university of
groningen

Cryptomorphic Descriptions of Matroids

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

June 2023

Contents

1 Introduction

1.1 (In)dependence

In English language, two people, objects or concepts are dependent on each other if both in some way influence one another. Two things being independent of each other in turn means that they in no way can affect each other.

In mathematics, there are many concepts where we can use these two words to describe certain phenomena, most notably in 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 vector does not *really* stand on its own. An equivalent and more general definition is:

Definition 1. *A set of vectors* $\{v_1, v_2, \cdots, v_n\}$ *is linearly dependent if there exists* $a_1, a_2, \cdots, a_n \in \mathbb{R}$ *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:

Definition 2. *A set of vectors* $\{v_1, v_2, \cdots, v_n\}$ *is linearly independent if* $a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$ *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 so, we can visualize the concept of independence in other fields of mathematics.

1.2 Matroids

A matroid is a structure that abstracts the notion of independence. To construct a matroid we 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 some collection of subsets of the ground set, following a couple of rules. Usually, this initial collection would be the collection of *independent sets*. However, it turns out that there are many surprisingly equivalent ways of defining a matroid, such as

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

We call any such equivalent way of defining a matroid a *cryptomorphism* [1]. 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, relating a new notion to a previously proved one. All of this will help us gain a deeper insight into the concept of dependence and independence and ultimately answer our guiding question **- how can we define matroids?**

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 3. *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*

(I1) We have $\emptyset \in \mathcal{I}$.

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

(I3) 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**.*

There are some alternatives to the third property 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 $|I_1| = |I_2|$.*

Example 2.1. In figure (1) we 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 colored in orange. It is clear 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 matroids* arising from linear algebra. We say that a subset of vectors is *independent* in a matroid, if and only if it is *linearly independent* in the usual sense.

Let $A \in \text{Mat}_{m\times n}(\mathbb{F})$ 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 2.2. We will pick a concrete example of $A \in \text{Mat}_{3\times 4}(\mathbb{R})$ to illustrate that the set of columns of a matrix has a natural matroid structure. Suppose we have a matrix

[1] In particular, we are interested in $\mathbb{Z}/p\mathbb{Z}$. By that we mean $\mathbb{Z}$ modulo $p\mathbb{Z}$ so the set of reminders when dividing by a prime number p. We will denote this field by $\mathbb{F}_p$

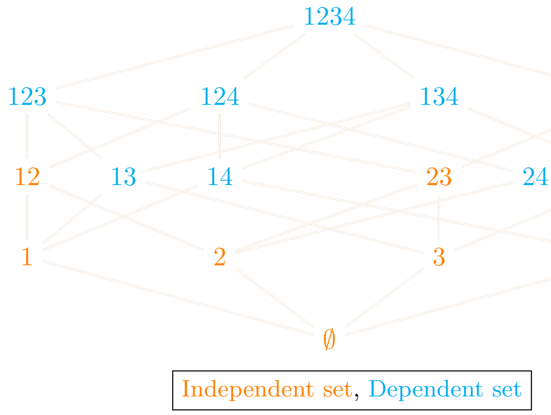


Figure 1: Diagram of a 4-element matroid, with dependent and independent sets colored accordingly.

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

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

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

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 $I \subseteq E$ 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. The idea of the proof is taken from [3, p. 8]. We need to check that the collection $\mathcal{I}$ satisfies the three properties for the collection of independent sets given in the definition.

(I1) First, $\emptyset$ is trivially in $\mathcal{I}$.

(I2) The second property is also satisfied because if $J \subseteq I$ 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 $j \leq i$. If for some linear combination we have $a_1 v_1 + \cdots + a_j v_j = 0$, where $a_i \in \mathbb{F}$ then it is also true that $a_1 v_1 + \cdots + a_j v_j + 0 \cdot a_{j+1} + \cdots + 0 \cdot a_i = 0$. 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 $J \in \mathcal{I}$.

(I3) 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 linear subspaces of $\mathbb{F}^n$ spanned by vectors corresponding to J and I respectively. Because the vectors corresponding to J and I 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 that 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 the dimension does not increase, then $v(e)$ can be expressed as a linear combination of vectors corresponding to J. However, this cannot hold true for *every* $e \in I - J$. Suppose for contradiction, that for every $e \in I - J$ it holds that the vector $v(e)$ is already in V_J. Because for all elements in the intersection, $i \in I \cap J$, we have $v(i) \in V_J$ by definition, we could then infer $V_I \subseteq V_J$. But this implies 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 4. *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 $K \subseteq F$ is independent if and only if $K = f(L)$ for some independent set $L \in \mathcal{I}$.*

Definition 5. *We call a matroid M representable, if M is isomorphic to a matrix matroid $N[A]$ for some $A \in \mathrm{Mat}_{m \times n}(\mathbb{F})$ over some field $\mathbb{F}$. Moreover, 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 6. *Let $E = \{1, 2, \cdots, n\}$ and $\mathcal{I} = \{L \subseteq E \text{ such that } |L| \leq m\}$. 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.

(I1) For any $m \geq 0$ we have $\emptyset \in \mathcal{I}$ since $|\emptyset| = 0$.

(I2) If $I \in \mathcal{I}$ and $J \subseteq I$ then $|J| \leq |I|$ so $|J| \leq |I| \leq m$ implying $J \in \mathcal{I}$ by definition.

(I3) 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 $B \subseteq E$ 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 for 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. Then all bases of M have the same size.*

Proof. Aiming for contradiction, suppose that the theorem does not hold. 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 computes 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.

Example 2.3. In figure (2), we find a depiction of the same matroid from figure (1). In addition, we also highlight the bases of the matroid in red. Two properties can be observed:

1. The bases are the maximally independent subsets, which means that all of their proper supersets are dependent.

2. Both bases contain two elements (they have the same size).

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

Theorem 4. *Let M be a matroid with E as its ground set, and $\mathcal{B}$ be the set of bases (maximal independent sets) of M. Then $\mathcal{B}$ satisfies the following properties.*

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

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

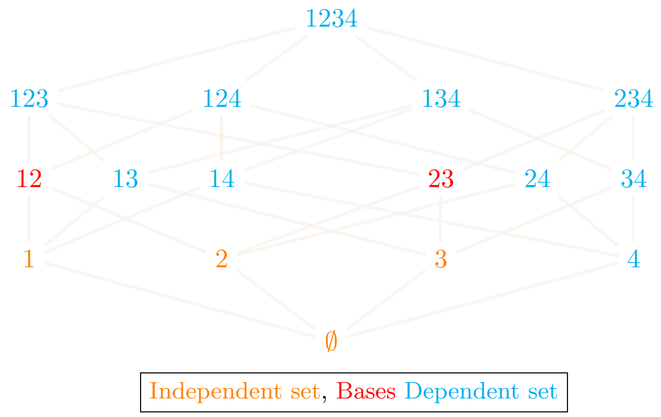


Figure 2: Diagram of a 4-element matroid, with bases in red.

Let us prove that the set of bases of a matroid satisfies the properties (B1) and (B2):

Proof. This proof was inspired by [3, p. 17]. We will prove each property individually:

(B1) To prove the first property, observe that by (I1), $\emptyset$ is always in $\mathcal{I}$ so the collection of independent sets is non-empty. All finite non-empty partially ordered sets have at least one maximal element (see lemma (12) in the appendix on partially ordered sets for more details). Applying this on the partially ordered set induced by inclusion on $\mathcal{I}$ proves a basis must exist.

(B2) 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 some $y \in B_2 - (B_1 - x)$ such that $(B_1 - x) \cup y \in \mathcal{I}$. Since $|(B_1 - x) + y| = |B_1|$ and all maximal independent sets have the same cardinality (see theorem (3)), $(B_1 - x) \cup y$ must be a maximal independent set — thus a basis. Because y is also in $B_2 - B_1$, the property is fulfilled.

□

Lemma 1. *Let E be a finite set, and let $\mathcal{B}$ be a collection of subsets of E satisfying (B1) and (B2). Then $\mathcal{B}$ is equicardinal, that is, all elements in $\mathcal{B}$ have the same cardinality.*

Even though we have already proven that the set of bases of a matroid is equicardinal, we will also show that this property holds for an *arbitrary collection of subsets* satisfying (B1) and (B2). This property will be useful in a future proof.

Proof of lemma (1). This proof was inspired by [3, p. 17] Suppose that $\mathcal{B}$ is not equicardinal, that is, we have $|B_1| > |B_2|$ for some $B_1, B_2 \in \mathcal{B}$. For all B_1, B_2 where that holds, choose the pair that minimizes $|B_1 - B_2|$. Since B_1 is larger than B_2, we know that $B_1 - B_2 \neq \emptyset$. Choose an element $b \in B_1 - B_2$ and apply (B2) to show that there exists some $d \in B_2 - B_1$ 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 the fact 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 indeed equicardinal. □

We are going to show the first cryptomorphism, referring to the idea that matroids can be defined not by the collection of independent sets but by its collection of bases. To show that the two properties (B1) and (B2) are sufficient to describe the bases of M, we will prove that if $\mathcal{B}$ is any collection of subsets satisfying the bases axioms, then the independent sets are all the possible subsets of the elements of $\mathcal{B}$.

Theorem 5. *Let $\mathcal{B}$ be a collection of subsets of a non-empty finite set E, satisfying (B1) and (B2). Let $\mathcal{I} = \{I \subseteq B \mid B \in \mathcal{B}\}$. Then $(E, \mathcal{I})$ is a matroid with $\mathcal{B}$ as its set of bases.*

Proof. This proof was inspired by [3, p. 17]. 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.

(I1) Since (B1) tells us that $\mathcal{B}$ is non-empty, and because $\emptyset$ is a subset of any set (in particular, $\emptyset \subseteq B$, where B is some member of $\mathcal{B}$), we by definition have $\emptyset \in \mathcal{I}$.

(I2) If $I \in \mathcal{I}$ and $J \subseteq I$, then by definition of $\mathcal{I}$ we have that $J \subseteq I \subseteq B$ for some $B \in \mathcal{B}$. We then see that $J \subseteq B$, and by definition $J \in \mathcal{I}$. So $\mathcal{I}$ satisfies (I2).

(I3) By contradiction, suppose (I3) fails for some $I, J \in \mathcal{I}$ with $|I| < |J|$. This means that for all elements $x \in J - I$ we have $I \cup x \notin \mathcal{I}$. Our goal is to show that $|I| \geq |J|$, yielding a contradiction. For this to be the case, we will derive some inequalities between cardinalities of the sets involved.

Let B_I and B_J be the elements of $\mathcal{B}$ that contain I and J respectively, by definition of $\mathcal{I}$, we know such sets exist. Choose some B_J such that $|B_J - (J \cup B_I)|$ is minimal.

It turns out that for our choice of I and J, we have $J - B_I = J - I$. The inclusion $J - B_I \subseteq J - I$ is clear because $I \subseteq B_I$. It then follows that if $J - B_I \neq J - I$, some element $e \in (J-I)-(J-B_I)$ would exist. We verify directly that this implies $e \in B_I$. Since e is a member of $J - I$, our initial assumption that for all $k \in J - I$ we have $I \cup k \notin \mathcal{I}$ tells us that $I \cup e \notin \mathcal{I}$. This contradicts $I \cup e \subseteq B_I$, since all subsets of a base are independent.

Suppose now that $B_J - (J \cup B_I)$ is non-empty. Let j be an element of this set. We then know by (B2) that there exists some element $i \in B_I - B_J$ such that $(B_J - j) \cup i \in \mathcal{B}$. However, $i \in B_I$ implies

$$|((B_J - j) \cup i) - (J \cup B_I)| = |(B_J - j) - (J \cup B_I)| < |(B_J - (J \cup B_I)|.$$

We've now found a new element $B = (B_J - j) \cup i$ in $\mathcal{B}$ that has $|B - (J \cup B_I)|$ smaller than $|B_J - (J \cup B_I)|$. Note how $j \notin J$ means that

$$J = J - j \subseteq B_J - j \subseteq (B_J - j) \cup i = B.$$

We then have $J \subseteq B$, which means that B should have been our choice for B_J that minimalizes $|B_J - (J \cup B_I)|$. Thus, minimality of our choice of B_J is contradicted, and thus, $B_J - (J \cup B_I) = \emptyset$. This now implies that $B_J \subseteq J \cup B_I$, which implies that $B_J - B_I \subseteq (J \cup B_I) - B_I = J - B_I$. Since $J - B_I \subseteq B_J - B_I$ already holds (because $J \subseteq B_J$), this proves equality between $B_J - B_I$ and $J - B_I$.

