$ follows a similar pattern as characterization of other encountered

collections such as $\mathcal{I}$ or $\mathcal{C}$. Specifically, we mean that we have two initializing properties, for example, the collection is non-empty, has $\emptyset$ or E, is downard closed, closed under intersections, inclusions... Followed by the third property which really tells us something non-trivial about how the sets of the collection interect with each other. Second, as with the previous proofs, we will see that it is not hard to prove the only if direction, i.e. knowing we have a collection of flats and proceeding further. However, we will require some clever ideas to prove the reverse direction.

So first suppose $\mathcal{F}$ is a collection of flats and our goal is to prove that the three properties hold.

1. We see that $E \subset \text{cl}(E)$ by the definition of the closure operator and $\text{cl}(E) \subset E$ because cl maps from 2^E into E. Thus $\text{cl}(E) = E$ implying E is a flat as desired.

2. Again, inclusion $F_1 \cap F_2 \subset \text{cl}(F_1 \cap F_2)$ is a fundemental property of closure operator (CL1). Because $F_1 \cap F_2 \subset F_1$ we have by (CL2) that $\text{cl}(F_1 \cap F_2) \subset \text{cl}(F_1) = F_1$ where the last equality follows by assumption that F_2 is a flat. Similarly $\text{cl}(F_1 \cap F_2) \subset F_2$, which implies $\text{cl}(F_1 \cap F_2)$ is contained in F_1 and F_2, in other words $\text{cl}(F_1 \cap F_2) \subset F_1 \cap F_2$. To conclude $F_1 \cap F_2 \subset \text{cl}(F_1 \subset F_2) \subset F_1 \cap F_2$ which implies $\text{cl}(F_1 \cap F_2) = F_1 \cap F_2$, and then by definition $F_1 \cap F_2 \in \mathcal{F}$ thus the second property is satisfied.

3. We pick a flat F and let $P = \{F_1, F_2, \cdots, F_k\}$ be the collection of all flats properly containing F. To show that P partitions $E - F$ we have to show two things; for any $i \neq j$ we must have $(F_i - F) \cap (F_j - F) = \emptyset$ and $\cup_k (F_k - F) = E - F$.

   The second property is evident, namely if we pick any $x \in E - F$ then there exists a flat containing $F \cup x$, in particular E will do. So there exists a minimal (not properply containing other with such properties) flat containing $F \cup x$, let us call it G and obviously, $G = \text{cl}(F \cup x)$. We would like G to also be a minimal flat properly containing F. If it is not there is some flat H such that $F \subset H \subset G$ where both inclusions are proper. By assumption H does not include x otherwise it would contradict the minimality of G. But there also has to be some $y \in H - F$. In particular, since all things involved are flats, we have that $y \in \text{cl}(F \cup x) - \text{cl}(F)$ so by (CL4) we have $x \in \text{cl}(F \cup y)$ which is a contradiction since $\text{cl}(F \cup y)$ is a flat which contains F and y so it is H. Therefore G is a minimal flat and we are done.

   The first property can be derived by contradiction. Namely, if for some $i \neq j$ we have that there exists $e \in (F_i - F) \cup (F_j - F)$ then we have that the intersection $F_i \cup F_j$ is a flat which contains $F \cup e$, but is also properly contained inside F_j and F_i - a contradiction.

   So we also have the last property.

Now for the if direction. In the previous proofs of proving the reverse direction of such statements we could directly relate the independent sets, which we consider to be our most elementary definition, to our objects. For example if you know your collection has to be the collection of circuits, then the independent sets are precisely all of the proper subsets of circuits. If you know your collection has to be a collection of bases, then the independent sets have to be all of their subsets. When proving

the equivalence of the rank function, the independent sets were precisely the sets with the propery $r(X) = |X|$.

However, with flats, there is no way (at least not as clear as with previous examples) to relate flats with independent sets. So we will prove the reverse direction by relating it to one definition we already know. So we have to prove that f satisfies the properties (CL1) - (CL4).

Suppose we are given a finite set E and collection $\mathcal{F}$ of its subsets satisfying properies 1., 2. and 3. Then let us define a *function* $f : 2^E \to \mathcal{F}$ by the rule that for any X, we have $f(X)$ is the minimal member of $\mathcal{F}$ containing X. Its clear what is our aim, namely to show that this is in fact a closure operator, then we will do two things at once - E will be a matroid with a closure operator f and the elements of $\mathcal{F}$ will be precisely the flats.

First we have to check f is well-defined. By the first property of $\mathcal{F}$ we have that $E \in \mathcal{F}$ and because for any subset $X \subset E$ we have $X \subset E$ we have that for every subset X there *exists* some element of $\mathcal{F}$ such that X is a subset of it (in the worst case it is E). Now, the minimal such subset has to be unique, since if F_1, F_2 have the same property that they are minimal members of $\mathcal{F}$ including X then by the second property of $\mathcal{F}$ we have that $F_1 \cap F_2 \in \mathcal{F}$ and so $X \subset F_1 \cap F_2$, so if they are not the same we are contradicting minimality of them. $F_1 \subset F_2$ and $F_2 \subset F_1$ hold so $F_1 = F_2$.

Now we check the closure axioms.

1. If $X \subset E$ then by definition, $f(X)$ is an element of $\mathcal{F}$ *containing* X so we have $X \subset f(X)$ and the first property follows.

2. If $X \subset Y \subset E$ then $f(X)$ is the minimal member of $\mathcal{F}$ containing X. Because $f(Y)$ is a minimal member of $\mathcal{F}$ which contains Y it thus also contains X so by minimality of $f(X)$ we have $f(X) \subset f(Y)$ as desired.

3. If $X \subset E$ is arbitrary then we have that $f(f(X))$ is the minimal member of $\mathcal{F}$ containing $f(X)$, but $f(X)$ is by defintion itself in $\mathcal{F}$ and it contains $f(X)$. So we have that $f(X) \subset f(f(X)) \subset f(X)$ implying $f(f(X)) = f(X)$.

