Matroid Theory

Alec Zabel-Mena
Text - Oxley, James, Matroid Theory [1]

30.07.2022

Chapter 1

Fundamental Definitions and Examples.

The goal of matroid theory is to provide an abstract theory of independence. Matroids have their roots in algebra (especially linear algebra), graph theory, and combinatorics; and each field provides a distinct flavor to the subject. The notion of independence was first covere by Whitney in 1935, and then Van der Waerden, in 1937, in his seminal work "Moderne Algebra". Gian Carlo Rota would also stumble upon the theory indepednetly. Pioneering work would later be done by Tutte, Nakasawa, Birkhoff, and Mac Lane.

Perhaps the most important aspect of matroids is that they have several equivalent definitions. We begin by studying two of them.

1.1 The Independence and Circuit Axioms.

Definition. A **matroid** M, on a finite set E, called the **ground set** is a pair $(E,\mathcal{I})$ where $\mathcal{I} \subseteq 2^E$ is a collection of **independent sets**, such that:

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

(I2) If $I_1 \in \mathcal{I}$, and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$.

(I3) If $I_1, I_2 \in \mathcal{I}$, and $|I_1| < |I_2|$, then there exists an $e \in I_2 \backslash I_1$ such that $I_1 \cup e \in \mathcal{I}$.

We call properties (I2) and (I3) the **inheretence** and **augmentation** axioms, respectively.

> **Example 1.1.** The emptyset $\emptyset$ together with $2^{\emptyset} = \{\emptyset\}$ forms a matroid called the **empty matroid** and the collection 2^E on an nonempty set E induces a matroid called the **trivial matroid**. It is easy to see why these two are matroids; since one encompasses only the empty set, and the other all subsets, these two matroids are not very interesting.

We provide some equivalent definitions with independent sets.

Example 1.2. (1) Let E be a finite set. Then $M = (E,\mathcal{I})$ is a matroid if, and only if:

(I′1) $\mathcal{I} \neq \emptyset$.

(I′2) Inheritance holds.

(I′3) If $I_1, I_2 \in \mathcal{I}$, with $|I_2| = |I_1| + 1$, then there is an $e \in I_2 \backslash I_1$ such that $I_1 \cup e \in \mathcal{I}$.

Notice, that if M is a matroid, then $\emptyset \in \mathcal{I}$, so (1) is satisfied. Moreover, the augmentation theorem implies (3), since if $|I_2| = |I_1| + 1$, we have $|I_1| < |I_2|$.

On the otherhand, if $\mathcal{I} \neq \emptyset$, then $\mathcal{I}$ contains, at least , since $\mathcal{I} \subseteq 2^E$. (I2) is also given by (2).

Now, if $I_1, I_2 \in \mathcal{I}$ such that $|I_2| = |I_1| + 1$, then $|I_1| < |I_2|$, and it follows from there that (3) implies (I3).

This gives us an equivalent way to define the matroid M, still using independent sets, but with different rules.

(2) A finite set E together with a collection $\mathcal{I} \subseteq 2^E$ is a matroid if, and only if the following hold:

(I″1) $\emptyset \in \mathcal{I}$.

(I″2) Inheritance holds; i.e. if $I \in \mathcal{I}$ and $J \subseteq I$, then $J \in \mathcal{I}$.

(I″3) If $X \subseteq E$, and $I_1, I_2 \in \mathcal{I}$ are maximal such that $I_1, I_2 \subseteq X$ (that is, I_1 and I_2 are maximal sets of the collection $\{I \in \mathcal{I} : I \subseteq X\}$), then $|I_1| = |I_2|$.

It is rather simple to prove (1) and (2), so the nontrivial work goes to showing that property (3) and (I3) are equivalent to each other.

Definition. Let $M = (E, \mathcal{I})$ be a matroid. A subset of E that is not independent, i.e. $X \subseteq E$ with $X \notin \mathcal{I}$ is called a **dependent set**.

the following example shows why Whitney gave the name "matroid" to these structures.

Example 1.3. (1) Consider an $m \times n$ matrix $A \in F^{m \times n}$, where F is a field. Define E to be the set of all column labels of the matrix A, i.e. $A = \{1, \ldots, m\}$ and define $\mathcal{I} \subseteq 2^E$ to be the collection of all multisets of E linearly independent over $F^{m \times n}$ considered as a vector space. Then $M = (E, \mathcal{I})$ is a matroid.

First notice that $\emptyset$ is trivially linearly independent, so $\emptyset \in \mathcal{I}$. Moreover, if $I_1 \in \mathcal{I}$ is linearly independent, and $I_2 \subseteq I_1$, then I_2 is also linearly independent, so $I_2 \in \mathcal{I}$.

Now, let $X, Y \in \mathcal{I}$ be linearly independent with $|X| < |Y|$, and consider the subspace $W \subseteq F^{m \times n}$ spanned by $X \cup Y$; i.e. $\operatorname{span} W = X \cup Y$. then $\dim W \geq |Y|$. Now, suppose tht $X \cup i$ is linearly dependent for all $i \in Y \backslash X$, then $W \subseteq \operatorname{span} X$, thus $\dim W \leq |X| < Y$, which is a contradiction. Thus, there is atleast one $i \in Y \backslash X$ for which $X \cup i \in \mathcal{I}$. This makes M a matroid which we call the **vector matroid** over A, and we denote it $M[A]$.

(2) Let

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

be a 2×5 matrix on $\mathbb{R}$. Then considering the vector matroid over M oveer A, with $E = \{1, 2, 3, 4, 5\}$, we get the independent sets are:

$$\begin{array}{cccc} \{1\} & \{2\} & \{4\} & \{1,2\} \\ \{1,5\} & \{2,4\} & \{2,5\} & \{4,5\} \end{array}$$

The collection of dependent sets are:

$$\begin{array}{cccc} \{3\} & \{1,3\} & \{1,4\} & \{2,3\} \\ \{3,4\} & \{3,5\} & \{1,2,5\} & \{2,4,5\} \end{array}$$

The minimal dependent sets of M on A is:

$$\begin{array}{cccc} \{3\} & \{1,4\} & \{1,2,5\} & \{2,4,5\} \end{array}$$

Remark. Since matroids are a pair of a ground set E and a subset of 2^E we can usually just specify the matroid by E and take the collection of independent sets (or another collection) to be imposed.

Lemma 1.1.1. *Let E be a subset of a vector space V, and let $\mathcal{I}$ be the collection of all linearly independent subsets of E. Then E, together with $\mathcal{I}$ forms a matroid.*

Proof. The proof of example **??**(1) can be repeated. In fact, notice that an $m \times n$ matrix is just a collection of n vectors of length m in F^m. We now prove this for arbitrary vector spaces.

$\emptyset$ is trivially linearly independent, so $\emptyset \in \mathcal{I}$; moreover, if I_1 is a set of linearly independnet vectors, and $I_2 \subseteq I_1$, then I_2 is also linearly independent; so inheritance holds.

Now, let $I_1 = \{v_1, \ldots, v_m\}$, and $I_2 = \{u_1, \ldots, u_n\}$ be linearly independent sets of vectors with $n < m$. Then $|I_2| < |I_1|$, with $u_i = v_i$ possibly equal for some $1 \leq i \leq n$. Then, there exists some $v_j \in I_1 \backslash I_2$ distinct from all other u_i. Now, suppose that $I_2 \cup v_j$ is linearly dependent. Then we have

$$\alpha_1 u_1 + \cdots + \alpha_n u_n + \alpha v_j = 0$$

which implies that $\alpha \neq 0$. So we get:

$$v_j = \alpha^{-1} \alpha_1 u_1 + \cdots + \alpha^{-1} \alpha_n u_n$$

This puts $v_j \in \operatorname{span} I_2$, thus $I_1 \backslash I_2 \subseteq \operatorname{span} I_2$, thus $(I_1 \backslash I_2) \cup I_2 = I_1 \subseteq \operatorname{span} I_2$. This makes $|I_1| < |I_2|$; but $|I_2| < |I_1|$, a contradiction. Therefore $I_2 \cup v_j$ must be linearly independent. This makes E into a matroid. $\square$

Remark. Most notably, if V is a vector space, then V together with the collection of all linearly independent subsets forms a matroid.

Definition. We call a matroid M **vectorial** if its ground set is a subset of a vector space V and the collection of independent sets consist of all linearly independent subsets of V.

Definition. We call a minimal dependent set of a matroid M a **circuit**. If C is a circuit of size $|C| = n$, we call C an n-circuit. We denote the collection of all circuits of M by $\mathcal{C}$.

This definition will also provide us with an alternative definition for a matroid.

Lemma 1.1.2 (The Circuit Axioms.)**.** *The collection $\mathcal{C}$ of circuits of a matroid satisfy the following:*

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

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

(C3) If $C_1, C_2 \in \mathcal{C}$ are distinct, and $z \in C_1 \cap C_2$, then there exists a circuit $C \in \mathcal{C}$ such that $C \subseteq (C_1 \cup C_2) \backslash z$.

Proof. If M is a matroid with $\mathcal{I}$ the collection of independent sets, then $\emptyset \in \mathcal{I}$, by definition, this makes $\emptyset \notin \mathcal{C}$. Moreover, if $C_1, C_2 \in \mathcal{C}$ are circuits, then they are minimally dependent, so if $C_1 \subseteq C_2$, it must be that $C_1 = C_2$, otherwise we would have $C_1 \in \mathcal{I}$, a contradiction.

Now, let $C_1, C_2 \in \mathcal{C}$ be distinct circuits, and let $z \in C_1 \cap C_2$. Now, suppose that $(C_1 \cup C_2) \backslash z$ does not contain a circuit; then $(C_1 \cup C_2) \backslash z \in \mathcal{I}$, Now, by the above, (C2), we have $C_2 \backslash C_1 \neq \emptyset$, so choose an $f \in C_2 \backslash C_1$. By minimality, we have $C_2 \backslash f \in \mathcal{I}$, so choose a maximally independent subset $I C_1 \cup C_2$ such that $C_2 \backslash f \subseteq I$. Then $f \notin I$; and since C_1 is a circuit, for some $g \in C_1$, $g \notin I$, moreover, $g \neq f$. Therefore, we have:

$$|I| \leq |(C_1 \cup C_2) \backslash \{f, g\}| = |C_1 \cup C_2| - 2 \leq |(C_1 \cup C_2) \backslash z| = |C_1 \cup C_2| - 1$$

By the augmentation axiom (I3), let $I_1 = I$, $I_2 = (C_1 \cup C_2) \backslash z$, then we get $I_1 \cup g \in \mathcal{I}$ which contradicts the maximality of I. □

Remark. This just establishes the validity of the circuit axioms for matroids. To actually show that these axioms provide an equivalent definition, we need the following theorem, and its corollary.