Next up, we apply a similar procedure to prove that $B_I - (I \cup B_J)$ is empty. Assume by contradiction that i is a member of the set. We can then apply $(B2)$ to get some $j \in B_J - B_I = J - B_I = J - I$ such that $(B_I - i) \cup j \in \mathcal{B}$. Since our choice of i tells us that $i \notin I$, we have that $I \cup j = (I - i) \cup j \subseteq (B_I - i) \cup j$, which means $I \cup j \in \mathcal{I}$. This precisely gives us $(I3)$, which contradicts our original assumption. Thus, $B_I - (I \cup B_J) = \emptyset$. By the same logic we used in the previous paragraph, $B_I - B_J = I - B_J \subseteq I - J$. This means that $|B_I - B_J| \leq |I - J|$.

We can use the fact that $\mathcal{B}$ is equicardical (lemma (1)), to see that $|B_I - B_J| = |B_J - B_I|$. At last, we use everything we've obtained so far to get the following

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

We therefore obtain the inequality $|I - J| \geq |J - I|$. We know that $I = (I - J) \cup (I \cap J)$, and $I - J$ is clearly disjoint with $I \cap J$. We notice that

$$|I| = |(I - J) \cup (I \cap J)| = |I - J| + |I \cap J| - |\underbrace{(I - J) \cap (I \cap J)}_{=\emptyset}|.$$

Therefore, $|I| = |I - J| + |I \cap J|$ and by the same reasoning $|J| = |J - I| + |I \cup J|$. We are now almost done. Combining the above ineqalities with $|I - J| \geq |J - I|$, we observe that $|I - J| + |I \cap J| \geq |J - I| + |I \cap J|$, which finally implies $|I| \geq |J|$. This contradicts our assumption that $|I| < |J|$.

Thus, we have derived a contradiction when assuming that a pair (I, J) of subsets violating (I3) exists. Hence, $\mathcal{I}$ satisfies (I3), and all in all $(E, \mathcal{I})$ 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 by definition maximal members of $\mathcal{I}$. □

2.3 Circuits

As mentioned above, we can define matroids in many different ways. One such way is defining matroids in terms of minimally dependent sets — which we refer to as circuits.

Definition 7. *Let $M = (E, \mathcal{I})$ be a matroid. Any subset $D \in E$ which is not independent is called dependent. Circuits are minimal dependent sets of M. We will denote the collection by $\mathcal{C}(M)$.*

The name is a reference to matroid circuits corresponding to circuits of the underlying graph when talking about graphic matroids (which we will discuss in section (3)).

Similarly, as with the independent set definition, we can use circuits to formulate an axiomatic definition of matroids. 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.

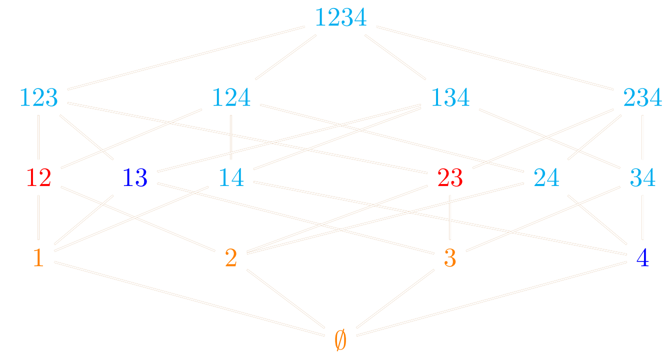
Definition 8. *Let E be a non-empty finite set, and $\mathcal{C}$ a collection of subsets of E, called circuits, such that:*

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

(C2) If C_1 and C_2 are members of $\mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$.

(C3) 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 $C_3 \subseteq (C_1 \cup C_2) - e$.

Example 2.4. Consider figure (3). This is the same matroid example as in figure (2). We've also highlighted circuits (in blue). The circuits are minimal dependent sets, where sets above are dependent. Also note how all independent sets contain no circuits.



Independent set, Basis, Dependent set, Circuit

Figure 3: Diagram of a 4-element matroid, with circuits in blue

Example 2.5. To get an intuition behind (C3), let us consider the matroid induced by the graph in figure (4). We will discuss graphic matroids later, but for now consider cycles of the graph as circuits. The diagram highlights two circuits — C_1 and C_2 — that share an edge (e). Taking the union of both circuits and removing e yields a subgraph contains another cycle — circuit C_3.

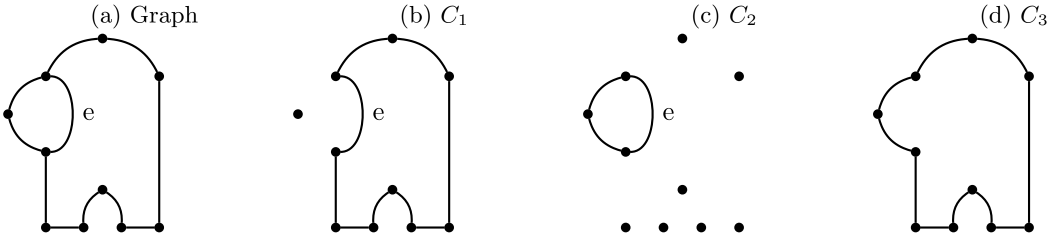


Figure 4: A graph having three cycles.

Lemma 2. *All circuits in a matroid satisfy (C1), (C2) and (C3).*

Proof. We will prove each property individually:

(C1) $\emptyset \in \mathcal{I}$, therefore $\emptyset$ is not dependent (which means it cannot be a circuit)

(C2) Assume that for C_1 and C_2 minimally dependent with $C_1 \subseteq C_2$, it holds that $C_1 \neq C_2$. In other words, C_1 is propperly contained in C_2. This contradicts the fact that C_2 is minimally dependent.

(C3) Assume a counterexample exists. Because $C_1 \cup C_2 - e$ does not contain a circuit, it must be an element of $\mathcal{I}$.

Aiming for contradiction, suppose that $C_2 - C_1$ is empty. 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 $f \in C_2 - C_1$ 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 $C_1 \nsubseteq I \in \mathcal{I}$ (otherwise C_1 would be independent). This means some $g \in C_1$ exists such that $g \notin I$. As $f \in C_2 - C_2$, 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 maximality.

□

Theorem 6. *Let E be a set and $\mathcal{C}$ be a collection of subsets of E which satisfies the conditions (C1), (C2) and (C3) outlined above. Let $\mathcal{I}$ be the collection of subsets of E that contain no member of $\mathcal{C}$, that is*

$$\mathcal{I} = \{I \in 2^E \,|\, \textit{for all } \ C \in \mathcal{C} \textit{ we have } C \nsubseteq I\}.$$

Then 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:

(I1) The only subset of $\emptyset$ is $\emptyset$, but $\emptyset \notin \mathcal{C}$, as $\emptyset$ satisfies $\mathcal{I}$, $\emptyset \in \mathcal{I}$.

(I2) Assume we have $X \subseteq Y \in \mathcal{I}$. Aiming for contradiction, 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.

(I3) Given $X, Y \in \mathcal{I}$ with $|X| < |Y|$ we must show there exists some $e \in Y - X$ such that $X \cup e \in \mathcal{I}$. Assume that a counterexample exists. That is, some pair $X, Y \in \mathcal{I}$ must exist such that for all $e \in Y - X$ we have $X \cup e \notin \mathcal{I}$. Assume such a counterexample exists. Pick such a counterexample which maximizes $|X \cap Y|$. Assume $X - Y$ is non-empty (otherwise $X \subseteq Y$ and by (I2) we can pick any $y \in Y - X$ such that $X \cup y \in \mathcal{I}$, because $X \cup y \subseteq Y$). Pick some $x \in X - Y$. We will proceed by cases:

(a) If $Y \cup x$ is independent, we claim that $(X, Y \cup x)$ is a counterexample as well. This is trivially shown by noticing how $(Y \cup x) - X = Y - X$, so any choice of $e \in (Y \cup x) - X$ is also in $Y - X$, which then implies that $X \cup e \notin \mathcal{I}$. We note that

$$|X \cap (Y \cup x)| = |(X \cap Y) \cup (X \cap x)| = |(X \cap Y) \cup x|,$$

but $x \notin X \cap Y$, so $|(X \cap Y) \cup x| = |X \cap Y| + |\{x\}| = |X \cap Y| + 1$. As $|X \cap Y| + 1 > |X \cap Y|$, we can conclude (X, Y) did not maximize $|X \cap Y|$, hence a contradiction.

(b) Otherwise, $Y \cup x$ is not independent. That is to say, some $C \in \mathcal{C}$ must exist such that $C \subseteq Y \cup x$. We make the five intermediate claims:

i. There exists some $y \in Y - X$ such that $y \in C$.

Proof. If there is no such y, then $C \subseteq X$. This means that there is a circuit inside X, which contradicts the fact that $X \in \mathcal{I}$. □

We will make use of this y in the rest of the proof.

ii. It holds that $x \in C$.

Proof. If this is not the case, we have $C \subseteq Y$, which would imply that $Y \notin \mathcal{I}$. □

iii. The circuit C is the unique circuit with the property $C \subseteq Y \cup x$.

Proof. Assume another distinct $D \in \mathcal{C}$ exists such that $D \subseteq Y \cup x$. As $x \in C$ and $x \in D$ (this follows similarly to the proof of $x \in C$), we can conclude that $x \in C \cap D$. We can now apply (C3) to generate some circuit $C' \subseteq C \cup D - x$. We recall that $C, D \subseteq Y \cup x$, therefore $C \cup D \subseteq Y \cup x$. Furthermore, $C \cup D - x \subseteq Y$. By transitivity with $C' \subseteq C \cup D - x$ we now have $C' \subseteq Y$, which implies by definition $Y \notin \mathcal{I}$, hence a contradiction. □

iv. $(Y \cup x) - y$ is independent.

Proof. If this is not the case, there must exist some $D \in \mathcal{C}$ with $D \subseteq (Y \cup x) - y$. Since $(Y \cup x) - y \subseteq Y \cup x$, this implies that D is a circuit with $D \subseteq Y \cup x$. By the uniqueness C proved before, we have $D = C$. But this would imply that $y \in C = D$ so $y \in (Y \cup x) - y$ which is a contradiction. □

v. $(X, (Y \cup x) - y)$ is a counterexample for (I3).

Proof. This trivially follows after noticing that

$$((Y \cup x) - y) - X \subseteq (Y \cup x) - X = Y - X.$$

Any choice $e \in ((Y \cup x) - y) - X$ is then also in $Y - X$, which implies that $X \cup e \notin \mathcal{I}$. This is exactly what it means to be a counterexample for (I3). □

We now notice that

$$\begin{aligned} |X \cap ((Y \cup x) - y)| &= |(X \cap (Y \cup x)) - y| \\ &= |((X \cap Y) \cup (X \cap x)) - y| \\ &= |((X \cap Y) \cup x) - y|. \end{aligned}$$

We note that $y \notin X$ means that $y \neq x$, and therefore $((X \cap Y) \cup x) - y = (X \cap Y) \cup x$. Furthermore, $x \notin Y$ means that $x \notin X \cap Y$, and therefore $|(X \cap Y) \cup x| = |X \cap Y| + 1$. We can now conclude that $|X \cap ((Y \cup x) - y)| = |X \cap Y| + 1$. As $|X \cap Y| + 1 > |X \cap Y|$ and $(X, (Y \cup x) - y)$ is a counterexample of (I3), we can conclude that (X, Y) did not maximize $|X \cap Y|$, hence a contradiction.

We now show that C is a circuit for the newly defined matroid if and only if it is a member of $\mathcal{C}$.

$\Longrightarrow$ If C is a circuit for $(E, \mathcal{I})$, then $C \notin \mathcal{I}$, which means that C contains some $D \in \mathcal{C}$. As C is minimally dependent, all its proper subsets are independent, but members of $\mathcal{C}$ cannot be independent (as seen in the definition of $\mathcal{I}$), which implies that $C = D$, hence $C \in \mathcal{C}$.

$\Longleftarrow$ Let $C \in \mathcal{C}$. Since $C \subseteq C$, $C \notin \mathcal{I}$ is implied by how we defined $\mathcal{I}$. The fact that C is now dependent means that there is a set D contained in C that is a circuit of the matroid. We have already shown that a circuit of the matroid is an element of $\mathcal{C}$, which implies that $D \in \mathcal{C}$. Now we can apply (C2) on D and C to see that $C = D$. Thus, C is a circuit of the matroid.