4. Up to this point we have not yet used the second and the third property of $\mathcal{F}$ so we better require them now. rephrase:

   Suppose $X \subset E$, $x \in E$ and $y \in f(X \cup x) - f(X)$. In particular, this means that $y \notin X$. Our goal is to show $x \in f(X \cup y)$. Let us call $f(X) = F_1$, $f(X \cup x) = F_2$ and $f(X \cup y) = F_3$ to remind us that output of f is always a member of $\mathcal{F}$. By the second property of "closure operator" we have already proved, we have $F_1 \subset F_2$ and $F_1 \subset F_3$. Not just that, F_2 and F_3 are in fact one of the minimal elements of $\mathcal{F}$ properly containing F_1.

   We know this, because by the third property of $\mathcal{F}$, all of the minimal elements of $\mathcal{F}$ containing F_1 *partition* $E - F_1$, so in particular, there is some $F_2' \in \mathcal{F}$ which contains $X \cup x$ and contains X minimaly and some $F_3' \in \mathcal{F}$ which contains $X \cup y$ and contains X minimally. So from

"Note that [...]" or "An observant reader might notice that..."

$X \cup x \subset F_2' \in \mathcal{F}$ we directly infer $F_2 \subset F_2'$ because $f(X \cup x)$ is an element of $\mathcal{F}$ which contains $X \cup x$ minimally. It is now clear that $F_2 = F_2'$ and $F_3 = F_3'$.

We are almost done. By the third property of $\mathcal{F}$, because F_2 and F_3 are minimal members of $\mathcal{F}$ properly containing X we have that $(F_2 - F_1) \cap (F_3 - F_1)$ is either empty or $F_2 = F_3$. It cannot be empty because, $y \in F_3 - F_1$ by definition and $y \in f(X \cup x) - f(X) = F_2 - F_1$ by assumption. So $F_2 = F_3$ which implies that $x \in F_3 = f(X \cup y)$. This shows the last closure axiom, and in particular, we know that we have a matroid with ground set E and closure operator f.

Finally, it is clear by defnition that the collection of all subsets of X such that $f(X) = X$ is precisely $\mathcal{F}$, so $\mathcal{F}$ is our collection of flats for this matroid.

. We conclud that

□

New page

7 Algebraic matroids

An interesting concept of independence arises in the study of field theory. We will present an interesting class of matroids derived from the concept of algebraic independence. For the rest of this section we will use the notation $\mathbb{K}/\mathbb{F}$ to refer to some field $\mathbb{K}$ and a subfield $\mathbb{F}$. define (sub) field in an appendix?

This is covered in 2B of year 2. If it's easy to check, write it out.

Example 7.1. For example, we might look at $\mathbb{F} = \mathbb{Q}$ and $\mathbb{K} = \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$. Then it is easy to check that $\mathbb{Q}(\sqrt{3})$ is indeed a field containing $\mathbb{Q}$ as a subfield.

Definition 12. *A subset $S = \{s_1 \dots s_n\} \subseteq \mathbb{K}/\mathbb{F}$ is said to be algebraically independent (over $\mathbb{F}$) if there does not exist any nonzero multivariable polynomial in n variables $f \in \mathbb{F}[X_1 \dots X_n]$, with coefficients in $\mathbb{F}$, such that the evaluation homomorphism $\mathrm{ev}_{(s_1, s_2, \cdots, s_n)}(f) = 0$.*

Intuitively, the definition says that if we just multiply and add the elements of S and multiplying them with elements of $\mathbb{K}$ we will never get 0. fix sentence p?

We know that an element $x \in \mathbb{R}$ is called transcendental with respect to $\mathbb{Q}$ if for nonzero polynomials with rational coefficients $\mathrm{ev}_x(p) \neq 0$. That means that any nontrivial polynomial evaluated at x will never give 0. Comparing with the definition of algebraically independent sets above, we see that a singleton x is algebraically independent by our defintion, if for any nonzero single variable ($n = 1$) polynomial p with coefficients in $\mathbb{Q}$ we will have that $\mathrm{ev}_x(p) \neq 0$. This is precisely the definition of transcendental numbers.

define

Although it is well known that the complex numbers e and π are transcendental over $\mathbb{Q}$, it hasn't yet been proven that $\{e, \pi\}$ is algebraically independent. This is not well-known to you

We will now discuss the notion of algebraic dependence.

Definition 13. *Let $a \in \mathbb{K}/\mathbb{F}$ and $B = \{b_1, \dots, b_n\} \subseteq \mathbb{K}/\mathbb{F}$. We say that a is algebraically dependent on B (over $\mathbb{F}$) if a is algebraic over $\mathbb{F}(b_1, \dots, b_n)$. Given some $A \subseteq \mathbb{K}/\mathbb{F}$, we say that A is algebraically dependent on B (over $\mathbb{F}$) if every element of A if algebraic on B (over $\mathbb{F}$).*

Before continuing onto the next lemma, we remind the reader that a field $\mathbb{K}$ has a natural $\mathbb{K}$-vector space structure, thus scalars are elements of $\mathbb{F}$ and vectors being elements of $\mathbb{K}$. Moreover, the vector space induced by $\mathbb{F}(a)$ over $\mathbb{F}$ when a is algebraic over $\mathbb{F}$ is finite dimensional.