Theorem 1.1.3. *Let E be a finite set having $\mathcal{C} \subseteq 2^E$ satisfying (C1)-(C3). Let $\mathcal{I}$ be the collection of all subsets of E which don't contain elements of $\mathcal{C}$; i.e.*

$$\mathcal{I} = \{X \subseteq E : Y \notin \mathcal{C} \text{ given } Y \subseteq X\}$$

Then $\mathcal{I}$ defines the collection of independent sets of a matroid on E.

Proof. Notice that $\emptyset$ contains no subsets of E contained in $\mathcal{C}$, so $\emptyset \in \mathcal{I}$; furthermore, if $I_1 \in \mathcal{I}$ contains no subsets of E contained in $\mathcal{C}$, neither does a subset $I_2 \subseteq I_1$, so $I_2 \in \mathcal{I}$.

Now, let $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$. Suppose for some $e \in I_2 \backslash I_1$, that $I_1 \cup e$ contains a member of $\mathcal{C}$. Now, $I_1 \cup I_2$ containes a set $I_3 \in \mathcal{I}$ with $|I_1| < |I_3|$, moreover, choose I_3 such that $I_1 \backslash I_3$ is minimal; we have $I_1 \backslash I_3 \neq \emptyset$. Now, choose an $e' \in I_1 \backslash I_3$. Then for each $f \in I_3 \backslash I_1$, let $T_f = (I_3 \cup e') \backslash f$. Then $T_f \subseteq I_1 \cup I_3$, and $|I_1 \backslash T_f| < |I_1 \backslash I_3|$. Since we chose

$I_1 \backslash I_3$ minimal, $T_f \notin \mathcal{I}$. So there exists a $C_f \in \mathcal{C}$ such that $C_f \subseteq T_f = (I_3 \cup e')\backslash f$. Then $f \notin C_f$, moreover $e' \in C_f$, for otherwise, $C_f \subseteq I_3$ contradiction the independence of I_3.

Suppose that $g \in I_3\backslash I_1$. If $C_g \cap (I_3\backslash I_1) = \emptyset$, then $C_g \subseteq ((I_1 \cap I_3) \cup e')\backslash g \subseteq I_1$, which cannot happen. So there exists an $h \in C_g \cap (I_3\backslash I_1)$ with $C_g \neq C_h$. Now, $e' \in C_g \cap C_h$, so by (C3), there exists a $C \in \mathcal{C}$ with $C(C_g \cap C_h)\backslash e'$, but both $C_g, C_h \subseteq I_3 \cup e'$, so $C \subseteq I_3$ another contradiction. Therefore, we find that $\mathcal{I}$ imposes a matroid on E. □

Corollary. *E has $\mathcal{C}$ as its collection of circuits.*

Proof. Notice that iof $I \in \mathcal{I}$ is maximal, then for any $e \in E$, $I \cup e$ is dependent. Moreover, since $I \cup e \notin \mathcal{I}$, we see that there is a $C \in \mathcal{C}$ with $C \subseteq I \cup e$. Now, since I is maxiamlly independent, this makes $I \cup e$ minimal, and so $C = I \cup e$. This makes $\mathcal{C}$ the set of circuits of the matroid on E. □

Corollary. *If I is independent in a matroid M, and $e \in E$ such that $I \cup e$ is dependent, then M has a unique circuit contained in $I \cup e$, containing e.*

Proof. By above, we have that $I \cup e$ contains a circuit $C = I \cup e$, so $e \in C$. Now, if $C' \subseteq I \cup e$ is another circuit contained in $I \cup e$, containig e, such that C' is distinct from C, then by (C3), there is another circuit $C'' \in \mathcal{C}$ such that $C'' \subseteq (C \cup C')\backslash e$; a contradiction. So $C' = C$. □

We can now provide an alternative definition.

Definition. A **matroid** M, on a finite set E, is a pair $(E, \mathcal{C})$ where $\mathcal{I} \subseteq 2^E$ is a collection of **circuits** such that

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

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

(C3) If $C_1, C_2 \in \mathcal{C}$ are distinct, and $z \in C_1 \cap C_2$, then there exists a circuit $C \in \mathcal{C}$ such that $C \subseteq (C_1 \cup C_2)\backslash z$.

We call the propery (C3) the **weak circuit elimination axiom**.

Example 1.4. (1) Let G be a graph with vertex set V and edge set E. Let $\mathcal{C}$ be the collection of edge-set defined cycles of G (i.e. all cycles determined by their edges). The $M = (E, \mathcal{C})$ is a matroid on G, with $\mathcal{C}$ the collection of circuits on G.

Notice that $\emptyset$ contains no edges, and hence no cycles, so $\emptyset \notin \mathcal{C}$. Moreover, let C_1, C_2 be cycles of G, then if $C_1 \subseteq C_2$, by definition of a cycle, it must be that $C_1 = C_2$.

Now, let $C_1, C_2 \in \mathcal{C}$ be distinct cycles of G, having a common edge e with endpoints $u, v \in V$; i.e. $e = \{u, v\}$. Now, for $1 \leq i \leq 2$, let P_i be the (u, v)-path with edges in $C_i\backslash e$. Now, walk on P_1 from u to v stoping at the vertex $w \in V$ such that w is the first vertex not in P_2. Then, walk from w to the vertex $x \neq w$ such that x is in P_2. Since P_1 and P_2 terminate at v, such a vertex exists. Now, adjoin P_1 from w to x to P_2 from x to w, and the resultant graph is a cycle contained in $(C_1 \cup C_2)\backslash e$. We call the corresponding matroid the **cycle matroid** of G.

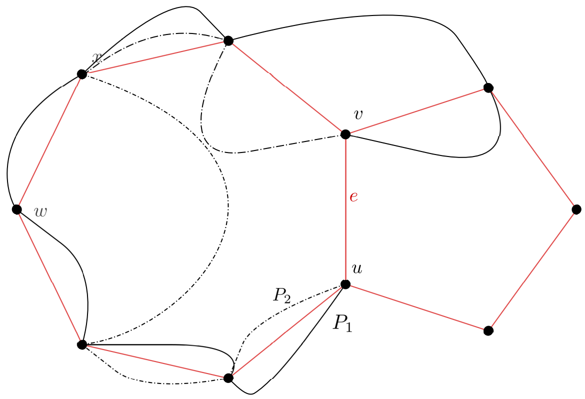


Figure 1.1: The cycle matroid corresponding to the graph G of example 1.2. Path P_1 is indicated by a solid line, and path P_2 indicated by a dotted line.

(2) Consider the graph in figure 1.2, and the cycle matroid M on G. The set of circuits $\mathcal{C}$ is given by the collection:

$$\{e_3\} \qquad \{e_1, e_4\} \qquad \{e_1, e_2, e_5\} \qquad \{e_2, e_4, e_5\}$$

Comparing this with the previous matroid M' on the 2×5 matrix A from example

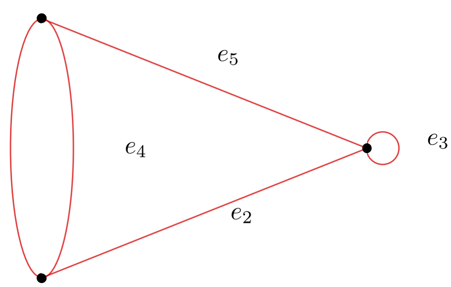


Figure 1.2:

1.1(2). We can see that they have the same structure. Take the map $\psi : i \to e_i$, which is $1-1$ and onto, then a set $X \subseteq E$ is a circuit in M if, and only if it is a circuit in M'.

Example 1.5. Let

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

and let $M_2(A)$ and $M_3(A)$ be the matroids on A over $\mathbb{F}_2$ and $\mathbb{F}_3$, respectively. We can list the set of circuits of $M_2(A)$ to be:

$$\begin{array}{cccc} \{1,2,4\} & \{1,3,5\} & \{2,3,6\} & \{4,5,6\} \\ & \{1,4,3,6\} & \{1,5,2,6\} & \{2,4,3,5\} \end{array}$$

while the set of circuits of $M_3(A)$ is:

$$\begin{array}{ccc} \{1,2,4\} & \{1,3,5\} & \{2,3,6\} \\ \{1,4,3,6\} & \{1,5,2,6\} & \{2,4,3,5\} \end{array}$$

So we can clearly see that the circuits of $M_2(A)$ and $M_3(A)$ are not the same. In fact, $M_2(A)$ ia grpahic while $M_3(A)$ is not. We also see that $M_2(A)$ is $\mathbb{F}_3$-representable, taking $A' = 2A$, while $M_3(A)$ is not $\mathbb{F}_2$ -representable.

The above example leads us to define what we mean by a matroid isomorphism. We present some definitions.

Definition. We call two matroids M_1 and M_2, with ground sets E_1 and E_2, respectively, **isomorphic** if there exists a $1-1$ map $\psi : E_1 \to E_2$ of E_1 onto E_2 such that X is independent in dependent in E if, and only if $\psi(X)$ is independent in E_2. We write $M_1 \simeq M_2$ and call ψ an **isomorphism** of the matroids.

Definition. Let G be a graph with edge set E. We call the matroid on E having $\mathcal{C}$ the collection of all egde-set defined cycles the **cycle matroid** of G. We call a matroid M **graphic** if it is isomorphic to the cycle matroid of some graph.

Definition. We call a matroid F**-representable** if it is isomorphic to some vector matroid over a field F. We call the ground set of the vector matroid a F**-representation**.

Example 1.6. (1) The matroid on the 2×5 matrix $\mathbb{R}$ of example 1.1(2) is $\mathbb{R}$-representable. It is also $\mathbb{F}_2$-representable.

(2) The above matroid is a graphic matroid, isomorphic to the cycle matroid of example 1.2(2); as a consequence, that cycle matroid is also $\mathbb{F}_2$-representable.

(3) Let M_1 and M_2 be isomorphic matroids via a map ψ. Then if $\mathcal{I}$ is the collection of independent sets of M_1, then $\psi(\mathcal{I})$ the collection of independent sets of M_2.

Lemma 1.1.4. *Let M_1 and M_2 be matroids with ground sets E_1 and E_2. If $M_1 \simeq M_2$ via the map ψ, then $C \subseteq E_1$ is a circuit of M_1 if, and only if $\psi(C) \subseteq E_2$ is a circuit of M_2.*

Proof. Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be the independent sets of M_1 and M_2, respectively, and let C be a circuit of M_1. Now, if $\psi(C) \in \mathcal{I}_2$, then by definition, we must have $C \in \mathcal{I}_1$, which contradicts that C is a circuit. Thus $\psi(C)$ must be a dependent set. Now, by definition, C is minimaly dependent, so $C\backslash e \in \mathcal{I}_1$, thus $\psi(C\backslash e) \in \mathcal{I}_2$. Notice, then that $\psi(C)\backslash\psi(e) \subseteq \psi(C\backslash e)$, so by inehritance, $\psi(C)\backslash\psi(e) \in \mathcal{I}_2$. So we have that for $\psi(e) \in E_2$, $\psi(C)\backslash\psi(e)$ is independent, but $\psi(C)$ is dependent. This makes $\psi(C)$ minimally dependent, and thus, by definition, a circuit. □

Corollary. *If $\mathcal{C}_1$ and $\mathcal{C}_2$ are the collection of circuits of M_1 and M_2, respectively, then $\mathcal{C}_2 = \psi(\mathcal{C}_1)$.*

Proof. Take the above lemma together with the fact that ψ is onto. □

Since a matroid is determined by its ground set, there is no loss of generality in refering to the ground set as the matroid itself, implying that we are imposing a collection of independent sets/circuits.