We can now conclude that $(E, \mathcal{I})$ is indeed a matroid with $\mathcal{C}$ as it's set of circuits. □

2.4 A Worked Example

Example 2.6. 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, we note that $U_{2,4} = (\{1, 2, 3, 4\}, \mathcal{I})$ 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 3. *Suppose a set of vectors $A = \{w_1, w_2, \cdots, w_r\} \subseteq \mathbb{F}_2^n$ is minimaly linarly dependent, that means that it is linarly dependent but any proper subset of it is linearly independent. Then $w_1 + w_2 + \cdots + w_r = 0$.*

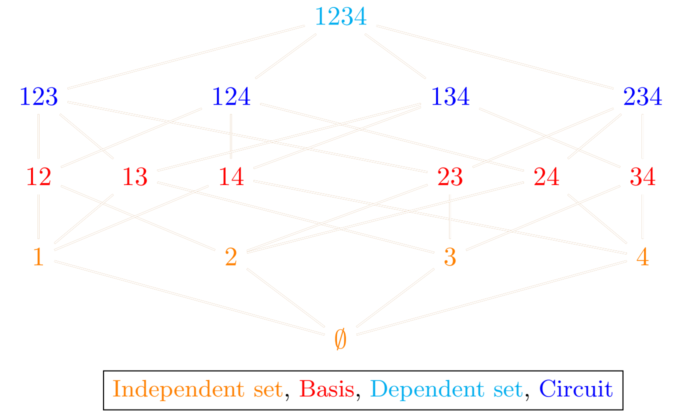


Figure 5: Representation of $U_{2,4}$

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 lemma (3) that $v_1 + v_2 + v_3 = 0$ and $v_1 + v_2 + v_3 = 0$. However, we are in $\mathbb{F}_2$ so

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

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, p. 20] works, namely

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

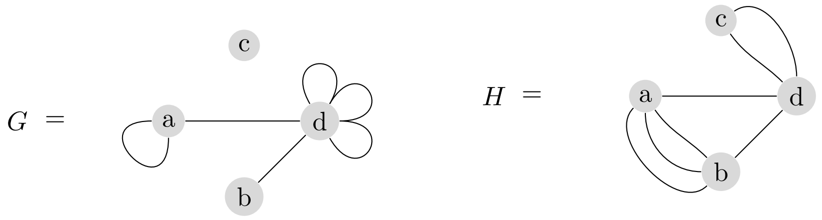
We see that no column vector of A is 0, so all single-element subsets are independent. No vector is a scalar multiple of each other, so two element subsets are independent. Finally, no 3-element subsets can be independent, since the dimension of the $\mathbb{F}_3^2$ is 2, so the dimension of any subspace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

To conclude the example of $U_{2,4}$, we will 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. But 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. It follows that $U_{2,4}$ is not graphic.

3 Graphic Matroids

First, we are not just interested in simple graphs. For reminder, a simple 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 illustrate the two notions. Intuitively, a loop is an edge going from a vertex to itself, and one can also have multiple loops on a single vertex. Parallel edges are intuitively multiple edges between the same vertices.



(a) Loops

(b) Parallel edges

Figure 6: Graph G with loops and graph H with parallel edges

In figure (6) we see graphs G and H, the first one has loops and the second one has parallel edges. One way to make both constructions formal is to use *multiset* of edges instead of a set, as in [3, 4].

However, the formal construction of loops and parallel edges is not so important, as we will see in the preceding text, and one can usually restrict its attention to simple graphs. What is important for us is how do the loops and parallel edges interact with the notion of a *cycles* in graphs.

For clarity, we define exactly what we mean by a cycle in a simple graph.

Definition 9. *Let $G = (V, E)$ be a simple graph. Then a sequence $v_0, v_1, \cdots, v_k$ of vertices, where $k \geq 3$, is called a cycle if the following condidtions are satisfied*

1. *If $v_i = v_j$ for some $0 \leq i, j \leq k$ then $i = j$ or $k = 0$, in other words $v_0 = v_k$ while all of the other vertices are distinct.*
2. *For all $0 \leq i < k$, we have that v_i and v_{i+1} are incident.*

We need to extend the notion of a cycle to non-simple graphs. To do this, we additionally define that a loop is a cycle of length one. Intuitively, this is consistent with the simple graph definition, because our initial and final vertex is the same without any vertices in between. Similarly, we define a set of two distinct parallel edges to be a cycle of length two. This makes sense because the first and the last vertex is the same with one in between, but edges cannot repeat, so we have to go via different edges connecting two vertices.

Also, for parallel edges, at most one from a class of parallel edges connecting the same two vertices can appear in a cycle.

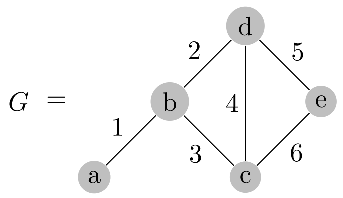


Figure 7: Simple graph on 6 edges

We 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 $\emptyset$ is not in $\mathcal{C}$, none of its members is properly contained in another, 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 7. *Let $G = (V, E)$ be a graph and let $\mathcal{C}$ be the collection of all sets of edges of cycles in G. Then M with the ground set E (the set of edges) is matroid with $\mathcal{C}$ as collection of circuits. In particular, this means that if C_1, C_2 are distinct sets of edges of cycles and $e \in C_1 \cap C_2$ then there exists a set of edges of cycle C_3 such that $C_3 \subseteq C_1 \cap C_2 - e$.*

Proof. To show that the set E is a matroid with the collection $\mathcal{C}$ of cycles as circuits we have to verify the three circuit axioms.

(C1) The empty set is by our definition not a cycle. For reminder, by our definition a cycle always includes a non-empty set of vertices it is build upon. If it is in a simple graph, then it has to have at least three vertices. Our extended notion also includes loops and parallel edges, which are still built upon at least one vertex.

(C2) To show the second property, suppose we have two sets of edges of cycles such that $C_1 \subseteq C_2$ 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 clear, because the only possibility is they are equal) the set of edges $C_2 - e$ corresponds to a path from the vertices which e connects. However, there is a cycle $C_1 \subseteq C_2 - e$ which is a subset of a path - a contradiction. So if $C_1 \subseteq C_2$ then $C_2 - C_1$ is empty, in particular then $C_2 = C_1$ and all the second circuit axiom is satisfied.

(C3) Finally, we prove the third property. The idea of the the rest of the proof is taken from [3, p. 10]. Let C_1 and C_2 be two distinct cycles and e be an element of $C_1 \cap C_2$. We would like to show that there is a set of edges of cycle $C_3 \subseteq C_1 \cap C_2 - e$.

First, if $C_1 \cap C_2 = \emptyset$ there is nothing to prove, because the conditional part of the if statement in (C3) is not satisfied.

Second, assume there exists $e \in C_1 \cap C_2$. 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 intersection be the edge $e = \{v_0, v_1\}$. The idea of the proof is very simple. Our goal is to find

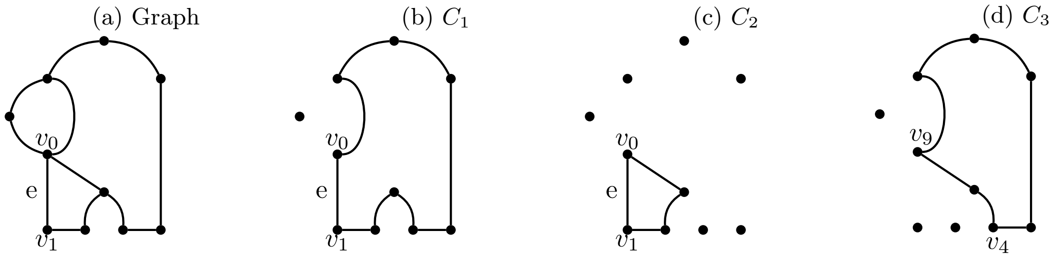


Figure 8: A graph together with three relevant cycles.

a cycle in the set of edges $C_1 \cup C_2 - e$. We go around C_1 until we can come to a vertex that is disjoint with C_2. Then we would like to come back that vertex as quickly as we can by using edges of C_2, thus avoiding e.

As an illustration of the procedure we see a graph in figure (8). The vertex v_4 is the first one not in C_2 and v_9 is the first one in C_1 which is after v_4 but is back in C_2. The cycle obtained in this procedure is C_3 which evidently does not include e.

Let k be the smallest integer $1 < k < n$ such that the vertex v_k is not in the cycle C_2. We know that such an integer exists because we have already proved (C2), so if C_1 and C_2 are distinct, then necessarily one is not contained in the other, which means both $C_2 - C_1$ and $C_1 - C_2$ are non-empty. Next, let l be the smallest integer $k < l \leq n$ such that v_l is in C_2. We know such an integer exist because $v_n \in C_2$.

Let $v_l, w_{l+1}, w_{l+2}, \cdots, v_{k-1}$ 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_l and v_{k-1} (they are distinct, since $k < l$ and it cannot hold that $k-1 = 0$ and $l = n$, since this would imply $k = 1$, which cannot hold) there are two paths going from v_l to v_{k-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

$$v_k, v_{k+1}, \cdots, v_l, w_{l+1}, \cdots, v_{k-1}, v_k,$$

is the desired one and denote its set of edges by C_3. By construction, the sequence of vertices $v_k, v_{k+1}, \cdots, v_l, w_{l+1}, \cdots, v_{k-1}, v_k$ is a cycle. This is because first of all, the neighboring vertices are incident and second of all, besides v_k there is no vertex repeating. The second statement holds because we have chosen $v_k, v_{k+1}, \cdots, v_{l-1}$ to be disjoint from C_2, while $v_l, w_{l+1}, \cdots, v_{k-1}$ is a path in C_2. Crucially, $e \notin C_3$, because we have chosen path $v_l, w_{l+1}, \cdots, v_{k-1}$ in C_2 to not include the edge e and $v_k, v_{k+1}, \cdots v_l$ does not include it because $e = \{v_n = v_0, v_1\}$ and there is no v_0 in our cycle. Finally, all the vertices of C_3 are inside the vertices of C_1 or C_2 by construction so, to conclude, the set C_3 has the desired property $C_3 \subseteq (C_1 \cup C_2) - e$.

We have 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 know 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 conclude, the collection of edges of cycles $\mathcal{C}$ satisfies the circuit axioms (C1), (C2) and (C3), therefore we know the cryptomorphic description of matroids in terms of circuits that E is in fact a matroid with having $\mathcal{C}$ as its collection of circuits.

□

Definition 10. *We call a matroid M graphic if it is isomorphic 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.

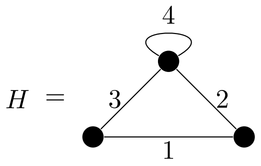
Suppose that the set of edges B is a base of a graphic matroid. Since B is maximally indepenent, adding any element not in B to B, i.e. any edge not in B to it, we get a *dependent set*, which means it contains a circuit. By our definition, this means that it has to contain an edge cycle. Combining all 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 forests.* Note that we cannot say spanning trees because the graph might not be connected.

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 forest, which means it is just a forest.

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

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

(a) Matrix A



(b) Graph H

Figure 9: Matroid $M[A]$ is graphic; it is isomorphic to the graphic matroid G

In figure (9) 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 non-zero 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 three vertices so the size of a spanning forest is at most 3 - 1 = 2.

4 Rank Function

We will introduce our first description of matroids that does not rely on a collection of subsets that satisfies certain properties, but rather on a *function* that satisfies certain properties.

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

$$\mathrm{r}(X) = \max\{\, |I| \mid I \in \mathcal{I} \text{ and } I \subseteq X\}.$$

For example, $\mathrm{r}(E(M)) = |B|$ for some $B \in \mathcal{B}(M)$, and we define $\mathrm{r}(M) = \mathrm{r}(E(M))$. We can characterize the rank function with the following properties:

Theorem 8. *Let M be a matroid on a ground set E, and let $\mathrm{r} : 2^E \to \mathbb{Z}_{\geq 0}$ be its rank function. Then r satisfies these properties.*

(R1) If $X \subseteq E$, then $0 \leq \mathrm{r}(X) \leq |X|$

(R2) If $X \subseteq Y \subseteq E$, then $\mathrm{r}(X) \leq \mathrm{r}(Y)$

(R3) If $X, Y \subseteq E$, then $\mathrm{r}(X \cup Y) + \mathrm{r}(X \cap Y) \leq \mathrm{r}(X) + \mathrm{r}(Y)$

In figure (10) we again find our example matroid drawing. We denote the rank of each set by writing it in subscript below the set. We can see that the rank of any set is at most 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.