Lemma 2. *Consider $a, b \in \mathbb{K}/\mathbb{F}$ such that a is algebraic over $\mathbb{F}(b)$ and b is algebraic over $\mathbb{F}$. It then follows that a is algebraic over $\mathbb{F}$.*

Proof. The vector spaces induced by $\mathbb{F}(b)$ and $\mathbb{F}(b)(a)$ must both be finite dimenssional over $\mathbb{F}$ and $\mathbb{F}(b)$ respectively (because b is algebraic over $\mathbb{F}$ and a is algebraic over $\mathbb{F}(b)$ respectively). It follows that $\mathbb{F}(b)(a)$ is finitely dimenssional over $\mathbb{F}$ (this can easily be seen by noticing that given a basis a_i for $\mathbb{F}(b)(a)$ over $\mathbb{F}(b)$ and a basis b_i for $\mathbb{F}(b)$ over $\mathbb{F}$, we can form a basis $a_i b_j$ for $\mathbb{F}(b)(a)$ over $\mathbb{F}$).

Let n be the dimenssion of $\mathbb{F}(b)(a)$ over $\mathbb{F}$. Let $S = \{a^0 \dots a^n\}$. Because $|S| = n + 1$, S cannot be linearly independent (in the vector space induced by $\mathbb{F}(b)(a)$ over $\mathbb{F}$), which means a polynomial $f \in \mathbb{F}[x]$ exists such that $f(a) = 0$. □

Lemma 3. *Consider $A, B, C \subseteq \mathbb{K}/\mathbb{F}$ such that A is algebraically dependent on B and B is algebraically dependent on C. It then follows that A is algebraically dependent on C.*

Proof. We will proceed by induction on the size of B:

1. If $|B| = 1$ then the result trivially follows from lemma (2).
2. Assume the result is true for $|B| = n$. We will attempt to prove it for $|B| = n + 1$. Let $a \in A$. We have to show that a is algebraic over $\mathbb{F}(c_1 \dots c_k)$. Given $1 \leq i \leq n$, each b_i is algebraic over $\mathbb{F}(c_1 \dots c_k)$ (because B is algebraically dependent on C (over $\mathbb{F}$)). It then follows that each such b_i is also algebraic over $\mathbb{F}(c_1 \dots c_k, b_{n+1}) = \mathbb{F}(b_{n+1})(c_1 \dots c_k)$. Moreover, we know that a is algebraic over $\mathbb{F}(b_1 \dots b_{n+1})$, which means it is also algebraic over $\mathbb{F}(b_{n+1})(b_1 \dots b_n)$. It then follows from the induction hypothesis (applied with $\mathbb{F}(b_{n+1})$ as the base field, $A = \{a\}$, $B = \{b_1 \dots b_n\}$ and the same C) that a is algebraic over $\mathbb{F}(b_{n+1})(c_1 \dots c_k) = \mathbb{F}(c_1 \dots c_k)(b_{n+1})$.

   We recall that b_{n+1} is algebraic on $\mathbb{F}(c_1 \dots c_k)$ (because B is algebraically dependent on C (over $\mathbb{F}$)). We can now apply lemma (2) to prove that a is algebraic over $\mathbb{F}(c_1 \dots c_n)$.

□

Theorem 11. *Given a finite subset $E \subseteq \mathbb{K}/\mathbb{F}$, the pair $(E, \mathcal{I})$ where $\mathcal{I}$ is the set of algebraically independent subsets of E forms a matroid.*

Although [3] offers a proof based on independent sets and the concept of algebraic dependence, we will instead present a proof based on the basis of our supposed matroid. The part focused on proving the exchange lemma is inspired by [2], although the rest will be a lot more simple (no need to involve Zorn's lemma) because we are working in a finite subset.

We start by proving the following lemma:

Lemma 4. *Consider finite $A, B \subseteq \mathbb{K}/\mathbb{F}$, such that A is independent over $\mathbb{F}$ and dependent on B (over $\mathbb{F}$). Then $|B| \geq |A|$.*

Proof. We will prove the statement by induction on the number of elements in $A \setminus B$:

Induction again

1. If $A \setminus B = \varnothing$ then $A \subseteq B$ and $|A| \leq |B|$ follows trivially.
2. Assume the statemenet is true for some $|A \setminus B| = |A| - (k+1)$ (where $k = |A \cap B)$. We will attempt to prove it for $|A \setminus B| = |A| - k$. Let $a_1 \dots a_n$ be the elements of A such that $a_1 \dots a_k$ are all the members of $A \cap B$ for some k. Let $a_1 \dots a_k, b_{k+1} \dots b_m$ be the elements of B. It remains to prove that $m \geq n$.

   As a_{k+1} is not dependent on $\{a_1 \dots a_k\}$ but is dependent on $B = \{a_1 \dots a_k, b_{k+1} \dots b_m\}$, there must exist some $k+1 \leq j \leq m$ such that a_{k+1} is dependent on $\{a_1 \dots a_k, b_{k+1} \dots b_j\}$ but not on $\{a_1 \dots a_k, b_{k+1} \dots b_{j-1}\}$. Because a_{k+1} is dependent on $\{a_1 \dots a_k, b_{k+1} \dots b_j\}$, we know there exists some polynomial $f \in \mathbb{F}[x_1 \dots x_{j+1}]$ such that

   $$f(a_1 \dots a_k, b_{k+1} \dots b_j, X) \neq 0 \wedge f(a_1 \dots a_k, b_{k+1} \dots b_j, a_{k+1}) = 0.$$

   We can write f as

   $$f(x_1 \dots x_{j+1}) = \sum_i f_i(x_1 \dots x_{j-1}, x_{j+1}) x_j^i.$$

   We know that $f(a_1 \dots a_k, b_{k+1} \dots b_j, X) \neq 0$, therefore at least one of $f_i \neq 0$. Let $g = f_i$ such that $f_i \neq 0$. Because a_{j+1} is not algebraic over $\{a_1 \dots a_k, b_{k+1} \dots b_{j-1}\}$, we know that

   $$g(a_1 \dots a_k, b_{k+1} \dots b_{j-1}, a_{k+1}) \neq 0.$$

   This implies that $f(a_1 \dots a_k, b_{k+1} \dots b_{j-1}, X, a_{k+1}) \neq 0$. Since $f(a_1 \dots a_k, b_{k+1} \dots b_j, a_{k+1}) = 0$, we can conclude that b_j is algebraic over $\{a_1 \dots a_{k+1}, b_{k+2} \dots b_j\}$.