Definition. Let M be a matroid. We call an element $e \in M$ a **loop** if the singleton $\{e\}$ is a circuit of M. We call two elements $f, g \in M$ **parallel** if the doubleton $\{f, g\}$ is a circuit of M and we write $f \| g$. We define a **parallel class** of M to be a maximal subset $X \subseteq M$ with the property that: if $f, g \in X$ distinct, then $f \| g$, and no element of X is a loop. We call a parallel class of M **trivial** if it contains only one element. We call a matroid **simple** if it cntains no loops, nor parallel elements.

Example 1.7. Let $A \in F^{m \times n}$ is an $m \times n$ matrix, and consider the vector matroid o A whose independent sets are linearly independent columns. Since any single nonzero column of A is linearly independent, we have the only loop in the matroid on A is the zero-column $(0 \ldots 0)^T$. Likewise, the parellel elements of the matroid on A are simply the linearly dependent pairs of columns.

Theorem 1.1.5 (The Strong Circuit Elimination Axiom.)**.** *Let M be a matroid with collection of circuits $\mathcal{C}$. If $C_1, C_2 \subseteq \mathcal{C}$ are distinct, such that $e \in C_1 \cap C_2$, and $f \in C_1 \backslash C_2$ then there exists a circuit $C \in \mathcal{C}$ such that $f \in C \subseteq (C_1 \cup C_2) \backslash e$.*

We now introduce one last example of a matroid for this section.

Example 1.8. Consider the following bipartition of the sets $X = \{1, 2, 3\}$ and $Y = \{a, b, c, d, e, f\}$, together with the relation $E = \{(1, a), (2, a), (2, b), (2, c), (3, a), (3, b), (3, a), (3, e), (3, e)\}$. We can represent this as the following bipartite graph, $G = (X \cup Y, E)$ in figure 1.3 Then if

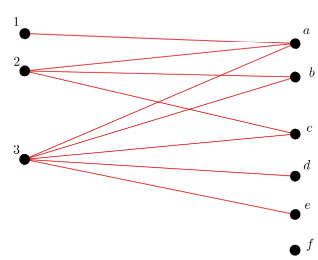


Figure 1.3:

we define those "independent sets" $\mathcal{I}$ consisting of all subsets of Y that can be "matched" to elements of X. i.e. those subsets of Y whose edges between X contain no incident edges. Then Y together with $\mathcal{I}$ forms a matroid.

Definition. Let G be a bipartite graph with bipartition (X, Y). For a subset U of Y, if E is the set of edges on (X, U), then we call E a **matching** between X and U if no two edges in E have a common endpoint. We say that U can be **matched** to X. We say that E is a complete matching if $U = Y$.

Lemma 1.1.6. *Let G be a bipartite graph, with bi-partition (X, Y). Let $\mathcal{I}$ be the collection of all subsets of Y that can be matched to X. Then $M = (Y, \mathcal{I})$ forms a matroid.*

Proof. We have that for $\emptyset \subseteq Y$, there are no two edges on the bipartition $(X, \emptyset)$ with a common endpoint; infact, there are no edges in this bipartition. now suppose that $I \subseteq Y$ can be matched to X, that means no two edges between the bipartition (X, I) has a common endpoint. Now, if $I' \subseteq I$, then it follows that no two edges between (X, I') has a common endpoint. Therefore (I1), and (I2) are satisfied.

Now suppose subsets I and I' of Y can be matched to X, and that $|I| < |I'|$. Then the bipartitions (X, I) and (X, I') have no two edges incident to each other. Then the bipartition $(X, I \cup I')$ have no two edges incident with each other. Now, choose an $e \in I' \backslash I$, then the edge from e to some point in X has no other incident edge, therefore the edges between X and $I \cup e$ have no two edges incident. That is no two edges are incident between $(X, I \cup e)$, therefor (I3) is satisfied. This makes $M = (Y, \mathcal{I})$ into a matroid. □

Remark. Notice that we can make G into a bi-partite graph by taking the set of edges to be all matchings from the set X to subsets of Y. Matroids of this type are called "transversal" and will be studied in more rigor later.

1.2 The Base Axioms.

Definition. We call a maximally independent set of a matroid M a **basis** of M. We denote the collection of all bases of M to be $\mathcal{B}$.

Lemma 1.2.1. *For any two bases B_1 and B_2 of a matroid, we have $|B_1| = |B_2|$.*

Proof. Suppose not, that $|B_1| < |B_2|$. Then, since $B_1, B_2 \in \mathcal{I}$, by augmentation, we can choose $e \in B_2 \backslash B_1$ such that $B_1 \cup e \in \mathcal{I}$. But B_1 is maximal, a contradiction! Terefore, $|B_1| \geq |B_2|$. Similarly, we get $|B_2| \geq |B_1|$. □

Lemma 1.2.2 (The Base Axioms). *The collection $\mathcal{B}$ of bases of a matroid has the following properties:*

(B1) $\mathcal{B} \neq \emptyset$.

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

Proof. For (B1), if $\mathcal{B} = \emptyset$, then necesarrily, $\mathcal{I} = \emptyset$, which cannot happen by (I1).

Now, notice that both $B_1 \backslash x$ and B_2 are independent, and that $|B_1 \backslash x| < |B_2|$ by lemma 1.2.1. Therefore, by augmentation, take $y \in B_2 \backslash (B_1 \backslash x)$, that is, $y \in B_2 \backslash B_1$, such that $(B_1 \backslash x) \cup y \in \mathcal{I}$. Then there is a basis $B' \in \mathcal{B}$ such that $(B_1 \backslash x) \cup y \subseteq B'$. Now, notice that $|(B_1 \backslash x) \cup y| = |B_2| = |B'|$, thus $(B_1 \backslash x) \cup y = B'$, makinng $(B_1 \backslash x) \cup y \in \mathcal{B}$ a basis. □

With this lemma, we have proved that the independence axioms imply the base axiom. We now show that the base axioms imply independence.

Theorem 1.2.3. *Let E be a finite set and $\mathcal{B} \subseteq 2^E$ a collection of subsets of E satisfying (B1) and (B2). let $\mathcal{I} = \{I \subseteq E : I \subseteq B, \text{ where } B \in \mathcal{B}\}$. Then $\mathcal{I}$ induces a matroid on E.*

Proof. If $\mathcal{B} \neq \emptyset$, then we have at least $\emptyset \in \mathcal{I}$. Moreover, if $I_1 \in \mathcal{I}$, then $I_1 \subseteq B$, for some $B \in \mathcal{B}$. Then if $I_2 \subseteq I_1$, $I_2 \subseteq B$ so that $I_2 \in \mathcal{I}$.

Now suppose that $B_1, B_2 \in \mathcal{B}$ with $|B_1| > |B_2|$, such that $|B_1 \backslash B_2|$ is minimal. Notice that $B_1 \backslash B_2 \neq \emptyset$, so choose $x \in B_1 \backslash B_2$. Then by (B2), there exists a $y \in B_2 \backslash B_1$ such that $(B_1 \backslash x) \cup y \in \mathcal{B}$. Notice then that $|(B_1 \backslash x) \cup y| = |B_1| > |B_2|$, so $|((B_1 \backslash x) \cup y \backslash B_2)| < |B_1 \backslash B_2|$ which contradicts minimality. So we have $|B_1| = |B_2|$.

Now suppose that the augmentation axiom, (I3), fails. Then for $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$, there is an $e \in I_2 \backslash I_1$ such that $I_1 \cup e \notin \mathcal{I}$. Now, by definition, there exists $B_1, B_2 \in \mathcal{B}$ with $I_1 \subseteq B_1$ and $I_2 \subseteq B_2$. Choose, then, B_2 such that $|B_2 \backslash (B_1 \cup I_2)|$ is minimal. Then $I_2 \backslash B_1 = I_2 \backslash I_1$. Now, supposing that $B_2 \backslash (B_1 \cup I_2) \neq \emptyset$, choose $x \in B_2 \backslash (B_1 \cup I_2)$. Then by (B2), there exists a $y \in B_1 \backslash B_2$ such that $(B_2 \backslash x) \cup y \in \mathcal{B}$; but then $((B_2 \backslash x) \cup y) \backslash (B_1 \cup I_2) < |B_2 \backslash (B_1 \cup I_2)|$, which contradicts minimality. So $B_2 \backslash (B_1 \cup I_2) = \emptyset$, and so $B_2 \backslash B_1 = I_2 \backslash B_1$; that is:

$$B_2 \backslash B_1 = I_2 \backslash I_1$$

Now suppose that $B_1 \backslash (B_2 \cup I_1) \neq \emptyset$. Then cor $x \in B_1 \backslash B_2 \cup I_1$, there exists $y \in B_2 \backslash B_1$ such that $(B_1 \backslash x) \cup y \in \mathcal{B}$. Now, we have $I_1 \cup y \subseteq (B_1 \backslash x) \cup y$, putting $I_1 \cup e \in \mathcal{I}$. Since $y \in B_2 \backslash B_1$, we have $y \in I_2 \backslash I_1$, which contradicts the hypothesis. So $B_1 \backslash (B_2 \cup I_1) = \emptyset$. Thus, $B_1 \backslash B_2 = I_1 \backslash B_2$. It follows then that $B_1 \backslash B_2 \subseteq I_2 \backslash I_1$. Now, $|B_1| = |B_2|$, so $|B_1 \backslash B_2| = |B_2 \backslash B_1|$, thus $|I_1 \backslash I_2| = |I_2 \backslash I_1|$, so that $|I_1| \geq |I_2|$. but $|I_1| < |I_2|$, a contradiction. Therefore, (I3) must be satisfied, making $(E, \mathcal{I})$ into a matroid. □

Corollary. *The matroid on E induced by $\mathcal{I}$ has $\mathcal{B}$ as its collection of bases.*

We now come to our next equivalent definition of a matroid.

Definition. A **matroid** on a finite set E is a pair $(E, \mathcal{B})$, where $\mathcal{B} \subseteq 2^E$, such that:

(B1) $\mathcal{B} \neq \emptyset$.

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

We call $\mathcal{B}$ the collection of **bases** of the matroid.

Corollary. *For any $B \in \mathcal{B}$ and $e \in E \backslash B$, $B \cup e$ contains a unique circuit $C(e, B)$ which contains e.*

Proof. This follows immediately from the analogous corollary to theorem 1.1.3. □

Definition. Let M be a matroid with ground set E and collection of bases $\mathcal{B}$. For $e \in E \backslash B$, we define the **fundamental circuit** of e with respect to B to be the circuit $C(e, B)$ with the property that $e \in C(e, B) \subseteq B$.