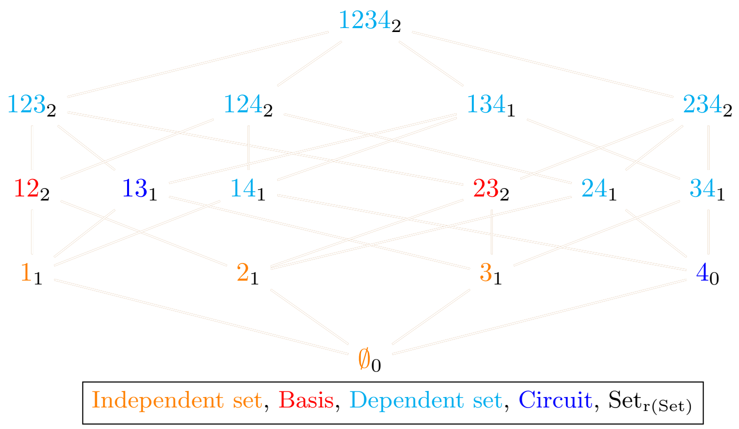


Figure 10: Description of a 4-element matroid, with the rank of each set as subscript.

Now, let us prove that the rank function of a matroid satisfies these properties.

Proof. This proof was inspired by [3, p. 23].

(R1) Since the co-domain of r is $\mathbb{Z}_{\geq 0}$ then $\mathrm{r}(X) \geq 0$. Let I_X be a maximal independent set contained in X. By definition, we see that $|I_X| = \mathrm{r}(X)$. Since $X \supseteq I_X$, it follows that $|X| \geq |I_X| = \mathrm{r}(X)$. Thus, $0 \leq \mathrm{r}(X) \leq |X|$ what we wanted to show.

(R2) Let I_X be a minimal independent set contained in X, so $\mathrm{r}(X) = |I_X|$. $I_X \subseteq X \subseteq Y$ implies that I_X is an independent set contained in Y. Since I_X is an independent set contained in Y then by definition $|I_X| \leq \mathrm{r}(Y)$ since $\mathrm{r}(Y)$ is the size of the *largest* independent set contained in Y. Finally, we get that $\mathrm{r}(X) = |I_X| \leq \mathrm{r}(Y)$ what we wanted to show.

(R3) We assume that $A \subseteq B \subseteq E$. Let $I_{A\cap B}$ be a maximal independent set contained in $A\cap B$. Since $A\cap B \subseteq A\cup B$, it means that $I_{A\cap B}$ 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 $A\cup B$. So $I_{A\cap B} \subseteq I_{A\cup B} \subseteq A\cup B$.

Now, let us take a look at the set $I_{A\cup B} \cap A$. Since the set is contained in A and $I_{A\cup B}$, the property (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 we know by definition, $|I_{A\cup B} \cap A| \leq \mathrm{r}(A)$. Similarly, $|I_{A\cup B} \cap B| \leq \mathrm{r}(B)$.

We will now use the well known fact that for any sets X and Y, it holds that $|X \cup Y| = |X| + |Y| - |X \cap Y|$, in other words $|X| + |Y| = |X \cup Y| + |X \cap Y|$.

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

Since $I_{A\cup B} \subseteq A \cup B$, we see that $I_{A\cup B} \cap (A \cup B) = I_{A\cup B}$.

Because $I_{A\cap B} \subseteq I_{A\cup B}$ and $I_{A\cap B} \subseteq A \cap B$, it tells us that $I_{A\cup B} \cap (A \cap B) \supseteq I_{A\cap B} \cap (A \cap B) = I_{A\cap B}$. Let $e \in I_{A\cup B} \cap (A \cap B)$. Aiming for contradiction, suppose $e \notin I_{A\cap B}$. Since $e \in I_{A\cup B}$, we can see that $I_{A\cap B} \cup e \subseteq I_{A\cup B}$. Then (I2) implies that $I_{A\cap B} \cup e$ is independent. Combining that fact with that $e \in A \cap B$, we see that $I_{A\cap B} \cap e$ is an independent set contained in $A \cap B$. This contradicts the maximality of $I_{A\cap B}$ in being independent and contained in $A \cap B$. Thus, the contradiction gives us that $e \in I_{A\cap B}$. This proves that $I_{A\cup B} \cap (A \cap B) \subseteq I_{A\cap B}$, 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 of course the independent set itself. With this property, we can define the set of independent sets with the three properties of the rank function.

Theorem 9. *Let E be a finite set, and let $\mathrm{r} : 2^E \to \mathbb{Z}_{\geq 0}$ be a function satisfying (R1)-(R3). Let $\mathcal{I} = \{I \subseteq E : \mathrm{r}(I) = |I|\}$. Then $(E, \mathcal{I})$ is a matroid with* r *as its rank function.*

Before we prove this, let us prove the following minor theorem first.

Theorem 10. *Let E be a finite set and $\mathrm{r} : 2^E \to \mathbb{Z}_{\geq 0}$ be a function satisfying (R2) and (R3). Let $X, Y \subseteq E$. If for all $y \in Y - X$, it holds that $\mathrm{r}(X \cup y) = \mathrm{r}(X)$, then we have that $\mathrm{r}(X \cup Y) = \mathrm{r}(Y)$.*

Proof. This proof was inspired by [3, p. 24]. We will prove that the statement holds with $Y - X = \{a_1, a_2, \cdots, a_k\}$ for all positive integers k.

1. Consider the case when $k = 1$. 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. Assume the statement holds for $k = n$. We will attempt to prove it also holds for $k = n + 1$.

   Let us see if the statement holds for $k = n + 1$: Let $Y - X = \{a_1, \cdots, a_{n+1}\}$ and assume that for all $i \in \{1, \cdots, n + 1\}$, it holds that $\mathrm{r}(X \cup a_i) = \mathrm{r}(X)$. Then, using the assumption and our induction hypothesis,

$$\begin{aligned}\mathrm{r}(X) + \mathrm{r}(X) &= \mathrm{r}(X \cup \{a_1, \cdots, a_n\}) + \mathrm{r}(X \cup a_{n+1}) \\ &\geq \mathrm{r}\left([X \cup \{a_1, \cdots, a_n\}] \cup [X \cup a_{n+1}]\right) + \\ &\quad\ \mathrm{r}\left([X \cup \{a_1, \cdots, a_n\}] \cap [X \cup a_{n+1}]\right) && \text{(using (R3))} \\ &= \mathrm{r}\left(X \cup \{a_1, \cdots, a_{n+1}\}\right) + \mathrm{r}\left(X\right) \\ &\geq \mathrm{r}(X) + \mathrm{r}(X). && \text{(using (R2))}\end{aligned}$$

   Since $\mathrm{r}(X) + \mathrm{r}(X)$ is on both sides, equality holds throughout.

   Thus, $\mathrm{r}(X \cup Y) = \mathrm{r}(X \cup \{a_1, \cdots, a_{n+1}\}) = \mathrm{r}(X)$. And thus, the statement holds for $k = n + 1$.

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

Finally, we can prove Theorem 9:

Proof of theorem (9). This proof was inspired by [3, p. 24]. To prove that $(E, \mathcal{I})$ is a matroid, we will prove that $\mathcal{I}$ satisfies (I1)-(I3).

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

(I2) Assume we have $J \subseteq I \in \mathcal{I}$. 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

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

Since $\mathrm{r}(J) = |J|$ means that $J \in \mathcal{I}$, we conclude that (I2) is satisfied.

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

For this next part, let e be anarbitrary member of $I - J$. Since $J \subseteq J \cup e$, we can use (R1) and (R2) to see that

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

We see that $J \cup e \notin \mathcal{I}$ tells us that $\mathrm{r}(J \cup e) \neq |J \cup e| = |J| + 1$. Since we just proven that $|J| \leq \mathrm{r}(J \cup e) \leq |J| + 1$, it must mean that $\mathrm{r}(J \cup e)$ is equal to what's on the left-hand side, so $|J| = \mathrm{r}(J)$.

This gives us that for all $e \in I - J$, it holds that $\mathrm{r}(J \cup e) = \mathrm{r}(J)$. With this, theorem (10) tells us that $\mathrm{r}(J \cup I) = \mathrm{r}(J) = |J|$. However, since $I \subseteq J \cup I$, we can use (R2) to see that $\mathrm{r}(J \cup I) \geq \mathrm{r}(I) = |I|$. Combining those two, we get that $|J| \geq |I|$. This contradicts our assumption that $|J| < |I|$. Thus, (I3) is satisfied.

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

5 Closure Operator

We will introduce one more important notion, the one of closure operator. As the name 'operator' 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 $X \subseteq E$ 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 also has interesting interpretation in the case of our main examples of representable and graphic matroids. In the case of representable matroids, it adds 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 the spanning forest).

Definition 11. *Let $M = (E, \mathcal{I})$ be a matroid. The closure operator is a function* $\mathrm{cl} : 2^E \to 2^E$ *such that*

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

The operator has numerous important properties. This time we will immediately prove the reverse statement. Namely, that these characteristic properties *uniquely characterize* the closure operator of a matroid.

Theorem 11. *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*

(CL1) For any $X \subseteq E$ we have $X \subseteq \mathrm{cl}(X)$.

(CL2) If $X \subseteq Y \subseteq E$ then $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$.

(CL3) For all X we have $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$.

(CL4) Let $X \subseteq E$ and $b \in \mathrm{cl}(X \cup a) - \mathrm{cl}(X)$ then $a \in \mathrm{cl}(X \cup b)$.

Proof. All the four statements in the *only if* direction (assuming cl is the closure operator) are rather straightforward, and we will prove them first.

$\Longrightarrow$ We first assume cl is the closure operator and would like to show the four properties.

(CL1) If $X \subseteq E$ 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 definition of the closure operator which shows the inclusion $X \subseteq \mathrm{cl}(X)$.

(CL2) Let $X \subseteq Y \subseteq E$ 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 immediately 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 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 $X \subseteq Y$ 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 $Y \cap (X \cup x) = X$. So

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

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 definition $x \in \mathrm{cl}(Y)$.

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

(CL3) By combining the first and the second property already of closure we have already proven, the inclusion $\mathrm{cl}(X) \subseteq \mathrm{cl}(\mathrm{cl}(X))$ 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 theorem (10), namely for all $v \in \mathrm{cl}(X)$ we by definition have $\mathrm{r}(X \cup v) = \mathrm{r}(X)$ so by theorem (10) we have $\mathrm{r}(\mathrm{cl}(X)) = \mathrm{r}(X)$. But now we have, since $X \subseteq \mathrm{cl}(X)$ 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 inequalities above. In particular, this means that $\mathrm{r}(X \cup z) = \mathrm{r}(X)$ which by definitions means that $z \in \mathrm{cl}(X)$. So the desired inclusion $\mathrm{cl}(\mathrm{cl}(X)) \subseteq \mathrm{cl}(X)$ also holds, which finally implies the desired equality of sets $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$.

(CL4) Let $X \subseteq E$ 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 definition $\mathrm{r}(X \cup b) \neq \mathrm{r}(X)$, and because $X \subseteq X \cup b$ 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 independent set inside a given subset, adding an element to a set can increase its rank by at most 1, so 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.

$\Longleftarrow$ Now we prove the more complicated reverse direction. We assume we have a finite set E and an arbitrary function $\beta : 2^E \to 2^E$ satisfying 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 immediately apparent.

So we will not relate the function β directly to the independent sets, but rather some other cryptomorphic definition of matroids we have already proven. In particular, observe that 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 independent set inside of X is a *basis.*

Therefore 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. The following proof is our own, in [3, p. 27], the author manages do define independent sets purely in terms of the closure, but we find our proof more intuitive, so we will present here. Therefore, we define $\mathcal{B}' = \{X \subseteq E \mid \beta(X) = E\ \}$ 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.

(B1) 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 inclusion in $E \subseteq \beta(E) \subseteq E$ 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 non-empty.