   Construct $B' = B + a_{k+1} - b_j$. Having proven that b_j is dependent on a subset of B', it is also dependent on B'. All other elements of B are also dependent on B' (because any variable is algebraic over a field extension it generates, i.e. t is algebraic over $\mathbb{F}(t)$). We recall that A is dependent on B, so by the transitivity of algebraic dependence (lemma (3)), we know that A is algebraic over B'. We also notice that A and B' have $k+1$ elements in common, therefore the statement is proven by the induction hypothesis.

bases?

□

We will now show that all basis in our supposed matroid have equal cardinality.

Lemma 5. *Given some finite subset $E \subseteq \mathbb{K}/\mathbb{F}$, maximal independent subsets of E (in the partially ordered set induced by inclusion) have equal cardinality.*

Proof. Let A and B be maximal independent subsets of E. If both sets are $\varnothing$, then our proof is done. If one set is $\varnothing$ and one isn't, we clearly have a contradiction, as $\varnothing$ is a strict subset of the other set, hence not maximal. We therefore assume the existence of some $a \in A$ and $b \in B$.

We know that A is maximal, therefore any $b \in B$ is algebraically dependent on A. We can therefore conclude that B is algebraically dependent over B. We recall that B is also independent, which means we can use lemma (4) to prove that $|A| \geq |B|$. We can apply a similar argument to show that $|B| \geq |A|$, which together with our previous statement shows that $|A| = |B|$, proving the lemma. □

Proof of theorem (11). We will construct the matroid using the basis definition. We need to first show that at least one exists, and then show that the exchange property holds.

We consider the partially ordered set of independent subsets of E ordered by inclusion. We notice that $\varnothing$ is independent (as the only polynomial of 0 variables which can be satisfied by $\varnothing$ is the trivial polynomial). Any finite nonempty partially ordered set has at least one maximal element, so a basis exists.

It now remains to prove the exchange property. That is, given two basis $A, B \subseteq \mathcal{B}$ and some $a \in A \setminus B$, we can find some $b \in B \setminus A$ such that $B - b + a \in \mathcal{B}$. Let $n = |A| = |B|$ (we know the two basis have equal cardinality from lemma (5)). Assume the statement is not true. That is, all $b_i \in B$ are dependent on $A - a$, which means B is dependent on $A - a$. It follows from lemma (4) that $|B| \leq |A - a|$, which is equivalent to $n \leq n - 1$, hence a contradiction. □

8 Dual Matroids

The concept of *duality* is an interesting feature of matroid theory. It helps to extend some of the constructions in our prototypical examples in representable and graphic matroids, such as the notion of orthogonality in vector spaces and the concept of a planar dual of a plane graph, to general matroids. In this section we will introduce the definitions and properties of dual matroids.

If we have a matroid M, with sets (E, B), or in other words M is a matroid on E with B as its collection of bases. Then its dual will refer to a different and new matroid, which we denote by $M*$. This new matroid has the property that it is "related" to the original matroid, so it has the same ground set E of the original matroid M, but a different basis set, this new basis collection will be called $B*$, so this gives us that $M*$ will be defined by the following pair of sets $(E, B*)$. Where B^* will a set such that is is the complement of the bases set B in M, which implies that, the bases set of M and M^* will be always disjoint.

This can be seen more clearly in the following digram:

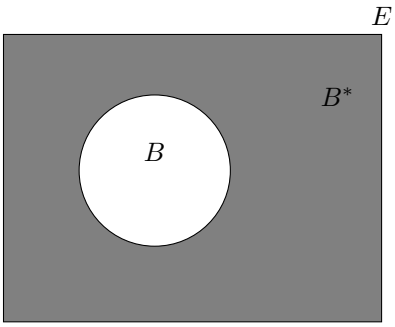
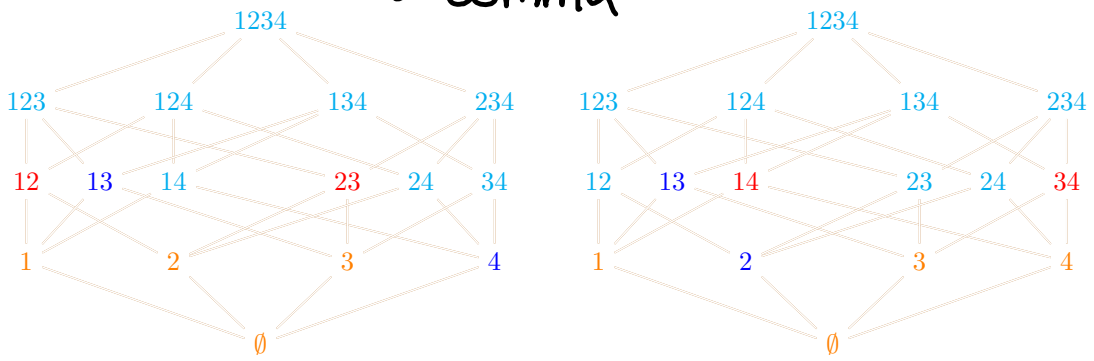


Figure 7: Venn diagram showing, B the basis set of M, and B^* the basis set of M^*

We also have the depiction from previous sections, but know we will also the one that will correspond to the dual on this specific case. To the **left** we have the depiction corresponding to the **original matroid**, and to the **rigth** we have the one corresponding to its **dual matroid**. Notice how the ground set will be composed of 4 components $E = \{1, 2, 3, 4\}$, and in the original matroid has bases 12 and 23, in red. So, its dual has bases 34 and 14, respectively, also in red but in the rigth-side diagram. This is because the complement of the elements 12 is 34, and the complement of 23 is 14.