Lemma 1.2.4 (Fundamental Circuit Theorem.)**.** *Every circuit of a matroid is the fundamental circuit of some element with respect to some basis.*

Proof. Let C be a circuit of some matroid M, and choose $e \in C$. Then choose some basis B of M in which $e \in E \backslash B$ (E the ground set of M). Then by the corollary to theorem 1.2.3, we have that there is a circuit $C(e, B)$ such that $e \in C(e, B) \subseteq B \cup e$. We then have that $e \in C \subseteq B \cup e$, and that $e \in C \cap C(e, B)$. Then by weak circuit elimination, there is a circuit $C' \subseteq (C \cup C(e, B)) \backslash e$. Then $C' \subseteq C \backslash e$ and $C' \subseteq C(e, B) \backslash e$. That is $C' \cup e \subseteq C$ and $C' \cup e \subseteq C(e, B)$. Thus, either $C \subseteq C(e, B)$ or $C(e, B) \subseteq C$; in either case we get $C = C(e, B)$. □

Example 1.9. (1) let $m, n \in \mathbb{Z}^+$ with $m \leq n$. Let E be an n-element set, and $\mathcal{B}$ the collection of all m-element subsets of E. Then $\mathcal{B}$ is the collection of bases for a matroid on E.

Notice that since $|E| = n$, and $m \leq n$, then there exists at least on m-element subset of E, so that $\mathcal{B} \neq \emptyset$. Now, let $B_1, B_2 \in \mathcal{B}$ be distinct with $|B_1| = |B_2| = m$. Then for $x \in B_1 \backslash B_2$, notice that $|B_1 \backslash x| = m - 1$. Thus, choose $y \in B_2 \backslash B_1$ (which exists), then $|(B_1 \backslash x) \cup y| = m$, making $B_1 \backslash x \cup y \in \mathcal{B}$. Then $(E, \mathcal{B})$ forms a matroid which we call the **uniform matroid** of rank m on an n-element set. We denote the uniform matroid by $U_{m,n}$.

(2) In the uniform matroid, $U_{m,n}$, we have the collection of independent sets is given by:

$$\mathcal{I} = \{X \subset E : |X| \leq m\}$$

and the collection of circuits is given by $\mathcal{C} = \emptyset$ if $m = n$, or

$$\mathcal{C} = \{X \subseteq E : |X| = m + 1\}.$$

if $m < n$.

(3) If $m = 0$, then the only independent sets of $U_{0,n}$ are emptysets, i.e. $\mathcal{I} = \mathcal{B} = \{\emptyset\}$. This makes all n-elements of the ground set loops. Likewise, if $m = 1$, then the only independent sets of $U_{1,n}$ are singletons, hence $U_{1,m}$ consists of n parallel elements. If $m \geq 2$, then $U_{m,n}$ is simple.

(4) $U_{n,n}$ has no circuits, since by above, $\mathcal{C} = \emptyset$, and $U_{0,0} = \emptyset$ the empty matroid. We call $U_{n,n}$ the **Boolean algebra**.

Definition. We call a matroid M **free** if its collection of circuits is empty.

Example 1.10. (1) Let E be a nonempty set and $(E_1, \ldots, E_r)$ be a partition π of E into nonempty subsets. Let $\mathcal{B}$ be the collection of all suubsets of E containing exactly one element of E_i for each $1 \leq i \leq r$. Then $\mathcal{B}$ is the collection of bases of a matroid on E called the **partition matroid**, M_π.

(2) M_π has as its collection of independent sets, bases, and circuits given by:

$$\begin{aligned}
\mathcal{I} &= \{X \subseteq E : |X \cap E_i| \leq 1, \text{ for all } 1 \leq i \leq r\} \\
\mathcal{B} &= \{X \subseteq E : |X \cap E_i| = 1, \text{ for all } 1 \leq i \leq r\} \\
\mathcal{C} &= \{\{a, b\} \subseteq E : \{a, b\} \subseteq E_i, \text{ for all } 1 \leq i \leq r\}
\end{aligned}$$

(3) If $|E_i| = 1$ for all i, then $M_\pi \simeq U_{r,r}$. In general. we also have that M_π is graphic, as it is isomorphic to the cycle matroid of a vertex-disjoint union of graphs $G_1, \ldots, G_r$ where G_i consists of 2 vertices joined by $|E_i|$ distinct edges.

Example 1.11. (1) Let G be a graph. Then a subset $X \subseteq E$ of edges of G is independent if, and only if they from a forest of the graph G. Then X is a basis if X is a forest such that for $e \in E \backslash X$, $X \cup e$ contains a cycle. That is, X forms a spanning tree in all connected components of G. If G is connected, then X is a spanning tree. Likewise, it can be shown that spanning trees are bases, so that we have that X is the basis of matroid on a graph G if, and onlt if it forms spanning trees across all connected components of G.

(2) Let A be an $m \times n$ matrix over a field F. Then the columns of A span a subspace W of dimension r. We also see that independent sets of columns of A are linearly independent. Thus, if we have a subset of columns of A, linearly independent, also spanning the subspace W, they form a basis of W. That is, a set B of columns of A forms a basis for W if, and only if B is linearly independent, and $|B| = r$; so that B is a set of basis vectors for the subspace W.

(3) If $A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$ is a 2×4 matrix over $\mathbb{F}_3$, then $\dim W = 2$, and so the bases are all 2 element subsets of linearly independnet columns. Thus $M(A) \simeq U_{2,4}$.

(4) Consider the graph G in figure 1.3, we would like to know how many spanning trees this graph has.

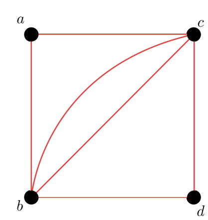


Figure 1.4:

We first form the $|V| \times |V| = 4 \times 4$ matrix L defined as follows:

$$(L_{u,v}) = \begin{cases} \deg v, & \text{if } u = v \\ -|E_{u,v}|, & \text{otherwise} \end{cases}$$

Where $E_{u,v}$ is the set of edges between u and v. We call L the **Laplacian** of G. By Kirchoff's matrix tree theorem combinatorics, the number of spanning trees of G is equal to any cofactor of L, in this case, we have:

$$L = \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & 4 & -2 & -1 \\ -1 & -2 & 4 & -1 \\ 0 & -1 & -1 & 2 \end{pmatrix}$$

Which has a cofactor of 12, and hence there are 12 spanning trees on G. This also means that the cycle matroid on G has 12 bases.

Theorem 1.2.5. *Let M be a graphic matroid. Then M is isomorphic to the cycle matroid of some connected graph G.*

Proof. Let M be a matroid, and dentoe the cycle matroid of any graph G by $M(G)$. Then $M \simeq M(H)$ for some graph H. If H is connected, we are done.

Now suppose that H is not connected. Consider then the connected components $H_1, \ldots, H_n$ of H. Choose a vertex $v_i \in H_i$ and form the graph G with vertices $v_1, \ldots, v_n$ all labeled as one vertex. Then the edge set $E(H) = E(G)$ the edge set of G; moreover, $X \subseteq E(G)$ is a cycle if, and only if it is a cycle in $E(H)$. Thus we have $M \simeq M(H)$. □

To finish the section, we make the following observation. The independence, base, and circuit axioms constitute the three main equivalent ways of definining a matroid. We can denote these definitions as $(\mathcal{I})$, $(\mathcal{B})$, and $(\mathcal{C})$. Now, by theorems 1.1.3 and 1.2.3, we have that $(\mathcal{I})$ is equivalent to $(\mathcal{B})$ and $(\mathcal{C})$. Moreover, notice that $(\mathcal{B})$ implies $(\mathcal{I})$, and $(\mathcal{I})$ implies $(\mathcal{C})$. Thus, by transitivity of implication, $(\mathcal{B})$ implies $(\mathcal{C})$. Conversely, we have that $(\mathcal{C})$ implies $(\mathcal{I})$, which implies $(\mathcal{B})$. So by transitivity again, we get that $(\mathcal{C})$ implies $(\mathcal{B})$. Therefore $(\mathcal{B})$ and $(\mathcal{C})$ are equivalent definitions of a matroid. Collecting our definitions into a digraph, whose edge set is given by implication, we get the following figure:

Remark. That is, two vertices a, b in the digraph form an edge (a, b) if a implies b.

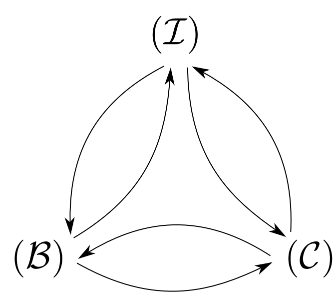


Figure 1.5: The implication digraph of $(\mathcal{I})$, $(\mathcal{B})$, and $(\mathcal{C})$.

1.3 The Rank of a Matroid.

Let $M = (E, \mathcal{I})$ be a matroid, and let $X \subseteq E$, and $\mathcal{I}|X = \{I \subseteq X : I \in \mathcal{I}\}$. Then the pair $(X, \mathcal{I}|X)$ forms a matroid which we can define as follows.

Definition. If $M = (E, \mathcal{I})$ is a matroid, and $X \subseteq E$, then we call the matroid $M|X = (X, \mathcal{I}|X)$ the **restriction** of M to X, or alternatively, the **deletion** of $E \backslash X$ from M.

This also motivates the following definition for the "rank" of a matroid.

Definition. Let $M = (E, \mathcal{I})$ bea matroid, and $X \subseteq E$. We define the **rank** of X to be the cardinality of some basis B of $M|X$, and denote it $\operatorname{rank} X$; we also call B a **basis** of X. We define the **rank function** of the matroid M to be the mapping $\operatorname{rank} : 2^E \to \mathbb{N}$, and we write $\operatorname{rank} M = \operatorname{rank} E$. That is the rank of the matroid M is the rank of its ground set.

Lemma 1.3.1. *Let M be a matroid on a set E, and let $X \subseteq E$. If* rank *is the rank function of M, then the following are true:*

(R1) $0 \leq \operatorname{rank} X \leq |X|$.

(R2) If $Y \subseteq E$ with $X \subseteq Y$, then $\operatorname{rank} X \leq \operatorname{rank} Y$.

(R3) If $X \subseteq E$ and $Y \subseteq E$, then $\operatorname{rank}(X \cup Y) + \operatorname{rank}(X \cap Y) \leq \operatorname{rank} X + \operatorname{rank} Y$.

Proof. Since rank maps a subset of E to a nonnegative integer in $\mathbb{N}$, we see that $\operatorname{rank} X \geq 0$. Now, if B is a basis of X, then $B \subseteq X$, so that $|B| \leq |X|$, so $\operatorname{rank} X \leq |X|$.