(B2) For the second property (B2) assume B_1, B_2 are distinct elements of $\mathcal{B}$. Because $\mathcal{B}$ consists 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 the elements of B_2 would be in $\beta(B_1 - x)$, but then we would have that $B_2 \subseteq \beta(B_1 - x)$ by (CL2) we would have that $E = \beta(B_2) \subseteq \beta(\beta(B_1 - e)) = \beta(B_1 - e) \neq E$. 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

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

where we have used (CL3) in the first equality and $x \in \beta((B_1 - x))$ in the second equality. 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 separately that all 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 $B_3 \subseteq \beta(B_{min} - x)$ which would mean that $E = \beta(B_3) \subseteq \beta(\beta(B_{min} - x)) = \beta(B_{min} - x)$ 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 it is 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 $X \subseteq E$. 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 $X \subseteq \beta(X)$). Then the largest independent set L of $\beta(X)$ has the size l. We know L is in some basis B of $\mathcal{B}$, i.e. $L \subseteq B$. 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

$$L \subseteq \beta(X) \subseteq \beta(X \cup (B - L)),$$

and

$$B - L \subseteq \beta(X \cup (B - L)),$$

which in particular means that $B \subseteq \beta(X \cup (B - L))$. Finally, this would mean that $E = \beta(B) \subseteq \beta(\beta(X \cup (B - L))) = \beta(X \cup (B - L))$ 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 contradiction. 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 the elements which preserve rank, we have thus obtained the inclusion $\beta(X) \subseteq \mathrm{cl}'(X)$ for all subsets X.

Finally, suppose for contradiction that for some X the latter inclusion $\beta(X) \subseteq \mathrm{cl}'(X)$ is proper and additionally assume that X is a maximal set with these 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 non-empty (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 $\beta(X) \subseteq \mathrm{cl}'(X)$ 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 $X \cup x \subseteq \beta(X \cup r)$ and since $X \cup r \subseteq \mathrm{cl}'(X)$ we have that $\mathrm{r}'(X \cup r) = \mathrm{r}'(X)$. But on the other hand

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

which is a contradiction. So our initial assumption that the inclusion $\beta(X) \subseteq \mathrm{cl}'(X)$ 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 define three more important family of subsets of a matroid that we will use in the later sections.

Definition 12. *Let $M = (E, \mathcal{I})$ be a matroid with the rank function* r *closure operator* cl. *We call a subset $X \subseteq E$ a flat if* $\mathrm{cl}(X) = X$ *holds. We call a subset $H \subseteq E$ a hyperplane if H is a rank with* $\mathrm{r}(H) = \mathrm{r}(E) - 1$. *Finally, we call a subset $S \subseteq E$ a spanning set if* $\mathrm{cl}(S) = E$.

6 Flats

An excercise in [3, p. 35] asks us to prove a cryptomorphic description of matroids in terms of their flats. 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), hence we will give our proof of the statement.

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

Theorem 12. *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.*

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

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

(F3) 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 $E - F$. By defintion of partition that means that for all $i \neq j$ we have $(F_i - F) \cup (F_j - F) = \emptyset$ and $\cup_{i=1}^{k}(F_i - F) = E - F$.

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.

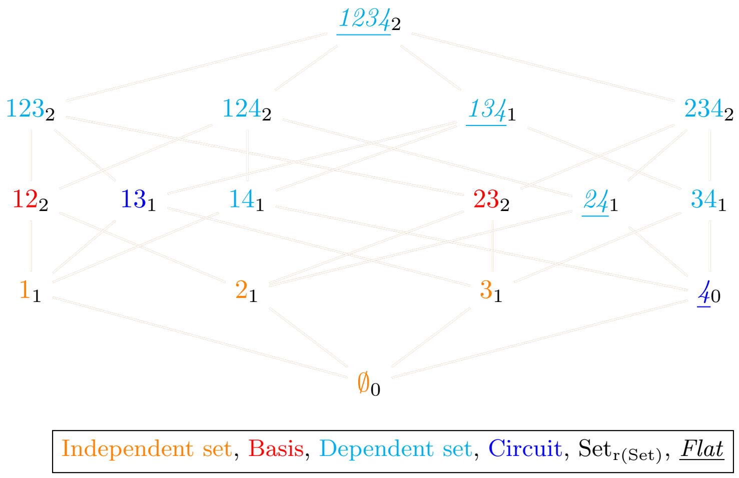

$\underline{\mathit{1234}}_2$
123_2
124_2
$\underline{\mathit{134}}_1$
234_2
12_2
13_1
14_1
23_2
$\underline{\mathit{24}}_1$
34_1
1_1
2_1
3_1
$\underline{\mathit{4}}_0$
$\emptyset_0$
Independent set, Basis, Dependent set, Circuit, $\mathrm{Set}_{\mathrm{r(Set)}}$, $\underline{\mathit{Flat}}$

Figure 11: Description of a 4-element matroid, with the flats in cursive and with a line below it.

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 downward closed, closed under intersections, inclusions, etc. Followed by the third property, which really tells us something non-trivial about how the sets of the collection interact 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.

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

(F1) We see that $E \subseteq \mathrm{cl}(E)$ by the definition of the closure operator and $\mathrm{cl}(E) \subseteq E$ because cl maps from 2^E into E. Thus $\mathrm{cl}(E) = E$ implying E is a flat as desired.

(F2) Again, inclusion $F_1 \cap F_2 \subseteq \mathrm{cl}(F_1 \cap F_2)$ is a fundamental property of closure operator (CL1). Because $F_1 \cap F_2 \subseteq F_1$ we have by (CL2) that $\mathrm{cl}(F_1 \cap F_2) \subseteq \mathrm{cl}(F_1) = F_1$ where the last equality follows by assumption that F_2 is a flat. Similarly, $\mathrm{cl}(F_1 \cap F_2) \subseteq F_2$, which implies $\mathrm{cl}(F_1 \cap F_2)$ is contained in F_1 and F_2, in other words $\mathrm{cl}(F_1 \cap F_2) \subseteq F_1 \cap F_2$. To conclude $F_1 \cap F_2 \subseteq \mathrm{cl}(F_1 \subseteq F_2) \subseteq F_1 \cap F_2$ which implies $\mathrm{cl}(F_1 \cap F_2) = F_1 \cap F_2$, and then by definition $F_1 \cap F_2 \in \mathcal{F}$ thus the second property is satisfied.

(F3) 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 properly containing others with such properties) flat containing $F \cup x$, let us call it G and obviously, $G = \mathrm{cl}(F \cup x)$. We would like G to also be a minimal flat properly containing F. If it is not, there is some flat H such that $F \subseteq H \subseteq G$ 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 $y \in \mathrm{cl}(F \cup x) - \mathrm{cl}(F)$ so by (CL4) we have $x \in \mathrm{cl}(F \cup y)$ which is a contradiction since $\mathrm{cl}(F \cup y)$ 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.

$\Longleftarrow$ 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 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 property $r(X) = |X|$.

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 properties 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. It is 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 $X \subseteq E$ we have $X \subseteq E$ 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 $X \subseteq F_1 \cap F_2$, so if they are not the same we are contradicting the minimality of them. Therefore $F_1 \subseteq F_2$ and $F_2 \subseteq F_1$ hold, so $F_1 = F_2$.

(CL1) If $X \subseteq E$ then by definition, $f(X)$ is an element of $\mathcal{F}$ *containing* X, so we have $X \subseteq f(X)$ and the first property follows.

(CL2) If $X \subseteq Y \subseteq E$ 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 $f(X) \subseteq f(Y)$ as desired.

(CL3) If $X \subseteq E$ is arbitrary then we have that $f(f(X))$ is the minimal member of $\mathcal{F}$ containing $f(X)$, but $f(X)$ is by definition itself in $\mathcal{F}$, and it contains $f(X)$. So we have that $f(X) \subseteq f(f(X)) \subseteq f(X)$ implying $f(f(X)) = f(X)$.

(CL4) Up to this point we have not yet used the second and the third property of $\mathcal{F}$ so we better require them now.

Suppose $X \subseteq E$, $x \in E$ 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 $F_1 \subseteq F_2$ and $F_1 \subseteq F_3$. 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 minimally and some $F_3' \in \mathcal{F}$ which contains $X \cup y$ and contains X minimally. So from $X \cup x \subseteq F_2' \in \mathcal{F}$ we directly infer $F_2 \subseteq F_2'$ 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 definition 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.

$\square$

7 Algebraic Matroids

An interesting concept of independence arises in the study of field theory. We will present a class of matroids derived from the concept of algebraic independence. Hence the term independent set will not refer to a *linearly independent set* but rather an *algebraically independent set.* 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 $\mathbb{F}$. See the appendix for an introduction to fields and subfields. This section will also make use of the concept of partially ordered sets and the appendix provides an introduction to them.

Definition 13. *A subset $S = \{s_1, \cdots, s_n\} \subseteq \mathbb{K}/\mathbb{F}$ is said to be algebraically independent (over $\mathbb{F}$) if there does not exist any non-zero multivariable polynomial in n variables $f \in \mathbb{F}[X_1 \cdots X_n]$, 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 no linear combination with coefficients in $\mathbb{F}$ of products of elements in S is equal to 0.

We know that an element $x \in \mathbb{R}$ is called transcendental with respect to $\mathbb{Q}$ if for non-zero polynomials with rational coefficients $\mathrm{ev}_x(p) \neq 0$. That means that any non-trivial 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 non-zero 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.

Example 7.1. According to [2, p. 113], although e and π are transcendental over $\mathbb{Q}$, it hasn't yet been proven that $\{e, \pi\}$ is algebraically independent.

We will now discuss the notion of algebraic dependence.

Definition 14. *Let $a \in \mathbb{K}/\mathbb{F}$ and $B = \{b_1, \cdots, b_n\} \subseteq \mathbb{K}/\mathbb{F}$. We say that a is algebraically dependent on B (over $\mathbb{F}$) if a is algebraic over $\mathbb{F}(b_1, \cdots, b_n)$. 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. For more details, see lemmas (10) and (11).

The next two lemmas' proofs are inspired by those in [3, p. 213].

Lemma 4. *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 dimensional over $\mathbb{F}$ and $\mathbb{F}(b)$ respectively (because b is algebraic over $\mathbb{F}$ and a is algebraic over $\mathbb{F}(b)$). It follows that $\mathbb{F}(b)(a)$ is finitely dimensional over $\mathbb{F}$ (this can 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 dimension of $\mathbb{F}(b)(a)$ over $\mathbb{F}$ and let $S = \{a^0 \cdots a^n\}$. 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 $ev_a(f) = 0$. □

Lemma 5. *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 (4).

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

   We recall that b_{n+1} is algebraic on $\mathbb{F}(c_1 \cdots c_k)$ (because B is algebraically dependent on C. We can now apply lemma (4) to obtain that a is algebraic over $\mathbb{F}(c_1 \cdots c_n)$ which is what we wanted to show.

□

We can now state the main theorem of our section, namely that a finite set E inside a field extension $\mathbb{K}/\mathbb{F}$ has a natural matroid structure if we declare the independent sets to be algebraically independet ones.

Theorem 13. *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 bases of our supposed matroid. The part focused on proving lemma (6) is inspired by [2, 214–216], although the proof for lemma (7) will be a lot simpler (no need to involve Zorn's lemma) because we are working in a finite subset.

We start by introducing some useful lemmas:

Lemma 6. *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 $A - B$:

1. If $A - B = \emptyset$ (hence $|A - B| = 0$) then it cannot happen that $x \in A$ and $x \notin B$, in other words $A \subseteq B$ and $|A| \leq |B|$ follows trivially.

2. Assume the statemenet is true for some $p \geq 0$. We will attempt to prove it for $|A - B| = p + 1$. Let $k = |A \cap B| = |A| - p - 1$. Let $a_1 \cdots a_n$ be the elements of A such that $a_1 \cdots a_k$ are all the members of $A \cap B$. Similarly we label the elements of B with $a_1 \cdots a_k, b_{k+1} \cdots b_m$. Our goal is to prove that $m \geq n$.

   As a_{k+1} is not dependent on $\{a_1 \cdots a_k\}$ (the set A is algebraically independent) but is dependent on $B = \{a_1 \cdots a_k, b_{k+1} \cdots b_m\}$ by assumption, there must exist some j with $k+1 \leq j \leq m$

such that a_{k+1} is dependent on $\{a_1 \cdots a_k, b_{k+1} \cdots b_j\}$ but not on $\{a_1 \cdots a_k, b_{k+1} \cdots b_{j-1}\}$. Because a_{k+1} is dependent on $\{a_1 \cdots a_k, b_{k+1} \cdots b_j\}$, we know there exists some polynomial $f \in \mathbb{F}[x_1 \cdots x_{j+1}]$ such that

$$f(a_1 \cdots a_k, b_{k+1} \cdots b_j, X) \neq 0 \qquad \text{and} \qquad f(a_1 \cdots a_k, b_{k+1} \cdots b_j, a_{k+1}) = 0.$$

The first equation means that the single-variable polynomial we get when evaulating the multi-variable polynomial at all variables except the last one with the chosen elements is non-zero.