Independent set, Basis, Circuit, Dependent set

We know that the basis set of a matroid is obtained from its set of independet sets I. Using this diagrams we highligth an idea that will be useful later in this chapter. This is, that the basis set of a matroid is given by a subset of E, the remaing elements in E that are not in de basis if added to the basis will be linearly dependent, but also we can take any remaining element of E and exchange it with an element in the basis and we will have another basis for E. With this intuition in mind, we can continue with a theorem.

To formalize the definition of B^* we have the following:

Theorem 12. *Let M be a matroid given by (E, B), and $B^*(M)$ be $\{E(M) - B : B \in B(M)\}$. Then $B^*(M)$ is the set of bases of a matroid on $E(M)$*

Or in other words, B* is the set of all the complement independent bases of B. Then we can give the following definition.

Definition 14. *Let M be a matroid with the pair (E,B), given B* as defined above, the new matroid M*=(E,B*) is the dual of M.*

In the theorem we say that B*(M) is the set of bases of a matroid on $E(M)$, but this is not be trivially clear, so we need to prove it.

However to prove it we will make use of the following result, that comes from our properties of the basis set B of our matroid M in Section 2.2

Lemma. The set B of bases of a matroid M has the following property: $(B2)^*$ If B_1 and B_2 are in B and $x \in B_2 - B_1$,then there is exist and element y of $B_1 - B_2$ such that $(B_1 - y) \cup x \in B$

For comparison this was the original (B2):

$(B2)$ *If* $B_1, B_2 \in \mathcal{B}$ *and* $x \in B_1 - B_2$*, then there exists a* $y \in B_2 - B_1$ *such that* $(B_1 - x) \cup y \in \mathcal{B}$.

First we will prove $(B2)^*$:

Proof. We note that B_1 is by definition a base, this means that if we add a new element in the ground set to it, it will become a minimal dependet set, in other words $B_1 \cup x$ contains a unique circuit $C_1 \in C$. Since we have C_1 a dependent set and B_2 another base, and thus independet, then $C_1 - B_2$ will be non-empty, there exists and element y such that $y \in C_1 - B_2$, but as C_1 is the circuit created from $B_1 \cup x$, then $y \in (B_1 \cup x) - B_2$, but as $x \neq y$, then $y \in B_1 - B_2$. Now, lets take $B_1 - y$, this will not be a basis, but it will be an independent set, if now we take $(B_1 - y) \cup x$, this will clearly not contain the circuit C_1, since this was the unique circuit generated from $B_1 \cup x$, the set $(B_1 - y) \cup x$ must be independent. Finally, we observe that $(B_1 - y) \cup x$ implies that we add and elemnts to the set and we take out one element to the set, so the cardinality will remain equal, that is: $|(B_1 - y) \cup x| = |B_1|$. As we have that $(B_1 - y) \cup x$ is and independent set and has the same cardinality as the the base B_1, then, by definition, $(B_1 - y) \cup x$ is also a base. □

Now, we prove that $B^*(M)$ is the set of a base of a matroid on $E(M)$.

Proof. As $B(M)$ is non-empty, $B^*(M)$ is non-empty, hence, the property (B_1) holds for $B^*(M)$. Now, consider two members of $B^*(M)$, B_1^* and B_2^*, not equal such that there exists an element $x \in (B_1^* - B_2^*)$. Let, $B_1 = E - B_1^*$ and $B_2 = E - B_2^*$. We can see that $B_1^* - B_2^* = B_2 - B_1$, thus $x \in B_2 - B_1$. By $(B2)^*$, there exists and element $y \in B_1 - B_2$ such that $(B_1 - y) \cup x$ is a base of M, but observe that $B_1 - B_2 = B_2^* - B_1^*$, hence this is the same as saying that there exists and element $y \in B_2^* - B_1^*$ such that $(B_1 - y) \cup x$ is a base of M. Hence, by definition of dual, $E - ((B_1 - y) \cup x) \in B^*(M)$. But, $E - ((B_1 - y) \cup x) = ((E - B_1) - x) \cup y) = (B_1^* - x) \cup y$, which is in the family B^*. Thus, $B^*(M)$ satisfes $(B2)$. As $B^*(M)$ satisfies properties $(B1)$ and $(B2)$, this is indeed the set of bases of a matroid on E. □

no comma

The matroid M*, is the dual of M. Note that by the way is defined, and thanks to the proof above we see that $B(M^*) = B^*(M)$, moreover, due the nature that the definition of dual has, this is, that is the complement of the basis set, we have that

- *The dual of the dual of a matroid M is the matroid M itself, i.e.,* $(M^*)^* = M$

This is because if we take the complement B^* of the basis set B, and then we take this complement B^* and take its complement once again, we will return to the original set B, or in other words: If $E - (E - B) = B$.

Completely different Style!

As an example, let $U_{k,n}$, be a k-uniform matroid. We know that its bases will be all the k-element subsets of $E(U_{k,n})$. We know that this matroid is defined over a set of n elements, and its basis has exactly k elements, hence the bases of $U_{k,n}{}^*$ are be all $(n-k) - element$ subsets of the ground set, as this will be the complement of the basis set of $U_{k,n}$. This is equal to saying that the dual of the matroid $U_{k,n}$ is given by $U_{k,n}{}^* = U_{n-k,n}$

Make shorter sentences

Now that we have introduced duals is useful to give some additional notation. That is, given a matroid M with a dual M^*, the *bases* of the matroid M^* are called *cobases* of M. Similarly, the *independent sets* of M^* are called *coindependent sets* of M, the circuits of M^* are called *cocircuits* of M, *hyperplanes* are called *cohyperplanes*, and the *spanning sets* are called *cospanning sets* of M and so on.