Moreover, if $X \subseteq Y$, and B is a basis of X, then it is a basis of the matroid $M|X$, as well as being an independent set of the matroid $M|Y$. So if B' is the basis for Y; i.e. a basis of $M|Y$, then we have $|B| \leq |B'| \leq |Y|$, so that $\operatorname{rank} X \leq \operatorname{rank} Y$

Now, let $B_{X\cap Y}$ be a basis of $X \cap Y$, then it is an independent set in $M|(X \cup Y)$, and hence contained in a basis $B_{X\cup Y}$ of $X \cup Y$. Now, we also have that $B_{X\cup Y} \cap X$ and $B_{X\cup Y} \cap Y$ are independent in $M|X$ and $M|Y$, respectively; So we get that $\operatorname{rank} X \geq |B_{X\cup Y} \cap X|$ and $\operatorname{rank} Y \geq |B_{X\cup Y} \cap Y|$, thus $\operatorname{rank} X + \operatorname{rank} Y \geq |B_{X\cup Y} \cap X| + |B_{X\cup Y} \cap y| = |B_{X\cup Y}| + |B_{X\cap Y}| = \operatorname{rank}(X \cup Y) + \operatorname{rank}(X \cap Y)$. □

Corollary. *For any matroid M on E with $X \subseteq E$ and $x \in E$:*

$$\operatorname{rank} X \leq \operatorname{rank}(X \cup x) \leq \operatorname{rank} X + 1$$

Example 1.12. (1) Let V be a vector space and consider the matroid $M[V]$ on V, the dimension of V is a rank function of $M[V]$ by definition. Moreover, if U and W are subspaces of V, then we can define matroids $M[U]$ and $M[W]$ on U and W, respectively by taking $M[U] = M[V]|U$ and $M[U] = M[W]|W$, morevoer, we also get by a well known theorem of linear algebra that

$$\dim(U + W) + \dim(U \cap W) = \dim U + \dim W$$

(2) Infact, for any representable matroid $M[V]$ over a vector space V, by above we get that (R3) attains equality, so that any matroid isomorphic to $M[V]$ attains equality on (R3).

(3) Let M be a matroid, and let B_X be a basis of X in M, now suppose that $I \subseteq E \backslash X$ such that $I \cup B$ is independent. Then by definition of independence via the rank, we have $\operatorname{rank}(I \cup B) = |I \cup B| = |I| + |B|$. Now suppose $X' \subseteq X$ is also independent, then $\operatorname{rank} X' = |X'|$. Then B is a basis of X, so $|X'| \leq |B|$, so we can take the complement of B with respect to X'. Now since B is independent, we must also have that $B \backslash X \subseteq B$ must also be independent, so we get that $\operatorname{rank}(B \backslash X') = |B| - |x'|$, then we have that $\operatorname{rank}(I \cup B) - \operatorname{rank}(B \backslash X') = |I| + |B| - |B| + |X'| = |I| + |X'| = |I \cup X'|$. Moreover, $\operatorname{rank}((I \cup B) \backslash (B \backslash X')) = \operatorname{rank}(I \cup X') = |I \cup X'|$. This makes $I \cup X'$ independent as well.

Lemma 1.3.2. *Let E be a set and $r : 2^E \to \mathbb{N}$ be a mapping satisfying (R1) and (R2). if X and Y are subsets of E such that $r(X \cup y) = r(X)$ for all $y \in Y \backslash X$, then $r(X \cup Y) = r(X)$.*

Proof. Let $X \backslash Y = \{y_1, \ldots, y_n\}$. Then by induction on n, when $n = 1$, we have by hypothesis thay $r(X \cup y_1) = r(X)$. Now suppose thta $r(X \cup \{y_1, \ldots y_n\}) = r(X)$ for all $n \geq 1$, and consider the set $\{y_1, \ldots, y_{n+1}\}$. Then we get that

$$\begin{aligned} r(X) + r(X) &= r(X \cup \{y_1, \ldots, y_n\}) + r(X \cup y_{n+1}) \\ &\geq r(X \cup \{y_1, \ldots y_{n+1}\}) + r(X \cap \{y_1, \ldots y_{n+1}\}) \\ &= r(X \cup \{y_1, \ldots y_{n+1}\}) + r(X) \\ &\geq r(X) + r(X) \end{aligned}$$

So by equality, we get that $r(X \cup \{y_1, \ldots, y_{n+1}\}) = r(X)$. □

Theorem 1.3.3. *Let E be a set and $r : 2^E \to \mathbb{N}$ be a mapping of 2^E into $\mathbb{N}$ such that r satisfies (R1)-(R3). If $\mathcal{I} = \{X \subseteq E : r(X) = |X|\}$ Then r is the rank function of a matroid M on E*

Proof. By (R1), we havbe that $0 \leq r(\emptyset) \leq |\emptyset| = 0$, so $r(\emptyset) = |\emptyset| = 0$; this makes $\emptyset \in \mathcal{I}$.

Now, suppose that $I \in \mathcal{I}$ and that $\mathcal{I}' \subseteq I$. Then $r(I) = |I|$, and $r(I' \cup (I \backslash I')) + r(I' \cap (I \backslash I')) \leq r(I') + r(I \backslash I')$, so $r(I) \leq r(I') + r(I \backslash I')$, i.e. $|I| \leq r(I') + r(I \backslash I') \leq |I'| + |I \backslash I'| = |I|$. This makes $r(I') = |I'|$, so that $I' \in \mathcal{I}$.

Now suppose that $I, I' \in \mathcal{I}$, with $|I| < |I'|$, and suppose for all $e \in I' \backslash I$ that $I \cup e \notin \mathcal{I}$, that is $r(I \cup e) \neq |I \cup e| = |I| + 1$. Now, we have that $|I| = r(I) \leq r(I \cup e) < |I| + 1$, so $r(U \cup e) = r(I) = |I|$; then by lemma 1.3.2, we have $r(I \cup I') = r(I)$, but we also have that $r(I \cup I') \geq r(I') = |I'|$ making $|I| \geq |I'|$, a contradiciton, therefore $I \cup e \in \mathcal{I}$ for all $e \in I' \backslash I$. This makes M into a matroid on E.

Now suppose that $X \in \mathcal{I}$ is independent. Then $r(X) = |X|$, moreover, X is a basis for the matroid $M|X$, so that $r(X) = \operatorname{rank} X$. Now if X isn't independent, and B is a basis for $M|X$, then we have $\operatorname{rank} B = |B|$, moreover, $B \cup x \notin \mathcal{I}$ for any $x \in X \backslash B$, so that $|B| = r(B) \leq r(B \cup x) < |B \cup x|$, making $r(B \cup x) = r(B)$. This makes $r(X) = r(B) = |B| = \operatorname{rank} X$, therefore $r = \operatorname{rank}$, and r is the rank function on M. □

Corollary. *r is the rank function of a matroid on E if, and only if it satisfies (R1)-(R3).*

This gives the next definition of a matroid.

Definition. A **matroid** on a finite nonempty set E is a pair $M = (E, \operatorname{rank})$ where $\operatorname{rank} : 2^E \to \mathbb{N}$ is a mapping taking subsets of E to $\mathbb{N}$ such that:

(R1) $0 \leq \operatorname{rank} X \leq |X|$ for all $X \subseteq E$

(R2) If $X \subseteq Y \subseteq E$, then $\operatorname{rank} X \leq \operatorname{rank} Y$.

(R3) If $X, Y \subseteq E$, then $\operatorname{rank} X \cup Y + \operatorname{rank} X \cap Y \leq \operatorname{rank} X + \operatorname{rank} Y$.

We call $\operatorname{rank} X$ the **rank** of X, and we call rank the **rank function** of the matroid M.

Theorem 1.3.4. *Let M be a matroid on a set E together with a rank function* rank. *Then the following are true for any $X \subseteq E$:*

(1) X is independent if, and only if $\operatorname{rank} X = |X|$.

(2) *X is a basis if, and only if* $\operatorname{rank} X = \operatorname{rank} M$.

(3) *X is a circuit if, and only if X is nonempty and for all $x \in X$,* $\operatorname{rank}(X \backslash x) = |X| - 1 = \operatorname{rank} X$.

Proof. The first statement follows immediately from theorem 1.3.3. Now, suppose that X is a basis of the matroid M, then X is independent, so $\operatorname{rank} X = |X|$, and by definition $\operatorname{rank} M = |X|$. Conversely, if $X \subseteq E$ such that $\operatorname{rank} M = \operatorname{rank} X$, then by definition $\operatorname{rank} M = |B|$ for some basis B of M, and $|B| = \operatorname{rank} X$, this makes X an independent set, then by the first statement, $\operatorname{rank} X = |X| = |B|$, making X a basis.

Now, suppose that X is a circuit, then by minimality, $X \backslash x$ is independent whenever $x \in X$, so that $\operatorname{rank}(X \backslash x) = |X \backslash x| = |X| - 1 = \operatorname{rank} X$. Conversely, suppose for X nonempty that $\operatorname{rank}(X \backslash x) = |X| - 1 = \operatorname{rank} X$ whenever $x \in X$. Then we have that since $\operatorname{rank}(X \backslash x) = |X| - 1 = |X \backslash x|$, $X \backslash x$ is independent, but since $\operatorname{rank} X = |X| - 1$, X is not independent. That makes X a minimally dependent set of E, thus X is a circuit of M. $\square$

Example 1.13. (1) Let E be any set, and consider the uniform matroid $U_{m,n}$ for $m, n \in \mathbb{Z}^+$. Then by definition, the rank function of $U_{m,n}$ is defined to be:

$$\operatorname{rank} X = \begin{cases} |X|, & \text{if } |X| < m \\ m, & \text{if } |X| \geq m \end{cases}$$

In fact, any matroid is isomorphic to a uniform matroid if and only if there are no circuits of size less than $\operatorname{rank} M + 1$. By definition, we have that if $U_{m,n}$ is the uniform matroid of rank m, then by definition the circuits are those sets C for which $|C| = m+1$; so any matroid isomorphic to $U_{m,n}$ must also satisfy this. Conversely, if M is a matroid of rank m, with all circuits C of size $m + 1$, then by minimality of C, $I = C \backslash c$ is maximally independent for appending any element makes it of size $m + 1$, which necesarily makes it a circuit. Thus I is a base, so that $\operatorname{rank} I = m$, since C is arbitrary, so is I, this then makes M isomorphic to $U_{m,n}$.

It happens for $U_{1,n}$, (R3) does not attain equality. Notice any basis B has $\operatorname{rank} B = 1$, and any circuit C has $\operatorname{rank} C = 1$, so $\operatorname{rank} B + \operatorname{rank} C = 2$. However, if B and C are disjoint, then $\operatorname{rank}(B \cup C) = 1$ and $\operatorname{rank}(B \cap C) = 0$, so that $\operatorname{rank}(B \cup C) + \operatorname{rank}(B \cap C) = 1 < 2$.

(2) If A is an $m \times n$ matrix over a field F, then the rank function of $M[A]$ is the rank of the $m \times |X|$ submatrix $A|X$ consisting of columns of A labeled by members of X. Moreover, the rank of X is the dimension of the subspace of the vector space over F spanned by the columns of $A|X$.