We can identify $\mathbb{F}[x_1, \cdots, x_{j+1}] = (\mathbb{F}[x_1, \cdots, x_{j-1}, x_{j+1}])[x_j]$, i.e. we are looking it as a polynomial with coefficients in $\mathbb{F}[x_1, \cdots, x_{j-1}, x_{j+1}]$ and variable x_j and write f as

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

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

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

This implies that $f(a_1 \cdots a_k, b_{k+1} \cdots b_{j-1}, X, a_{k+1}) \neq 0$, because we see that one of its coefficients, namely g, is non-zero. Since $f(a_1 \cdots a_k, b_{k+1} \cdots b_j, a_{k+1}) = 0$, we can conclude that b_j is algebraic over $\{a_1, \cdots, a_{k+1}, b_{k+2}, \cdots, b_{j-1}\}$ (because there exists a non-zero polynomial with coefficients in $\mathbb{F}(a_1, \cdots, a_{k+1}, b_{k+2}, \cdots, b_{j-1})$, namely $p = f(a_1 \cdots a_k, b_{k+1} \cdots b_{j-1}, X, a_{k+1})$, such that $p(b_j) = 0$).

We define $B' = B \cup a_{k+1} - b_j$. Having proven in the previous paragraph 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' by definition, since they are included in B'. Hence we have that B is dependent on B'. We recall that A is dependent on B, so we can apply the transitivity of algebraic dependence, that is lemma (5), to conclude that A is dependent on B'. We also notice that, by construction A and B' have $k+1$ elements in common and $|B'| = |B \cup a_{k+1} - b_j| = |B|$. Therefore

$$|A - B'| = |A| - |A \cap B'| = |A| - (k+1) = |A| - (|A| - p - 1 + a) = p,$$

where we used the definition of k in the last equality. Thus we apply the induction hypothesis (A is independent, A dependent on B' and $|A - B'| = p$) to conclude that $|A| \leq |B'| = |B|$. So we have $|A| \leq |B|$ which is what we wanted to show and this concludes the inductive step.

□

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

Lemma 7. *Given some finite subset $E \subseteq \mathbb{K}/\mathbb{F}$, maximally independent subsets (bases) of E have equal cardinality.*

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

Let $A = \{a_1, a_2, \cdots, a_n\}$ and we know that A is maximal. We would like to prove that any $b \in B$ is algebraically dependent on A. If $b \in A \cap B$ then this is true by definition. If $b \in B - A$ then this is true by the maximality of A, which guarantees us that $A \cup b$ is not algebraically independent. This means that there exists non-zero $p \in \mathbb{F}[x_1, \cdots, x_n, x_{n+1}]$ such that $p(a_1, \cdots, n, b) = 0$. Then we identify p as $(\mathbb{F}[x_1, \cdots, x_n])[x_{n+1}]$ to see that we can look at it as polynomial with coefficients in $\mathbb{F}(a_1, \cdots, a_n)$ which evaluates to 0 at b. This precisely means that b is dependent over A what we wanted to show.

Therefore, we can conclude that B is algebraically dependent on A. Furthermore, we recall that B is also independent, which means we can use the lemma (6) to prove that $|A| \geq |B|$. We can apply completely the same argument with the roles of A and B reversed to show that $|B| \geq |A|$, which together with our previous statement shows that $|A| = |B|$, proving the lemma. □

Proof of theorem (13). We will construct the matroid using the basis definition (theorem (5)). We need to first show that at least one exists, and then show that the exchange property holds.

(B1) We consider the partially ordered set $\mathcal{I}$ ordered by inclusion - $(\mathcal{I}, \subseteq)$. We notice that $\emptyset$ is independent (as the only polynomial of 0 variables which can be satisfied by $\emptyset$ is the trivial polynomial). Any finite non-empty partially ordered set has at least one maximal element (see lemma (12)), so a basis exists.

(B2) It now remains to prove the exchange property. That is, given two bases $A, B \subseteq \mathcal{B}$ and some $a \in A - B$, we can find some $b \in B - A$ such that $B - b + a \in \mathcal{B}$. Let $n = |A| = |B|$ (we know the two bases have equal cardinality from lemma (7)). 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 (6) that $|B| \leq |A - a|$, which is equivalent to $n \leq n - 1$, hence a contradiction.

□

8 Dual Matroids

8.1 Introduction to Duality

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 $(E, \mathcal{B})$, or in other words M is a matroid on E with $\mathcal{B}$ as its collection of bases. Then its dual will refer to a 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 $\mathcal{B}^*$. We will then define M^* by the pair of sets $(E, \mathcal{B}^*)$, where $\mathcal{B}^*$ contains the complements of all bases in $\mathcal{B}$. This can be seen more clearly in the following digram:

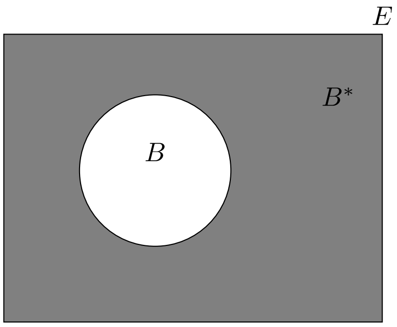


Figure 12: Venn diagram showing a basis $B \in \mathcal{B}(M)$ of M, and a basis $B^* \in \mathcal{B}(M^*)$ of it's dual

We will consider the matroid depicted in previous sections (figure (3)). We also consider it's dual (figure (13)). To the **left** we have the depiction corresponding to the **original matroid**, and to the **right** we have the one corresponding to its **dual matroid**. We notice the ground set is composed of 4 components $E = \{1, 2, 3, 4\}$, and the original matroid has bases 12 and 23 (highlighed in red). Its dual has bases 34 and 14 respectively (also highlighted in red). This is because the complement of the elements 12 is 34, and the complement of 23 is 14.

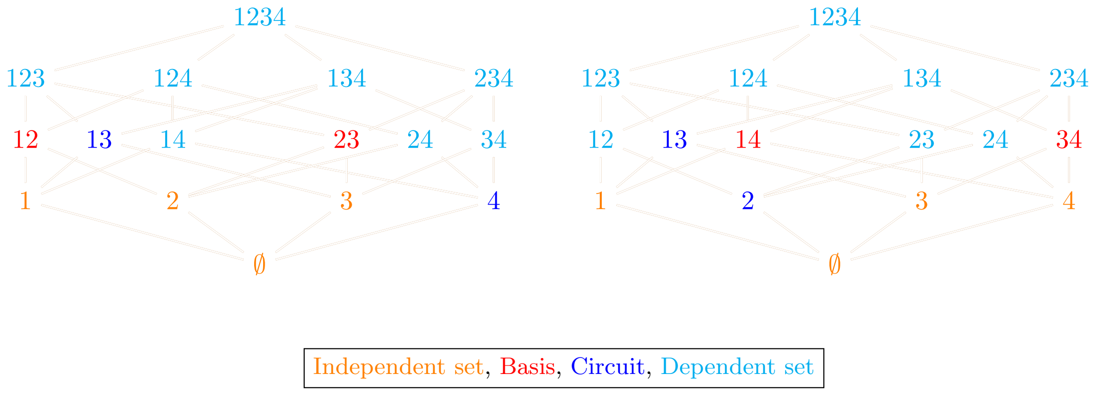


Figure 13: Diagram of a 4-element matroid and its corresponding dual.

We can formalize the definition of $\mathcal{B}^*$ and use it to construct the definition of the dual matroid.

Theorem 14. *Let M be a matroid given by $(E, \mathcal{B})$, and $\mathcal{B}^*(M)$ be $\{E(M) - B | B \in \mathcal{B}(M)\}$. Then $\mathcal{B}^*(M)$ is the set of bases of a matroid on $E(M)$.*

Definition 15. *The matroid that satisfies theroem (14), i.e., whose ground set is $E(M)$ and whose set of basis is $\mathcal{B}^*(M)$, is called the dual of M, and is denoted by M^**

In Theorem (14) we say that $\mathcal{B}^*(M)$ is the set of bases of a matroid on $E(M)$, but this may not be trivially clear, so we need to prove it. However, to prove it we make use of an equivalent property, which we will refer to as (B2)* (The idea to take this approach was motivated by [3, p. 64]). This property comes from our property (B2) in Section 2.2 (theorem (4)).

Lemma 8 ((B2)*)**.** *Let $\mathcal{B}$ be the set of bases of some matroid M. If $B_1, B_2 \in \mathcal{B}$ and $x \in B_2 - B_1$,then there exists an element y of $B_1 - B_2$ such that $(B_1 - y) \cup x \in \mathcal{B}$*

For comparison, the original statement of (B2) is the following:

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

Proof of lemma (8). Assume B_1 and $B_2 \in \mathcal{B}$ and $x \in B_2 - B_1$.

We note that B_1 is by definition a basis. This means that adding any element $x \notin B_1$ to B_1 introduces an unique circuit $C_1 \in \mathcal{C}$ (if this circuit is not unique, and some other circuit C_2 exists, we can apply (C3) to create a circuit $C_3 \subseteq (C_1 \cup C_2) - x \subseteq B_1$, which would be a contradiction). Since C_1 is dependent and B_2 is independent, then $C_1 - B_2$ will be non-empty (otherwise we would have $C_1 - B_2 = \emptyset$ which implies that $C_1 \subseteq B_2$, which is a contradiction, as independent sets cannot contain dependent sets). This implies that there exists an element y such that $y \in C_1 - B_2$, but as C_1 is the circuit created from $B_1 \cup x$, then $y \in (B_1 \cup x) - B_2$. Similarly, as $x \neq y$ (because $x \in B_2$ and $y \notin B_2$), then $y \in B_1 - B_2$.

Consider the set $B_1 - y$. This will not be a basis (because all bases have equal cardinality), but it will be an independent set (implied by (I2)). We notice that $(B_1 - y) \cup x$ will clearly not contain the circuit C_1, since $y \in C_1$ and $y \notin (B_1 - y) \cup x$. Furthermore, this set cannot contain any other distinct circuit $C_2 \in \mathcal{C}$, because that would imply $C_2 \subseteq B_1 \cup x$, which would contradict the uniqueness of C_1. We can now conclude that the set $(B_1 - y) \cup x$ must be independent. We observe that $(B_1 - y) \cup x$ implies that we add an element to the set, and we take out one element of the set, so the cardinality will remain equal, that is: $|(B_1 - y) \cup x| = |B_1|$.

As $(B_1 - y) \cup x$ is independent and has the same cardinality as the basis B_1, then by definition $(B_1 - y) \cup x$ is also a basis. □

Now, using the equivalent property $(B2)^*$ that we have just proven, we prove theorem (14).

Proof of (14). As $\mathcal{B}(M)$ is non-empty, $\mathcal{B}^*(M)$ is non-empty, hence, the property (B_1) holds for $\mathcal{B}^*(M)$. Consider two distinct members $B_1^*, B_2^* \in \mathcal{B}^*(M)$, 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 $B_1 - B_2 = B_2^* - B_1^*$, so this is the same as saying that there exists an element $y \in B_2^* - B_1^*$ such that $(B_1 - y) \cup x$ is a base of M. As a result, by definition of the dual, $E - ((B_1 - y) \cup x) \in \mathcal{B}^*(M)$. But, $E - ((B_1 - y) \cup x) = ((E - B_1) - x) \cup y) = (B_1^* - x) \cup y$, which is in the family $\mathcal{B}^*$. Therefore, we can conclude that $B^*(M)$ satisfes $(B2)$. As $\mathcal{B}^*(M)$ satisfies properties $(B1)$ and $(B2)$, this is indeed the set of bases of a matroid on E. □

Note that, by the way the dual matroid is defined, and and by the intuition provided in the proof above, we see that $\mathcal{B}(M^*) = \mathcal{B}^*(M)$. Furthermore, we have the following lemma:

Lemma 9. *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. In other words:

$$E - (E - B) = B.$$

Example 8.1. Let $U_{k,n}$, be a uniform matroid. We know that its bases will be all the k-element subsets of $E(U_{k,n})$. We also know, by definition (6), that this matroid is defined over a set of n elements, and its basis has exactly k elements. Therefore, the bases of $U_{k,n}{}^*$ are 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

$$U^*_{k,n} = U_{n-k,n}.$$

Now that we have introduced the notion of duals, it is useful to provide 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* (see definition (12)) are called *cohyperplanes*, and the *spanning sets* (see definition (12)) are called *cospanning sets* of M and so on. This leads us to some elementary relationships between these sets.