This leads us to some elemenary relationships between these sets.

Proposition : Let M be a matroid in a set E and suppose $X \subseteq E$. Then,

1. X is independent if and only if $E - X$ is cospanning.
2. X is spanning if and only if $E - X$ is coindependent.
3. X is a hyperplane if and only if $E - X$ is a cocircuit
4. X is a circuit if and only if $E - X$ is a cohyperplane.

? . Fix Layout

??? .

Proof. All of the proofs follow directly from the definitions. [We will prove a) and b)]

a) Suppose X is independent. This means there exists a basis $B \in \mathcal{B}(M)$ so that $X \subset B$. Because $X \subset B \subset E$ and the operation of taking complements is "inclusion reversing" we have $E - B \subset E - X$. Verifying directly, if $x \in E - B$ this means $x \in E$ and $x \notin B$. Because $X \subset B$ this implies that $x \in E$ and $x \notin X$ so by definition $x \in E - X$ and the conclusion follows. Because $E - B$ is a cobasis and $E - X$ is a set containing a cobasis, then it is a cospanning by definion.

Similarly if $E - X$ is cospanning then it contains a cobasis which is by definition of the form $E - B$ for some $B \in \mathcal{B}(M)$. By the analagous reasoning as for the forward direction $E - B \subset E - X$ implies $X \subset B$. That is because if $x \in X$ then $x \notin E - X$ and $x \notin X - B$. This means $x \in B$ concluding $X \in B$. Since B is an independent set then X is independent set as well, we are done.

?

b) Same as a). A set $X \subset E$ being spanning implies it contains a $B \in \mathcal{B}(M)$. So BX which implies $E-X \subset E-B$. Because $E-B$ is cobasis by definition, any of its subsets are coindependent.

If $E - X$ is coindependent, it is contained in a cobasis, so by definition there exists a $B \in \mathcal{B}$ so that $E - X \subset E - B$. As before this implies that $B \subset X$ and X is spanning.

c) If X is a hyperplane, then X is not spanning but for all $y \in E - X$ we have $X \cup y$ is spanning, which means there is for every such y a basis $B_y \in \mathcal{B}$ so that $B_y \subset X \cup y$. By b) we know that X is not spanning implies $E - X$ is not coindependent. But for any $z \in E - X$ we have $(E - X) - z = E - (X \cup z)$ is coindependent because $X \cup z$ is spanning. So $E - X$ is a cocircuit by definition.

Conversly, if $E - X$ is a cocirucuit, then $E - X$ is not coindependent but for all $x \in E - X$ we have $(E - X) - x = E - (X \cup x)$ is coindependent. By b) this means that X is not spanning but for all $x \in E - X$, we have $X \cup x$ is spanning, so X is a hyperplane.

d) Same as things before. □

Similar to the case with the bases and cobases, the rank function of the dual matroid is usually denoted by r^*, and is normally referred as the *corank function* of M. Using the definition of bases of the dual matroid, this is, that is build with the complement bases of the set of the orginal matroid, as well as the fact that matroid and its dual are both on the same ground set, we have the following:

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

And in fact, we can generalize this to obtain an explicit formula for the for the corank function of the matroid.

For all subsets X of the ground set E of a Matroid M,

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

Proof. Let I^* be a independet subset of X in M^*, such that it is not a subset of some other set in X, this is $r^*(X) = |I^*|$. Similarly, let I be a independent subset of $E - X$ in M, such that it is not a subset of some other set in $E - X$, this is $r(E - X) = |I|$. And let B be an independent subset of $E - I^*$, such that it is not a subset of some other set in $E - I^*$ and contains I. Since, this are independent subsets that are not subsets of any other element in their respective sets, then we have $r(B) = r(E - I^*)$ and $r(E - I^*) = r(M)$, and hence B is a base of M. Now, let $B^* = E - B$, since B is a base of M, by definition B is a base of M^*. We can onserve that $I^* \subseteq B^*$ and $B^* \cap X = I^*$. Similarly, $I \subseteq B$ and $B \cap (E - X) = I$. In particular we see that, $|B \cap X| = |B| - |I|$, thus $|X| = |X \cap B| + |X \cap B^*| = |B| - |I| + |I^*| = r(M) - r(E - X) + r^*(X)$ □

Now we will talk about duals of representble matroids. Let A be an $m \times n$ matrix over the field F, and let M be vector matroid $M[A]$ of A. Then we have that the groud set of M is the set E of column labels of A. Note that, in general, $M[A]$ does note uniquely determine A. Furthermore, M remains unchanged if we perform any of the following operarations on A, which include the *elementary row operations* ~~seen in the linear algebra courses~~.

1. Interchange two rows.
2. Multiply a row by a non-zero member of $\mathbb{F}$.
3. Replace a row by the sumof that row with another row.
4. Adjoin or remove a zero row.
5. Interchanging two columns (the labels moving with the columns).
6. Multiply a column by a non-zero member of $\mathbb{F}$.

The reason for this is because when constructiong the matroid M form a matrix A, we only care about the independence (or dependence) that each column vector in the matrix has with one another. So, as long as the independence and dependece between this is keep the same, the values inside the columns are not relevant.

Assume that the matrix A is non-zero. It is known that by using the operations previusly mentioned A can be reduced to be of the form $[I_r|D]$, where I_r is the $r \times r$ identity matrix and D is some $r \times (n-r)$ matrix over F. We can clearly see that $r(M) = r$ (the dimension fo the identity matrix).