(3) Let G be a graph and $M(G)$ be the graphic matroid on G. If G is conneced, then a basis of G is a spanning tree T of G, for which $|V(T)| = |E(T)| + 1$, so the rank of $M(G)$ in this case is:

$$\operatorname{rank} M(G) = |V(G)| - 1$$

Now, if G has ω connected components, then by similar reasoning, the rank of $M(G)$ is:

$$\operatorname{rank} M(G) = |V(G)| - \omega$$

Now, if X is a subset of edges of G, then

$$\operatorname{rank} X = |V(X)| - \omega_X$$

where ω_X is the number of connected components of X.

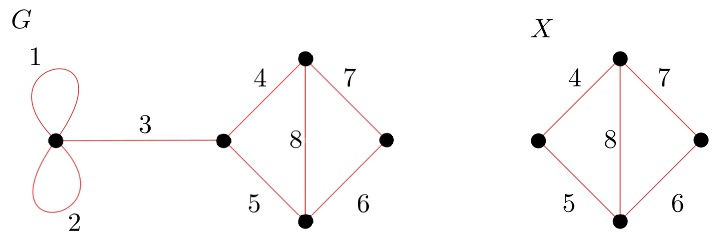


Figure 1.6:

(4) Let G be the graph in figure 1.6, then G is a connected graph so $\operatorname{rank} M(G) = |V(G)| - 1 = 4$. Now, if $X = \{4, 5, 6, 7, 8\}$, then $M(X) = M(G)|X$ has as a basis the set $\{4, 7, 8\}$, so that $\operatorname{rank} X = 3$. If $Z = \{1, 2\}$, then $M(Z)$ only has $\emptyset$ as a basis, so that $\operatorname{rank} Z = 0$.

(5) In any matroid M, we have an element x is a loop if, and only if $\operatorname{rank}\{x\} = 0$, and two elements x and y are parallel if and only if $\operatorname{rank}\{x, y\} = 1$.

Certainly, if x is a loop, then $\{x\}$ is a circuit, so that the only basis of $M|\{x\}$ is $\emptyset$, this makes $\operatorname{rank}\{x\} = 0$. Likewise, if x and y are parallel, then $\{x, y\}$ is a circuit, making $\{x\}$ and $\{y\}$ maximally independnet, and hence bases of $M|\{x, y\}$, thus $\operatorname{rank}\{x, y\} = 1$.

Conversely, if $\operatorname{rank}\{x\}$, then $\{x\}$ only has $\emptyset$ as a basis, hence $\{x\}$ is minimally dependent, hence a circuit, hence it is a loop. By similar reasoning for parallel elements, if $\operatorname{rank}\{x, y\} = 1$, then $x||y$.

Lemma 1.3.5. *Let M be a matroid and $k \in \mathbb{N}$ such that $k \leq \operatorname{rank} M$. Define the map $r_{(k)} : 2^E \to \mathbb{N}$ by $r_{(k)}(X) = \min\{k, \operatorname{rank} X\}$. Then $r_{(k)}$ is the rank function for a matroid.*

Proof. Certainly by definition, we have $0 \leq r_{(k)}(X) \leq |X|$. Moreover, if $X \subseteq Y$, then $\min\{k, \operatorname{rank} X\} \leq \min\{k, \operatorname{rank} Y\}$, so we get $r_{(k)}(X) \leq r_{(k)}(Y)$.

Now, if X and Y, then we get $r_{(k)}(X \cup Y) = \min\{k, \operatorname{rank}(X \cup Y)\}$, and $r_{(k)}(X \cap Y) = \min\{l, \operatorname{rank}(X \cap Y)\}$, then $r_{(k)}(X \cup Y) + r_{(k)}(X \cap Y) = \min\{k, \operatorname{rank}(X \cup Y) + \operatorname{rank} X \cap Y\} \leq \min\{k, \operatorname{rank} X + \operatorname{rank} Y\} = r_{(k)}(X) + r_{(k)}(Y)$. This makes $r_{(k)}$ the rank function of the matroid. $\square$

Corollary. $r_{(k)}(M) = k$

Proof. We have that $k \leq M$, so $r_{(k)}(M) = \min\{k, \operatorname{rank} M\} = k$ in all cases. $\square$

Remark. We call this matroid obtained through $r_{(k)}$ a matroid obtained by a sequence of "truncations" . The collection of independent sets on these matroids are the collection of all independent sets of M of size less than or equal to k. That is:

$$\mathcal{I} = \{I \subseteq M : |I| \leq k\}$$

Definition. We call a matroid **paving** if it has no circuits of size less than $\operatorname{rank} M$.

Example 1.14. For any $m, n \in \mathbb{Z}^+$, the uniform matroid $U_{m,n}$ only has circuits of size $m+1$, thus $U_{m,n}$ is paving for all $m, n \in \mathbb{Z}^+$. In general, a matroid has circuits of size at most $\operatorname{rank} M + 1$, so that M is uniform if, and only if it has no circuits of size less than $\operatorname{rank} M + 1$. So a useful check for determining whether a matroid is paving is to show that it is uniform. However, not every paving matroid is uniform. For example, the matroid $M(K_5)$ on the complete graph on 5 vertices is paving, but not uniform.

Theorem 1.3.6. *Let $\mathcal{D}$ bea collection of nonempty subsets of a set E. Then $\mathcal{D}$ is the collection of circuits of a paving matroid on E if, and only if there is a $k \in \mathbb{Z}^+$ with $k < |E|$, and a subcollection $\mathcal{D}' \subseteq \mathcal{D}$ such that:*

(1) Every $D' \in \mathcal{D}'$ has k elements and if $D', D'' \in \mathcal{D}'$ are distinct, then $\binom{D' \cup D''}{k} \in \mathcal{D}'$.

(2) $\mathcal{D} \backslash \mathcal{D}'$ consists of all $k+1$-element subsets containing no member of $\mathcal{D}'$.

Lemma 1.3.7 (Brylawski)**.** *Let M be a matroid on a set E, and let $k \in \mathbb{N}$ such that $\operatorname{rank} M \leq k \leq |E|$. Then if S_k is the collection of all k-element subsets of E with rank $\operatorname{rank} M$, then S_k is the collection of basis of a matroid on E.*

Proof. Notice by definition that if $S, S' \in S_k$, then $|S| = |S'|$. Now, if S_k is empty that means no k-element suibset of E has rank $\operatorname{rank} M$, then if $k = |E|$, $\operatorname{rank} E \neq \operatorname{rank} M$, which cannot happen. So we have that S_k is nonempty.

Now let $S, S' \in S_k$, then $\operatorname{rank} S = \operatorname{rank} S' = \operatorname{rank} M$. Now choose $s \in S \backslash S'$, then $S \backslash s$ is a $k-1$-element set. Taking $s' \in S' \backslash S$, we have $(S \backslash s) \cup s'$ is a k-element subset of E, hence $|(S \backslash s) \cup s'| \leq |E|$ so we get $\operatorname{rank}(S \backslash s) \cup s' \leq \operatorname{rank} E = \operatorname{rank} M$, moreover, we have that $\operatorname{rank} S \leq \operatorname{rank}((S \backslash s) \cup s')$ by the corollary to lemma 1.3.1, so we get that $\operatorname{rank}(S \backslash s) \cup s' = \operatorname{rank} S = \operatorname{rank} M$, which makes $(S \backslash s) \cup s' \in S_k$. This makes S_k the collection of bases of a matroid on E. $\square$

Definition. Let M be a matroid on E, we define the **elongation** of M to rank k, where $\operatorname{rank} M \leq k \leq |E|$ to be the matroid on E having collection of bases S_k the collection of all k-element subsets of E of $\operatorname{rank} M. If$ k=$\operatorname{rank} M + 1$, we call the elongation of M the **Higgs lift** of M.

Lemma 1.3.8 (Edmonds and Rota)**.** *Let $f : 2^E \to \mathbb{N}$ be a mapping of subsets of a set E satisfying the following:*

(1) $f(\emptyset) = 0$.

(2) If $X \subseteq Y$, then $f(X) \leq f(Y)$.

(3) $f(X \cup Y) + f(X \cap Y) \leq f(X) + f(Y)$.

Then f defines a matroid M on E having the collection of independent sets $\mathcal{I}(f) = \{X \subseteq E : f(X) \geq |X|\}$.

Proof. By definition, we have $f(\emptyset) = 0 = |\emptyset|$, so $\emptyset \in \mathcal{I}(f)$. Now, suppose that $Y \in \mathcal{I}(f)$, then $f(Y) \geq |Y|$, now if $X \subseteq Y$, we either have $|X| \leq f(X) \leq |Y| \leq f(Y)$, or $|X| \leq |Y| \leq f(X) \leq f(Y)$; either case inheretence is satisfied, and $X \in \mathcal{I}(f)$.

Now suppose that $X, Y \in \mathcal{I}(f)$, and that $|X| < |Y|$. Now, let $y \in Y \backslash X$, and suppose that $f(X \cup y) < |X \cup y| = |X| + 1$, then we have $f(X \cup y) \leq f(X) + f(y) - f(X \cap y) = f(X) + f(y) \leq |X| + 1 \leq f(X) + f(y)$, which makes $f(X) = |X|$ and $f(y) = 1$, thus we get $f(X \cup y) = f(X) + f(y) = |X| + 1$, which contradicts the assumption. Thus we must have that $|X \cup e| \leq f(X \cup e)$. This makes $X \cup e \in \mathcal{I}(f)$, and makes $\mathcal{I}(f)$ the collection of independent sets of a matroid on E. □

Corollary. *The rank function of the matroid $M = (E, \mathcal{I}(f))$ is the map $r : 2^E \to \mathbb{N}$ defined by:*

$$r(X) = \begin{cases} |X|, & \text{if } f(X) = |X| \\ |B|, & \text{for some } B \subseteq X \text{ such that } f(B) = |B| \end{cases}$$

Proof. Let $X \in \mathcal{I}(f)$ be independent. Then we see that $f(X) \geq |X|$. Then X is dependent if $f(X) < |X|$. Thus, X is a basis if, and only if $f(X) = |X|$. □

Remark. We call mappings satisfying properties (1)-(3) of lemma 1.3.8 **submodular functions**, and we will study them and their matroids later on. It is no surprise that the rank function is also a submodular function.

1.4 The Closure Operator of a Matroid.

Definition. Let M be a matroid on a set E, we define a mapping $\mathrm{cl} : 2^E \to 2^E$ called the **closure operator** of M by the rule:

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

For all $X \in E$. We call $\mathrm{cl}\, X$ the **closure**, or the **span** of X in M.

Example 1.15.

(1) For any vector space V, and a vector $v \in V$, v is in the span of a set of vectors $\{v_1, \ldots, v_n\}$ if the subspaces spanned by $\{v_1, \ldots, v_n\}$ and $\{v_1, \ldots, v_n, v\}$ have the same dimension. Indeed, the span of a subset of vectors ion V is the closure operator for the matroid $M[V]$.