Theorem 15. *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.*

Proof. Let us prove theorem (15). All of the proofs follow directly from the definitions.

1. $\Longrightarrow$ Suppose X is independent. This means there exists a basis $B \in \mathcal{B}(M)$ so that $X \subseteq B$. Because $X \subseteq B \subseteq E$ and the operation of taking complements is "inclusion reversing" we have $E - B \subseteq E - X$. Verifying directly, if $x \in E - B$ this means $x \in E$ and $x \notin B$. Because $X \subseteq B$ 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 definition.

   $\Longleftarrow$ 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 analogous reasoning as for the forward direction $E - B \subseteq E - X$ implies $X \subseteq B$. 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 an independent set as well, we are done.

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

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

3. $\Longrightarrow$ 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 $B_y \subseteq X \cup y$. 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.

   $\Longleftarrow$ Conversly, if $E - X$ is a cocircuit, 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.

4. The proof is completely analogous to the previous ones. □

Similar to 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, as well as the fact that a matroid and its dual have the same ground set, we have the following

Theorem 16. *The following equality holds* $r(M) + r^*(M) = |E(M)| = |E(M^*)|$.

In fact, we can generalize the above theorem to obtain an explicit formula for the *corank function* of the matroid.

Theorem 17. *For all subsets* $X \subseteq E(M)$ *of some matroid* M*, we have:*

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

Proof of theorem (17). Let $I^* \subseteq X$ be an independent subset of X in M^*, such that it is not a subset of some other set in X. That is, $r^*(X) = |I^*|$. Similarly, let I be an independent subset of $E - X$ in M, such that it is not a subset of some other set in $E - X$. That is, $r(E - X) = |I|$. 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, these 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 basis of M. Let $B^* = E - B$. Since B is a basis of M, then B^* is also a basis of M^*. We observe 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

$$|X| = |X \cap B| + |X \cap B^*| = |B| - |I| + |I^*| = r(M) - r(E - X) + r^*(X).$$

□

8.2 Duals of Representable Matroids

Let $A \in \mathrm{Mat}_{m\times n}(\mathbb{F})$, and let M be a vector matroid $M[A]$ of A. The ground set of M is then the set E of column labels of A. Note that, in general, $M[A]$ does not uniquely determine A. Furthermore, M remains unchanged if we perform any of the following operations on A, which includes the *elementary row operations* [3, p. 77].

1. Interchange two rows.

2. Multiply a row by a non-zero member of $\mathbb{F}$.

3. Replace a row by the sum of that row with another row.

4. Add 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 that when constructing the matroid M from a matrix A, we only care about the independence (or dependence) between column vectors in the matrix. As long as the independence and dependence between them is kept the same, the exact values inside the columns are not relevant.

Assume that A is non-zero. It is easy to prove that by using the previously mentioned operations, A can be reduced to be of the form $[I_r|D]$, where I_r is the $r \times r$ identity matrix ($1 \leq r < n$) and D is some $r \times (n-r)$ matrix over $\mathbb{F}$. This is because using the *elementary row operations* we can reduce the matrix A to its *reduced row echelon form* and then using the remaining operations we can remove any zero row (operation 4.) and interchange any columns to make sure is in the desired from (operation 5.). We also can clearly see that $r(M) = r$ (the dimension for the identity matrix).

Suppose the columns of $[I_r|D]$ are labelled as $e_1, e_2, \cdots, e_n$. We then have the ground set $E = \{e_1, e_2, \cdots, e_n\}$. Let, $\{e_1, e_2, \cdots, e_r\}$ be a basis B of M. We also label the rows and columns of the submatrix D in the following form:

- We label the rows from top to bottom as $e_1, e_2, \cdots, e_r$.

- We label the columns as left to right $e_{r+1}, e_{r+2}, \cdots, e_n$.

This way to represent $M[A]$ can be seen more clearly in figure (14). We will refer to both $[I_r|D]$ and D as the *standard representative matrices* for M, *with respect to* $\{e_1, e_2, \cdots, e_r\}$. Similarly, we use *reduced standard representative matrix* if we want to refer only to D.

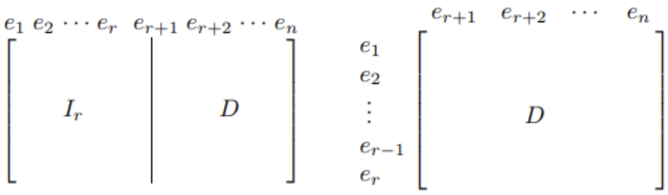

e_1 e_2 $\cdots$ e_r e_{r+1} e_{r+2} $\cdots$ e_n
I_r
D
e_{r+1} e_{r+2} $\cdots$ e_n
e_1
e_2
$\vdots$
e_{r-1}
e_r
D

Figure 14: Standard representative matrices for M (Taken from [3, p. 78]).

Note that in the matrix $[I_r|D]$ from figure (14), only the columns are labelled, but in D, both the rows and columns ae labelled. Also note that, for the basis $B = \{e_1, e_2, \cdots, e_r\}$ of M defined in figure (14), the columns correspond to the columns of the identity matrix.

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

Theorem 18. *Let M be the vector matroid of the matrix $[I_r|D]$ where the columns are labelled, in order $e_1, e_2, \cdots, e_n$ and $1 \leq r < n$. Then M^* is the vector matroid of $[-D^T|I_{n-r}]$, where its columns are also labelled $e_1, e_2, \cdots, e_n$ in that order.*

The following proof was inspired by that in [3, p. 78].

Proof. We assume that $[I_r|D]$ is as in the contruction of the theorem above. Then $[-D^T|I_{n-r}]$ is as shown in figure (15).

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

Figure 15: Standart representative form of the dual of a matroid as established in theorem (18) ((Taken from [3, p. 78]).

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 rearrange the columns of $[-D^T|I_{n-r}]$, such that $B = \{e_1, \cdots, e_s, e_{r+1}, \cdots, e_{r+(r-s)}\}$, for some $s \leq r$. This is possible because we know that it does not affect the corresponding matroid since we are only doing the elementary row operations. Therefore the only change it bring to rearrange rows and columns of $[I_r|D]$ is the rearrange 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

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

We will analyze the way $[I_r|D]$ is partitioned. Here, we make the partitioning such that the first component I_s has columns $(e_1 \cdots e_s)$, the component I_{r-s} has columns $(e_{s+1} \cdots e_r)$, the components D_{11} and D_{21} have columns $(e_{r+1} \cdots e_{2r-s})$, and finally, D_{12} and D_{22} have columns $(e_{(2r-s)+1} \cdots e_n)$.

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 we take the components in the partition that contain the column components in the basis, we get the following matrix

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

As this matrix has the partition components that contain all the elements in the basis, it must have a *rank* of r (the *rank* of $[I_r|D]$). Here $r(I_s) = s$, as it is the identity matrix, hence $r(D_{21}) = r-s$, which also corresponds to the rank of $-D_2 1^T$.

If we now observe the partition of $[-D^T|I_{n-r}]$, this will give 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 $(e_1 \cdots e_s)$. The components $-D_{22}^T$ and $-D_{21}^T$ have columns $(e_{s+1} \cdots e_r)$, the component I_{r-s} has columns $(e_{r+1} \cdots e_{2r-s})$. And finally, $I_{n-(2r-s)}$ has columns $(e_{(2r-s)+1} \cdots e_n)$.

As this time we are dealing with the dual, instead of taking the components that contain the elements in the basis like before, we take the components in the partition of $[-D^T|I_{n-r}]$ that contain the complement of the elements in the basis. Therefore, we obtain the matrix

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

The rank of this submatrix is the sum of the ranks of $I_{n-(2r-s)}$ and $-D_{21}^T$. We have previously stated that the rank of $-D_{21}^T$ is the same as the one of D_{21}. That is, $r(-D_{21}^T) = r - s$, and the *rank* of $I_{n-(2r-s)}$ is $n - (2r - s)$, which means the total rank is

$$(r - s) + (n - (2r - s)) = r - s + n - 2r + s = n - r.$$

This implies 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 the dual, whose basis B^* must satisfy $|B^*| = n - r$, 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 $[-D^T|I_{n-r}]$ is used instead of $[D^T|I_{n-r}]$. However, it is important to remark that this does not bring any issues, because the use of *elementary row operations* does not affect the matroid of a matrix.

A remarkable result follows almost directly from theorem (18):

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

Proof. Let us prove the Corollary above. Suppose we have a matroid M with rank m. That is, the bases of M have size m. Then, by assumption, we can say (without loss of generality) that M can be represented by some $m \times n$ matrix H (with $1 \leq n < m$), such that $H = [I_m|D_{m\times(n-m)}]$ over $\mathbb{F}$. By theorem (18), its dual is then represented by

$$H^* = [-D^T|I_{(n-m)\times(n-m)}] = [-D_{(n-m)\times m}|I_{(n-m)}],$$

which is also a matrix over $\mathbb{F}$, hence by definition, the dual M^* is also representable over $\mathbb{F}$. □

Example 8.2. Consider the vector matroid M with the following representation over $\mathbb{R}$

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

Then, by theorem (18), 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 an interesting note, the vector matroid M with matrix representation A is associated to the graph K_4. In other words, this means that the matrix A and the graph K_4 (figure (16)) produce the same matroid.

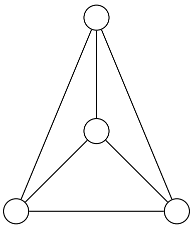


Figure 16: K_4, the complete graph on 4 vertices.

Additionally, we can also verify the *rank* and *corank* propositions established before (theorem (16)). That is, we can clearly observe that A has a ground set $E = \{e_1, e_2, \cdots, e_6\}$ with 6 elements, where each $e_i; i = 1, 2, \cdots, 6$ 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 $r(A^*) = 3$ as well. We conclude that

$$r(A) + r(A^*) = 3 + 3 = 6 = |E|.$$

8.3 Dual of Graphic Matroids

We have studied many concepts related to dual matroids, including some representations for vector matroids. We have however not gone into detail with regard to graphic matroids. We then pose the question — *"Is it possible to have a graphic matroid whose dual is not graphic?"*

To answer this question, we have the following theorem.

Theorem 19. *The dual of a graphic matroid is itself graphic if and only if the underlying graph is planar.*

The proof for this theorem is outside the scope of this article. A proof can be found in [3, p. 140, section 5.2].

Example 8.3. Let us consider the bipartite graph $K_{3,3}$.

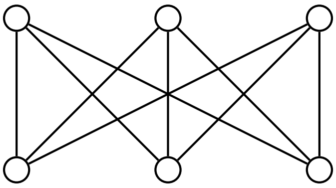


Figure 17: The bipartite graph $K_{3,3}$

This graph has 9 edges, which means it has $E = \{1, 2, 3, \cdots, 9\}$ as its ground set. 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 the case because labelling the columns of J as $E = \{e_1, \cdots, e_9\}$ and defining a matroid $M(J)$ on E, lets us associate each column of J to the correspondingly labeled edge in $K_{3,3}$ and we can directly verify that they represent the same matroid (the matroids are isomorphic). Moreover, this means that we can take a basis for the column space of J, such as $B = \{e_1, e_2, e_3, e_4, e_5\}$, that corresponds to a spanning tree T of $K_{3,3}$ (see figure (18)). In other words, this means that adding any other column to J yields a linear dependency (more precisely, a circuit in $M(J)$), and adding any edge to T generates a cycle.

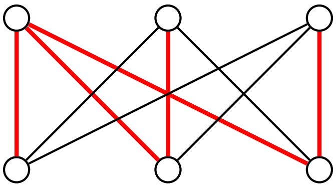


Figure 18: Graph $K_{3,3}$, showing in red an example of edges that form a spanning tree, that can be associated accordingly to the basis of J.