Suppose that the columns of $[I_r|D]$ are labelled, in order, in the following form, $e_1, e_2, ..., e_n$. This will be the ground set $E = \{e_1, e_2, ..., e_n\}$. Then, we see that $\{e_1, e_2, ..., e_r\}$ is a basis B of M, once agina due to the dimesion of the identity matrix. We also label both, the rows and colums of D, in the following form, for the rows from top to bottom, $e_1, e_2, ..., e_r$ and for the columns, $e_{r+1}, e_{r+2}, ..., e_n$. This way to represent $M[A]$ can be seen more clearly in the following figure. We will refer to both $[I_r|D]$ and D as the *standard representative matrices* for M, *with respect to* $\{e_1, e_2, ..., e_r\}$. Similarly, we use *reduced standard representative matrix* if we want to refer only to D.

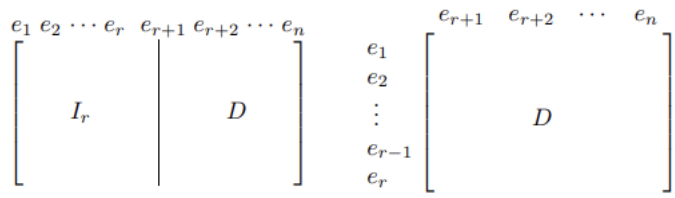


Figure 8: Standard representative matrices for M. [3]

Note that, ~~in the figure,~~ in $[I_r|D]$ only the columns are labelled, but in D, both the rows and columns ae labeled.

We can now use this construction to determine the dual of a vector matroid using the following theorem.

Theorem 13. *Let M be the vector matroid of the matrix $[I_r|D]$ where the columns of this matrix are labelled, in order, $e_1, e_2, ..., e_n$ and $1 \leq r < n$. Then M^* is the vector matroid of $[-D^T|I_{n-r}]$ where its columns are also labelled $e_1, e_2, ..., e_n$ in that order.*

Proof. We assume that $[I_r|D]$ is as in the contruction of the theorem above. Then $[-D^T|I_{n-r}]$ is as follows

$$\begin{array}{c} e_1 \;\; e_2 \cdots e_r \;\; e_{r+1} \; e_{r+2} \cdots e_n \\ \left[\begin{array}{c|c} -D^T & I_{n-r} \end{array}\right] \end{array}$$

Let B be a basis of M. We need to show that $E-B$ is a basis of the vector matroid of $[-D^T|I_{n-r}]$. We can rearrege the columns of $[-D^T|I_{n-r}]$, such that $B = \{e_1, \ldots, e_s, e_{r+1}, \ldots, e_{r+(r-s)}\}$, for some $s \leq r$. This is possible becasue we know that it does not affect the corresponding matroid, so the only change it bring to rearrange rows and columns of $[I_r|D]$ is the re-arrenge of columns and rows of $[-D^T|I_{n-r}]$.

Using this we can partition $[I_r|D]$ and $[-D^T|I_{n-r}]$ in the following form

$$\begin{bmatrix} I_s & 0 & D_{11} & D_{12} \\ 0 & I_{r-s} & D_{21} & D_{22} \end{bmatrix} \rightarrow \begin{bmatrix} -D_{11}^T & -D_{21}^T & I_{r-s} & 0 \\ -D_{12}^T & -D_{22}^T & 0 & I_{n-(2r-s)} \end{bmatrix}$$

First, lets analyse the partition of $[I_r|D]$. Here me made the partition such that the first component I_s has columns from $(e_1 \ldots e_s)$. I_{r-s} has columns from $(e_{s+1} \ldots e_r)$, D_11 and D_21 have from $(e_{r+1} \ldots e_{2r-s})$, and finally D_12 and D_22 have from $(e_{(2r-s)+1} \ldots e_n)$.

We have that B is a base, this means that it must have the same size as I_r. Due to the way the matrix $[I_r|D]$ is partitioned, if the we take the components in the partirtion that contain the columns components in the basis, we have the following matrix:

$$\begin{bmatrix} I_s & D_{11} \\ 0 & D_{21} \end{bmatrix}$$

As this matrix has the components that contain all the elements in the basis implies that it must have $rank = r$ (the rank of $[I_r|D]$), but here I_s has $rank = s$, as it is the identity matrix. Hence, the the rank of D_{21} is $r - s$, which also corresponds to the rank of $-D_21^T$.

If we now observe the partition of $[-D^T|I_{n-r}]$, this will gave the same partition lengths in each component as the ones mentioned for $[I_r|D]$ above. That is, the first component $-D_{11}^T$ and $-D_{12}^T$

have columns from $(e_1 \dots e_s)$. $-D_{22}^T$ and $-D_{21}^T$ have columns from $(e_{s+1} \dots e_r)$, I_{r-s} has from $(e_{r+1} \dots e_{2r-s})$, and finally $I_{n-(2r-s)}$ has from $(e_{(2r-s)+1} \dots e_n)$. As this time we ar dealing with the dual we make a change, we take in this case the components in the partirtion of $[-D^T|I_{n-r}]$ that contain the complement of the elements in teh basis and we have the ~~following matrix~~ matrix below.

$$\begin{bmatrix} -D_{21}^T & 0 \\ -D_{22}^T & I_{n-(2r-s)} \end{bmatrix}$$

The rank of this submatrix is the sum of the ranks of $I_{n-(2r-s)}$ and $-D_{21}^T$, previously we stated that the rank of $-D_{21}^T$ is the same as the one of D_{21}, that is $rank = r - s$, and the rank of $I_{n-(2r-s)}$ is clearly $rank = n-(2r-s)$, so the total rank is $(r-s)+(n-(2r-s)) = r-s+n-2r+s = n-r$. This imples that $E - B$ is a basis of the vector matroid of $[-D^T|I_{n-r}]$, since $|E| = n$ and $|B| = r$ this corresponds to the definition of dual, whose basis B^* must have $|B^*| = n - r$, which holds in this case. This argument could be easily extended to show that every basis of the matroid appears in this way. Therefore $[-D^T|I_{n-r}]$ is indeed a representation of M^*. □

By convention the form $[D^T|I_{nr}]$ instead of $[D^T|I_{nr}]$. However it is important to remark that this does not bring any problem, because, as we previusly stated, the use of *elementary row operations* does not affect the matroid of a matrix.