(2) In example 1.13(2), we have $\mathrm{cl}\,\emptyset = Z$, $\mathrm{cl}\,\{1, 3, 5\} = \{1, 2, 3, 4, 5\}$, and $\mathrm{cl}\,\{4, 5, 6\} = X$.

Lemma 1.4.1. *Let M be a matroid on a set E, then for every $X \subseteq E$,* $\mathrm{rank}\, X = \mathrm{rank}\,(\mathrm{cl}\, X)$.

Proof. Let B be a basis of X, then for each $x \in (\mathrm{cl}\, X) \backslash X$, $\mathrm{rank}\,(B \cup x) = \mathrm{rank}\, X = \mathrm{rank}\, B \leq \mathrm{rank}\,(B \cup x)$. Then $(B \cup x) < |B \cup x|$, so that $B \cup x$ is a dependent set. This makes B a basis of $\mathrm{cl}\, X$. □

Lemma 1.4.2. *The closure operator of a matroid M on a set E satisfies the following for all $X, Y \subseteq E$:*

(CL1) $X \subseteq \mathrm{cl}\, X$.

(CL2) If $X \subseteq Y$*, then* $\operatorname{cl} X \subseteq \operatorname{cl} Y$*.*

(CL3) $\operatorname{cl} X = \operatorname{cl}(\operatorname{cl} X)$*.*

(CL4) If $x \in E$*, and* $y \in \operatorname{cl}(X \cup x) \backslash \operatorname{cl} X$*, then* $x \in \operatorname{cl} X \cup y$*.*

Proof. By definition of closure, we have that $\operatorname{rank} X \cup x = \operatorname{rank} X$ for all $x \in X$, so $x \in \operatorname{cl} X$. Now suppose that $X \subseteq Y$, and let $x \in (\operatorname{cl} X)\backslash X$, then $\operatorname{rank}(X \cup x) = \operatorname{rank} X$. Now if B is a basis of X, then it is a basis for $X \cup x$. Then $Y \cup x$ has a basis B' which contains $B \backslash x$. Then it follows that $\operatorname{rank} Yc \cup x = \operatorname{rank} Y$, so that $x \in \operatorname{cl} Y$. So $\operatorname{cl} X \subseteq \operatorname{cl} Y$.

Notice also that $\operatorname{cl} X \subseteq \operatorname{cl}(\operatorname{cl} X)$. Then for $x \in \operatorname{cl}(\operatorname{cl} X)$, $\operatorname{rank}(\operatorname{cl} X \cup x) = \operatorname{rank}(\operatorname{cl} X) = \operatorname{rank} X$, by lemma 1.4.1, now we have that $\operatorname{rank} X \leq \operatorname{rank})X \cup x \operatorname{rank}(\operatorname{cl} X \cup x)$, so equality holds and $x \in \operatorname{cl} X$.

Now suppose that $y \in (\operatorname{cl}(X \cup x))\backslash \operatorname{cl} X$, then $\operatorname{rank} X \cup x \cup y = \operatorname{rank} X \cup x$, and $\operatorname{rank} X \cup y \neq \operatorname{rank} X$. Then by the corollary to lemma 1.3.1, we het $\operatorname{rank}(X \cup y) = X + 1$. Thus we have that $\operatorname{rank} X + 1 = \operatorname{rank}(X \cup y) \leq \operatorname{rank}(X \cup x \cup y) = \operatorname{rank}(X \cup y) = \operatorname{rank} X + 1$, so by equality, we get $\operatorname{rank}(X \cup x \cup y) = \operatorname{rank} X \cup y$, so that $x \in \operatorname{cl}(X \cup y)$. □

Lemma 1.4.3. *Let M be a matroid on a set E. Let $X \subseteq E$, and $x \in E$. If X is an independent set, and $X \cup x$ a dependent set, then* $x \in \operatorname{cl} X$*.*

Proof. We have that $X \cup x \notin \mathcal{I}$, is dependent, so that for $y \in X \cup x$, $y \in \operatorname{cl}(X \cup x)\backslash y$. Now, if $y = x$, we are done as $(X \cup x)\backslash y = X$. On the otherhand, if $y \neq x$, then $(X \cup x)\backslash y = (X\backslash y) \cup x$, so $y \in \operatorname{cl}((X\backslash y) \cup x)\backslash \operatorname{cl}(X\backslash y)$. Therefore, $x \in \operatorname{cl}((X\backslash y) \cup y) = \operatorname{cl} X$. □

Theorem 1.4.4. *Let E be a set and* $\operatorname{cl} : 2^E \to 2^E$ *be a mapping satisfying (CL1)-(CL4). If* $\mathcal{I} = \{X \subseteq X : x \notin \operatorname{cl}(X\backslash x),$ *for all* $x \in X\}$*, then $\mathcal{I}$ is the collection of independent sets of a matroid M on E having* cl *as its closure operator.*

Proof. We have $\emptyset \in \mathcal{I}$. Now, let $I \in \mathcal{I}$ with $I' \subseteq I$, then for any $x \in I$, we have $x \notin \operatorname{cl}(I\backslash x)$, and $\operatorname{cl}(I'\backslash x) \subseteq \operatorname{cl}(I\backslash x)$, so $x \notin \operatorname{cl}(I\backslash x)$. Therefore $I' \in \mathcal{I}$.

Now let $I, I' \in \mathcal{I}$ with $|I| < |I'|$, and suppose there is no $e \in I'\backslash I$ such that $I \cup e \in \mathcal{I}$, and suppose additionally that for all pairs of I and I', that $|I \cap I'|$ is maximal. Choose then a $y \in I'\backslash I$ and take $I'\backslash y$. Suppose that $I \subseteq \operatorname{cl}(I'\backslash y)$, then $\operatorname{cl} I \subseteq \operatorname{cl}(I'\backslash y)$, so that $y \notin \operatorname{cl} I\backslash y)$, therefore by the above lemma we have that $I \cup y \in \mathcal{I}$, which contradicts our assumption. So we get that $\operatorname{cl} I \operatorname{cl}(I'\backslash y)$, and there is some $t \in I$, and $t \notin \operatorname{cl}(I'\backslash y)$. Now, $t \in I\backslash I'$, and $(I'\backslash y) \cup t \in \mathcal{I}$. Now $|I \cap (I'\backslash y) \cup t| > |I \cap I'|$, so that $x \in ((I'\backslash y) \cup t)\backslash I$, making $I \cup x \in \mathcal{I}$, but $x \in I'\backslash I$, a contradiction. Therefore such an e stated in the assumption must exist. This makes M into a matroid with $\mathcal{I}$ as its collection of independent sets.

Now suppose that $x \in (\operatorname{cl} X)\backslash X$ and that B is a basis of X. Then $\operatorname{rank}(X \cup x) = \operatorname{rank} X$, and $B \in \mathcal{I}$, and $B \cup x \notin \mathcal{I}$. Then it follows that $x \in \operatorname{cl} B$ by the above lemma. Likewise, if $x \in (\operatorname{cl} X)\backslash X$ and B is a basis of X, then $B \cup y \notin \mathcal{I}$ for all $y \in X\backslash B$. So again we get that $X \subseteq \operatorname{cl} B$, so $\operatorname{cl} X \subseteq \operatorname{cl} B$. Thus $x \in \operatorname{cl} B$ so that $B \cup x \in \mathcal{I}$, making $B \cup x$ a basis of $X \cup x$, and $\operatorname{rank}(X \cup x) = |B| = \operatorname{rank} X$. Therefore cl is the closure operator of M. □

Corollary. *For any set E, the mapping* $\operatorname{cl} : 2^E \to 2^E$ *is the closure operator for a matroid on E if, and only if it satisfies (CL1)-(CL4).*

Definition. We define a matroid M on a set E to be the pair (E, cl) where $\mathrm{cl} : 2^E \to 2^E$ is a mapping satisfying the following:

(CL1) $X \subseteq \mathrm{cl}\, X$.

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

(CL3) $\mathrm{cl}\, X = \mathrm{cl}\,(\mathrm{cl}\, X)$.

(CL4) If $x \in E$, and $y \in \mathrm{cl}\,(X \cup x) \setminus \mathrm{cl}\, X$, then $x \in \mathrm{cl}\, X \cup y$.

We call cl the **closure operator** of M, and we call $\mathrm{cl}\, X$ th **closure**, or **span** of X in M.

We have thge immediate lemma concerning the closure operator.

Lemma 1.4.5. *Let M be a matroid on a set E, then the following are true for all $X, Y \subseteq E$.*

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

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

(3) The intersection of all flats containing X is precisely $\mathrm{cl}\, X$.

(4) $\mathrm{rank}\,(X \cup Y) = \mathrm{rank}\,(X \cup \mathrm{cl}\, Y) = \mathrm{rank}\,(\mathrm{cl}\, X \cup \mathrm{cl}\, X) = \mathrm{rank}\,(\mathrm{cl}\,(X \cup Y))$.

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

Proof. Let $X \subseteq Y$, and $\mathrm{cl}\, Y \subseteq \mathrm{cl}\, X$, then we have $\mathrm{cl}\, X \subseteq \mathrm{cl}\,(\mathrm{cl}\, Y) = \mathrm{cl}\, Y$, this shows equality.

Now, if $Y \subseteq \mathrm{cl}\, X$, then for all $y \in Y$, $\mathrm{rank}\,(X \cup y) = \mathrm{rank}\, X$, then by lemma 1.3.2, $\mathrm{rank}\,(X \cup Y) = \mathrm{rank}\, X$.

To prove (3), let $\mathcal{F} = \bigcap_{X \subseteq F} F$ be the intersection of all flats F containing X. Then for each F, $\mathrm{cl}\, F = F$, by containment, this makes $\mathrm{cl}\, X = X$, so that $\mathrm{cl}\, X \subseteq \mathcal{F}$. On the otherhand, if $x \in \mathcal{F}$, then $x \in F$, F, arbitrary. If $x \in \mathrm{cl}\, X$, then we are done, otherwise, $\mathrm{rank}\,(X \cup x) = \mathrm{rank}\, X + 1$, but $\mathrm{rank}\,(F \cup x) = \mathrm{rank}\, F$, which makes $\mathrm{rank}\,(X \cup x) > \mathrm{rank}\, X$, which contradicts the rank properties. Therefore $x \in \mathrm{cl}\, X$. This makes $\mathcal{F} \subseteq \mathrm{cl}\, X$.

Now, for (4), we have $Y \subseteq \mathrm{cl}\, Y$, so $\mathrm{rank}\,(X \cup Y) \leq \mathrm{rank}\,(X \cup \mathrm{cl}\, Y) \leq \mathrm{rank}\,(\mathrm{cl}\, X \cup \mathrm{cl}\, Y) \leq \mathrm{rank}\,(\mathrm{cl}\,(X \cup Y)) = \mathrm{rank}\,(X \cup Y)$, since $e \in \mathrm{cl}\,(X \cup Y)$ implies $\mathrm{rank}\,(X \cup Y \cup e) = \mathrm{rank}\,(X \cup Y)$.