Now that we have show that $K_{3,3}$ has an associated matrix, which produces the same matroid, we can use theorem (18) to obtain the corresponding dual:

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

As a sanity check, we can see that $r(J) = 5$, $r^*(J) = 4$, and $|E(M)| = 9$. We then notice the following does indeed hold:

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

According to 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, 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 independent subsets of vector spaces. We then proceeded by showing the description in terms of maximal independent sets - bases. Afterward we moved to circuits and how they can, in one hand, be interpreted as minimal dependent, or on the other, as object naturally abstracting graphic cycles. We then moved on to more intricate objects, which described the matroid by assigning 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 function. Lastly, we introduced the concept of flat. Along the way, we proved the cryptomorphism - that is, that the matroid can be described starting many different viewpoints. 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. With all of this, we achieved our objective of answering our guiding question - **how can we define matroids?** As our last illustration of matroids we turned away from cryptomorphisms and defined the concept of a matroid dual which had many interesting new properties, and also extended the existing ones, such as it was the case with the corank function, coindependent sets, cobases and cocircuits. Finally, we showed that it is possible for the dual of a graphic matroid to 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, 2011.

10 Appendices

A Fields

This section provides a basic introduction to working with fields. For a more formal in depth treatment of the topic, check [2].

Definition 16 (Fields)**.** *Intuitively, a field is a triplet consisting of a set and two binary operations, which are usually referred to as addition and multiplication. Both these operations are associative, commutative, and have identity elements (usually referred to as* 0 *and* 1 *respectively). All elements have inverse elements for addition. Similarly, all non-zero elements have inverses for multiplication. Furthermore, the two operations obey distributivity laws.*

Definition 17 (Subfields)**.** *Intuitively, given a field* $\mathbb{K}$*, a subfield is a subset* $\mathbb{F} \subseteq \mathbb{K}$ *together with restrictions of addition and multiplication to* $\mathbb{F}$*. Formally, the following three properties must hold:*

1. *We have* $1 \in \mathbb{F}$*.*
2. *If* $a, b \in \mathbb{F}$ *then* $a - b \in \mathbb{F}$*.*
3. *If* $a, b \in \mathbb{F}$ *and* $b \neq 0$ *then* $ab^{-1} \in \mathbb{F}$

Definition 18 (Algebraic elements)**.** *Given a field* $\mathbb{K}$ *and a subfield* $\mathbb{F}$*, an element* $a \in \mathbb{K}$ *is said to be algebraic over* $\mathbb{F}$ *if there exists a non-zero polynomial* f *with coefficients in* $\mathbb{F}$ *such that* $f(a) = 0$*. Elements which are not algebraic are said to be transcendental.*

Throughout the section on algebraic matroids we use the notation $\mathbb{F}[X_1 \cdots X_n]$ to refer to the set of polynomials with n variables and coefficients in some field $\mathbb{F}$. This set presents a ring structure, but understanding that is not necessary for understanding this article. A more in depth treatment of polynomial rings can be found in [2].

Definition 19 (Adjoining elements to a field)**.** *Given a field* $\mathbb{F}$ *and some element* e*, we can construct a new field* $\mathbb{F}(e)$ *with elements of the form:*

$$\frac{\sum a_i e^i}{\sum b_i e^i},$$

where $a_i, b_i \in \mathbb{F}$*.*

Furthermore, we will use the notation $\mathbb{F}(a_1, \cdots, a_n)$ *to refer to* $\boldsymbol{F}(a_1) \cdots (a_n)$*.*

Example A.1. Consider the field $\mathbb{Q}$ and the element $\sqrt{3}$. We notice that

$$(\sqrt{3})^{2k} = 3^k \qquad \text{and} \qquad (\sqrt{3})^{2k+1} = 3^k\sqrt{3}.$$

This let us rewrite the form the elements are introduced in by definition (19) as

$$\begin{aligned}
\frac{\sum a_i(\sqrt{3})^i}{\sum b_i(\sqrt{3})^i} &= \frac{\sum a_{2i}3^i + \sum a_{2i+1}3^i\sqrt{3}}{\sum b_{2i}3^i + \sum b_{2i+1}3^i\sqrt{3}} \\
&= \frac{a + b\sqrt{3}}{c + d\sqrt{3}} \\
&= \frac{(a + b\sqrt{3})(c - d\sqrt{3})}{(c + d\sqrt{3})(c - d\sqrt{3})} \\
&= \frac{(ac - 3bd) + (bc - da)\sqrt{3}}{c^2 - 3d^2} \\
&= \frac{ac - 3bd}{c^2 - 3d^2} + \frac{bc - da}{c^2 - 3d^2}\sqrt{3},
\end{aligned}$$

where the second equality follows by choosing rationals $a, b, c, d \in \mathbb{Q}$ defined as

$$a = \sum a_{2i}3^i \qquad b = \sum a_{2i+1}3^i \qquad c = \sum b_{2i}3^i \qquad d = \sum b_{2i+1}3^i$$

We can now define $p = \frac{ac-3bd}{c^2-3d^2}$ and $q = \frac{bc-da}{c^2-3d^2}$ to show that all elements of $\mathbb{Q}(\sqrt{3})$ are of the form $p + q\sqrt{3}$. Moreover, it follows trivially from definition (19) that all elements of the form $p + q\sqrt{3}$ are elements of $\mathbb{Q}(\sqrt{3})$. Let $\mathbb{F} = \{p + q\sqrt{3} \mid p, q \in \mathbb{Q}\}$ Having proven both

$$\mathbb{F} \subseteq \mathbb{Q}(\sqrt{3}) \qquad \text{and} \qquad \mathbb{F} \supseteq \mathbb{Q}(\sqrt{3}),$$

we can conclude that $\mathbb{Q}(\sqrt{3}) = \mathbb{F}$.

Addition will then be performed component-wise, i.e.

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3}.$$

Multiplication is a bit more involved:

$$(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}.$$

We will now prove that $\mathbb{Q}(\sqrt{3})$ is indeed a field, as stipulated by the definition. Associativity, commutativity, and distributivity follow by direct computation. Similarly, 0 and 1 are both of the form $p + q\sqrt{3}$, so both additive and multiplicative identities exist ($a + 0 = a$ and $a \cdot 1 = a$ can also be checked by direct computation). Furthermore, for any $p + q\sqrt{3}$ we have $-p - q\sqrt{3}$ such that

$$p + q\sqrt{3} + (-p - q\sqrt{3}) = (p - p) + (q - q)\sqrt{3} = 0.$$

Similarly, if $p, q \neq 0$ we notice that $p^2 - 3q^2 = 0$ holds only if $p = q\sqrt{3}$, but this is never the case since $p, q \in \mathbb{Q}$. We construct $\frac{p}{p^2-3q^2} - \frac{q}{p^2-3q^2}\sqrt{3}$ such that

$$\begin{aligned}(p+q\sqrt{3})\left(\frac{p}{p^2-3q^2} - \frac{q}{p^2-3q^2}\sqrt{3}\right) &= \frac{p^2}{p^2-3q^2} - \frac{pq}{p^2-3q^2}\sqrt{3} + \frac{pq}{p^2-3q^2}\sqrt{3} - 3\frac{q^2}{p^2-3q^2} \\ &= \frac{p^2-3q^2}{p^2-3q^2} \\ &= 1.\end{aligned}$$

We can now conclude that all elements have additive inverses, and that all non-zero elements have multiplicative inverses. This, together with the previously proven properties, let us conclude that $\mathbb{Q}(\sqrt{3})$ is indeed a field.

Definition 20 (Field extensions)**.** *Given a field $\mathbb{K}$ and a subfield $\mathbb{F}$, the field $\mathbb{K}$ is said to be a field extension of $\mathbb{F}$.*

Lemma 10 (Vector space structure of field extensions)**.** *Given a field $\mathbb{F}$ and a field extension $\mathbb{K}$, we can construct a vector space with elements of $\mathbb{F}$ as scalars, elements of $\mathbb{K}$ as vectors:*

- *vector addition (together with its identity element and inverse) is defined the same way as addition in $\mathbb{K}$.*
- *scalar-vector multiplication (together with its identity element and inverse) is defined the same way as multiplication in $\mathbb{K}$ (because all scalars are also vectors, since elements of $\mathbb{F}$ are also elements of $\mathbb{K}$).*
- *scalar-scalar multiplication (together with its identity element and inverse) is defined the same way as multiplication in $\mathbb{F}$.*

Lemma 11. *Given a field $\mathbb{K}$ and a subfield $\mathbb{F}$, with some $a \in \mathbb{K}$ algebraic over $\mathbb{F}$, the vector space induced by $\mathbb{F}(a)$ over $\mathbb{F}$ will be finite-dimenssional.*

Proving the above lemma is outside the scope of this article, but a proof can be found in [2].

Example A.2. We will study the vector space induced by $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$. We recall from example (A.1) that elements of $\mathbb{Q}(\sqrt{3})$ are of the form $p + q\sqrt{3}$ where $p, q \in \mathbb{Q}$. We notice that $B = \{1, \sqrt{3}\}$ forms a basis for the vector space induced by $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$. It's clear that span $B = \mathbb{Q}(\sqrt{3})$ (because for any $v = p + q\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ we can pick scalars $p, q \in \mathbb{Q}$ such that $p \cdot 1 + q \cdot \sqrt{3} = v$).

It remains to show that 1 and $\sqrt{3}$ are linearly independent. Assume this is not the case. We now have non-zero $p, q \in \mathbb{Q}$ such that $p + q\sqrt{3} = 0$. If $q = 0$ then $p = 0$, hence a contradiction. Some simple algebraic manipulations then imply that $\sqrt{3} = \frac{p}{-q}$, but $\frac{p}{-q} \in \mathbb{Q}$ and $\sqrt{3} \notin \mathbb{Q}$, hence another contradiction.

B Partially ordered sets

Definition 21 (Partially ordered set)**.** *A partially ordered set is a pair containing a set S and a partial order $\leq$. A partial order is a binary relation on S with the following properties:*

- *For all $x \in S$ we have $x \leq x$ (reflexivity)*
- *For all $a, b \in S$ if $a \leq b$ and $b \leq a$ then $a = b$ (anti-symmetry)*
- *For all $a, b, c \in S$, if $a \leq b$ and $b \leq c$ then $a \leq c$ (transitivity)*

Example B.1. Given a set U, inclusion induces a partial order $(S, \subseteq)$ on any subset $S \subseteq 2^U$. All three properties follow directly from the definition of $\subseteq$.

Definition 22 (Maximal elements)**.** *Given a partially ordered set $(S, \leq)$ an element $M \in S$ is said to be maximal if for all $c \in S$ such that $c \leq M$ we have $c = M$.*

Example B.2. Consider the partially ordered set induced by $\subseteq$ on the subsets of $U = \{1, 2, 3\}$. It can be checked by cases that $\{1, 2, 3\}$ is the only maximal element on $(2^U, \subseteq)$.

Remark 1. Given a partially ordered set $(U, \leq)$ and a subset $S \subseteq U$, we can define a new partially ordered set $(S, \leq)$ by restricting $\leq$ to S.

Example B.3. Consider the partially ordered set introduced in example (B.2). We can remove $\{1, 2, 3\}$ to form a new partially ordered set $(S, \subseteq)$ where $S = 2^U - \{1, 2, 3\}$. We now have multiple maximal elements - they are $\{1, 2\}, \{1, 3\}$ and $\{2, 3\}$.

Lemma 12. *Every non-empty finite partially ordered set $(S, \leq)$ has at least one maximal element.*

Proof. We will prove the statement by induction on the size of S:

- If $S = \{e\}$ then e is a maximal element.
- Assume the statement holds for all sets S such that $|S| = n$. We will attempt to prove it holds for $|S| = n + 1$ as well.

  Consider some arbitrary $s \in S$. By the induction hypothesis, $(S - s, \leq)$ (see remark (1)) has a maximal element M. We will proceed by cases:

  1. If M is also a maximal element for $(S, \leq)$, we are done.
  2. Otherwise, there must exist some $c \in S - M$ such that $M \leq c$. If $c \in S - s$ we have a contradiction (because M wouldn't be a valid maximal element for $(S - s, \leq)$). It then follows that $c = s$.

     We claim that c is a maximal element. Consider $d \in S$ satisfying $c \leq d$. If $d = c$ we are done. Otherwise, $d \in S - s$, so $d \leq M$ (M is maximal for $(S - s, \leq)$), and by transitivity with $M \leq c$ we have $d \leq c$, which by anti-symmetry implies $d = c$.

□