From the previous theorem a remarkable result follows almost directly. (prove it?)

- **Corollary 1. :** If a matroid M is *representable* over a field $\mathbb{F}$, then M^* is also representable over the same field $\mathbb{F}$.

Example : Consider the vector matroid M with the following representation over R

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

The ~~by the theorem the~~ corresponding dual matroid M^* is the vector matroid represented by

$$A^* = \begin{bmatrix} -1 & -1 & 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 1 & 0 \\ -1 & 0 & -1 & 0 & 0 & 1 \end{bmatrix}$$

As and interesting note, this vector matroid A is associated to the graph K_4

Fix layout

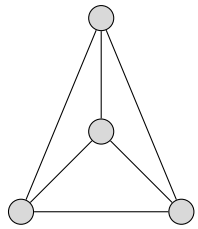


Figure 9: K_4, the complete graph on 4 vertices

Aditionally, from this we can also verify the *rank* and *corank* propositions established before. This is, we can clearly observe that A has a ground set $E = \{e_1, e_2, \ldots, e_6\}$ with 6 elements, where each $e_i; i = 1, 2, \ldots, 6$ represents a column, hence $|E| = 6$. We also see that A has rank $r(A) = 3$, which can be easily verified by observing the first 3 columns that correspond to the identity matrix in the construction of the form $[I_r|D]$. Similarly, if we observe the dual we notice that also $r(A^*) = 3$. So, $r(A) + r(A^*) = 3 + 3 = 6 = |E|$

We have seen many concepts related to dual matroids, including some representations for vector matroids, however we have not gone that much into detail with graphic matroids. So, the reader could still be wondering, *"Is it possible to have a graphic matroid whose dual is not graphic?"*

To answer that we have the following theorem

Theorem 14.

The dual of a graphic matroid is itself graphic if and only if the underlying graph is planar.

Example : Let us consider the bipartite graph $K_{3,3}$.

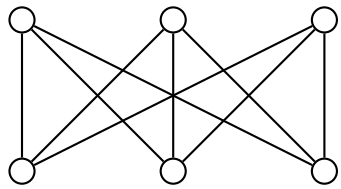


Figure 10: The bipartite graph $K_{3,3}$

We can see it has 9 edges, so the ground set is $E = \{1, 2, 3, \ldots, 9\}$.

The matrix associated to the matroid $M(K_{3,3})$ is the following:

$$J = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

This is because if we label the columns of J as $E = \{e_1, \ldots, e_9\}$ and define a matroid $M(J)$ on E, it is easy to see that we associate each column of J to the correspondingly labeled edge in $K_{3,3}$, so that they generate the same matroid. Moreover, this means that we can take a basis for the column space of J, such as, $B = \{e_1, e_2, e_3, e_4, e_5\}$, such that it corresponds to a spanning tree T of $K_{3,3}$ (See Figure 11.). In other words, this means that adding any other column to J gives a linear dependency, more precisely a circuit in $M(J)$, and adding any edge to T generates a cycle.

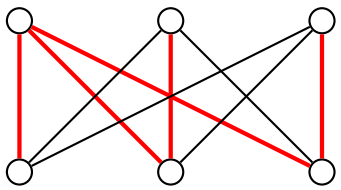


Figure 11: Graph $K_{3,3}$, showing in red an example of edges that form a spanning tree, that can be associated accordingly to the basis of J.

Now that we have show that $K_{3,3}$ has an associated matrix, which produces the same Matroid, we can use the Theorem 13. to obtain the corresponding dual. So we get,

$$J^* = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

As a sanity check we can see that: $r(J) = 5$; $r^*(J) = 4$, and $|E(M)| = 9$. Hence, we see that $r(M) + r^*(M) = |E(M)|$ holds. According to the **Corollary 1.**, *If a matroid M is representable over a field $\mathbb{F}$, then M^* is also representable over $\mathbb{F}$*. Here we see that both matroids are vector matroids over the field $\mathbb{F}_2$. Finally, in this example we can observe that $K_{3,3}$ is not a planar graph. This implies that, although $M(K_{3,3})$ is a graphic matroid, its dual, $M^*(K_{3,3})$ is not graphic.

9 Conclusion

In the article we discussed several equivalent definitions of matroids. As a starting point we choose the definition in terms of independent sets. We saw they naturally abstract the linear indepenent subsets of vector spaces. We then proceeded by showing the description in terms of maximal independent sets - bases. Afterwards we moved to circuits and how they can on the one hand be interpreted as minimal dependent or as object naturally abstracting graphic cycles on the other. We then moved on to more intricate objects which described the matroid by assining some value to each set. First we saw the rank function and second the closure operator, both providing a new perspective on how to describe the matroids by not listing subsets directly, but rather present it using a fucntion. Lastly, we introduced the concept of flat. Along the way we

proved the cryptomorphism - that is that the matroid can be described starting from any viewpoint. As an example we showed that the algebraically dependent sets in field extensions also have a natural matroid structure, even though the matroid modeled a much broader concept of algebraic independence and no longer linear independence. As our last illustration of matroids we turned away from cryptomorphisms and defined the concept of a matroid dual which had many interesting properties. Finally we showed that a dual of a graphic matroid can be non-graphic.

References

[1] G. Gordon and J. McNulty. *Matroids: A geometric introduction.* Cambridge University Press, 2012.

[2] J. S. Milne. *Fields and Galois Theory.* Kea Books, Ann Arbor, MI, 2022.

[3] J. G. Oxley. *Matroid theory.* Oxford Science Publications. Oxford University Press, USA, 1993.

[4] R. P. Stanley. *An introduction to hyperplane arrangements.* IAS/Park City Mathematics Series Volume 00, 0000, 2006.