Lastly, let $X \subseteq Y$ with $\mathrm{rank}\, X = \mathrm{rank}\, Y$. First we have $\mathrm{cl}\, X \subseteq \mathrm{cl}\, Y$. Now if $y \in \mathrm{cl}\, Y$, then $\mathrm{rank}\,(Y \cup y) = \mathrm{rank}\, Y = \mathrm{rank}\, X$, then $\mathrm{rank}\,(X \cup y) \leq \mathrm{rank}\, X + 1 = \mathrm{rank}\, Y + 1$. Now, if equality holds, then (R2) is contradicted, so we must have $\mathrm{rank}\,(X \cup y) < \mathrm{rank}\, Y + 1$, so that $\mathrm{rank}\,(X \cup y) = \mathrm{rank}\, Y = \mathrm{rank}\, X$. □

We also have the additional definitions.

Definition. if M is a matroid on a set E with closure operator cl, then we call a subset X of E a **flat** if $\mathrm{cl}\, X = X$. We call X a **hyperplane** if it is a flat of rank $\mathrm{rank}\, M - 1$, and we call X a **spanning set** of M if $\mathrm{cl}\, X = E$. If $Y \subseteq \mathrm{cl}\, X$, we also say that X **spans** Y.

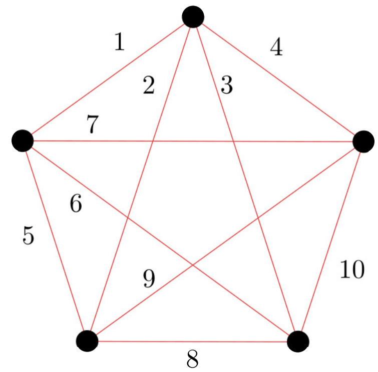


Figure 1.7:

Example 1.16. Consider the graphic matroid on K_5 labeled as in figure 1.7. then $M(K_5)$ has $\emptyset$ as the unique flat of rank 0. The rank-1 flats of $M(K_5)$ are the edges of K_5, the rank-2 flats of $M(K_5)$ are the edgesets of K_3 along with pairs of adjacent edges of K_5. the rank-3 flats of $M(K_5)$ are teh hyperplanes of $M(K_5)$, and consists of the edgesets of K_4 along with edgesets that are isomorphic to the disjoint union $K_2 \cup K_3$. Finally, the rank-4 flat of $M(K_5)$ is $M(K_5)$ itself.

Lemma 1.4.6. *let M be a matroid on E, and let $X \subseteq E$. If $x \in \operatorname{cl} X$, then $\operatorname{cl}(X \cup x) = \operatorname{cl} X$.*

Theorem 1.4.7. *Let M be a matroid on E, and let $X \subseteq E$. Then:*

(1) X is a spanning set if, and only if $\operatorname{rank} X = \operatorname{rank} M$.

(2) X is a basis if, and only if X is a independent spanning set.

(3) X is a basis if, and only if it is a minimal spanning set.

(4) X is a hyperplane if, and only if it is a maximal nonspanning set.

Proof. First, let X be a spanning set of M, then $\operatorname{cl} X = E$, ten by lemma 1.4.1, $\operatorname{rank} X = \operatorname{rank}(\operatorname{cl} X) = \operatorname{rank} E = \operatorname{rank} M$, so X is a basis of M. Conversely, if $\operatorname{rank} X = \operatorname{rank} M$, then for all $e \in E$, $\operatorname{rank}(X \cup e) = \operatorname{rank} X = \operatorname{rank} M$. This makes $\operatorname{cl} X = E$, and hence X is spanning.

Now, if X is a basis, then $\operatorname{rank} X = \operatorname{rank} M$, and X is independent, so X is an independent spanning set. Conversely, if X is an independent spanning set, we have $\operatorname{rank} X = \operatorname{rank} M$, and by theorem 1.3.4, X must be a basis.

let X be a minimal spanning set. Then $\operatorname{rank} X = \operatorname{rank} M$, and if $x \in X$, then $X \backslash x$ is not spanning. so by theorem 1.4.8, $x \notin \operatorname{cl}(X \backslash x)$, this makes X independent, and hence X is a basis. Now, if X is a basis, then X is spanning and independent. Then $\operatorname{cl} X = E$. Now let $x \in X$, then $\operatorname{rank}(X \cup x) = \operatorname{rank} X$, and $\operatorname{rank}(X \backslash x) \leq \operatorname{rank} X$, if equality holds, then $\operatorname{rank}(X \backslash x) = \operatorname{rank} M$, making $\operatorname{cl}(X \backslash x) = E$, which contradicts the spanning of X. Therefore $X \backslash x$ cannot be spanning, making X minimal.

Lastly suppose that X is a hyperplane, then it is a flat of rank $\operatorname{rank} M - 1$; that is $\operatorname{rank} X = \operatorname{rank} M - 1$, and $\operatorname{cl} X = X$. Now, if $x \in E \backslash X$, then $\operatorname{rank}(X \cup x) = \operatorname{rank} X + 1 = \operatorname{rank} M$, so that $X \cup x$ is not a flat, and hence not a hyperplane. Moreover, if $\operatorname{rank}(X \cup x) =$

$\operatorname{rank} M$, then $E \subseteq \operatorname{cl} X$, making X a spanning set. On the other hand, suppose that X is a maximal nonspanning set. That is $\operatorname{cl}(X \cup x) = E$. Then $\operatorname{rank}(X \cup x) = \operatorname{rank} M$, hence $\operatorname{rank} X = \operatorname{rank} M - 1$. Now, by maximality, we also have that $\operatorname{cl} X \neq E$, but that for any $x \in \operatorname{cl} X$, $\operatorname{rank}(X \cup x) = \operatorname{rank} X$, so that $x \in X$. Therefore $\operatorname{cl} X = X$. This makes X a flat of rank $\operatorname{rank} M - 1$, and hence a hyperplane. □

Theorem 1.4.8. *Let M be a matroid on a set E. Then:*

(1) X is a circuit if, and only if X is a minimal nonempty set such that $x \in \operatorname{cl}(X \backslash x)$ for all $x \in X$.

(2) $\operatorname{cl} X = X \cup \{x : x \in C \subseteq X \cup x,$ where C is a circuit of $M\}$.

Proof. The first statement mjust reasserts that circuits are minimal dependent sets. Now, for the second statement, suppose that $x \in \operatorname{cl} X \backslash X$, then $\operatorname{rank} X \cup x = \operatorname{rank} X$, so if B is a basis of X, then $B \cup x$ is a dependent set. Therefore there exists a circuit C with $x \in C \subseteq B \cup x$. Thus $x \in C \subseteq X \cup x$. Conversly, if C is a circuit, ten by (1) and (CL2), $x \in \operatorname{cl}(C \backslash x) \subseteq \operatorname{cl}(X \backslash x)$. □

The above theorem motivates the following theorem.

Theorem 1.4.9 (The Strong Circuit Elimination Axiom)**.** *The collection $\mathcal{C}$ of circuits of a matroid satisfies the following:*

($C'3$) If $C_1, C_2 \in \mathcal{C}$ with $e \in C_1 \cap C_2$, and $f \in C_1 \backslash C_2$, then there exists a $C \in \mathcal{C}$ such that $f \in C \subseteq (C_1 \cup C_2) \backslash e$.

Proof. Notice that $e \in \operatorname{cl}(C_2 \backslash e)$ and that $C_2 \backslash e \subseteq (C_1 \cup C_2) \backslash \{e, f\}$. Then $e \in \operatorname{cl}((C_1 \cup C_2) \backslash \{e, f\})$, therfore we get $\operatorname{cl}((C_1 \cup C_2) \backslash \{e, f\}) = \operatorname{cl}((C_1 \cup C_2) \backslash f)$. But $f \in \operatorname{cl}(C \backslash f) \subseteq \operatorname{cl}((C_1 \cup C_2) \backslash f)$, so $f \in \operatorname{cl}((C_1 \cup C_2) \backslash \{e, f\})$ Thus, by theorem 1.4.8, the matroid of $\mathcal{C}$ has a circuit C with $f \in C \subseteq (C_1 \cup C_2) \backslash e$. □

Corollary. *A collection $\mathcal{C}$ of subsets of a set E is the collection of circuits of a matroid if, and only if it satisfies the following:*

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

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

($C'3$) If $C_1, C_2 \in \mathcal{C}$ with $e \in C_1 \cap C_2$, and $f \in C_1 \backslash C_2$, then there exists a $C \in \mathcal{C}$ such that $f \in C \subseteq (C_1 \cup C_2) \backslash e$.

Lemma 1.4.10. *Let M be a matroid on a set E. Then the following are equivalent for any $e \in E$.*

(1) e is in every basis of M.

(2) e is in no circuit of M.

(3) If $X \subseteq E$ and $e \in \operatorname{cl} X$, then $e \in X$.

(4) $\operatorname{rank}(E \backslash e) = \operatorname{rank} E - 1$

(5) $E \backslash e$ *is a flat.*

(6) $E \backslash e$ *is a hyperplane.*

(7) If I *is independent, then so is* $I \cup e$

Proof. If e is in any basis, of M, then e cannot be in any dependent set, and hence no circuit.

Now suppose that e is in no circuit, and that for $X \subseteq E$, that $e \in \operatorname{cl} X$. Then if $e \notin X$, $e \in \{x : x \in C \subseteq X \cup x$ where C is a circuit of $M\}$. This makes e contained in a circuit contained in $X \cup e$, which contradicts our supposition. So $e \in X$.

Now supposse that for $X \subseteq E$, and $e \in \operatorname{cl} X$, that $e \in X$. Then we get that $\operatorname{cl} X = X$, so that X is a flat of M. Then $\operatorname{rank}(X \cup e) = \operatorname{rank} X$. Then notice that $E \subseteq E$, and that $e \in \operatorname{cl} E$, then we have $\operatorname{rank}(E \backslash e) = \operatorname{rank} E - 1$. This makes $E \backslash e$ a flat, since for any other $f \in E \backslash e$, $\operatorname{rank}((E \backslash e) \cup f) = \operatorname{rank}(E \backslash e) = \operatorname{rank} E - 1$. We also get that $E \backslash e$ is a hyperplane.

Now, if $E \backslash e$ is a hyperplane, then $E \backslash e$ is a flat, so that $\operatorname{cl}(E \backslash e) = E \backslash e$. This makes any $X \subseteq E \backslash e$ a flat as well, so that $\operatorname{cl} X = X$. So if I is independent, then $\operatorname{cl} I = I$, so that e is in no circuit contained in $I \cup e$. This makes $I \cup e$ independnet.

Moreover, suppose that if I and $I \cup e$ are independent, then e is in no circuit contained in $I \cup e$, and since I is arbitrary, we get that e is in no circuit of M. Which means e has to be contained in every basis of M. □

Theorem 1.4.11. *If* M *is a matroid of rank* r*, with* $\mathcal{C}'$ *a collection of nonspanning circuits, then:*

$$\mathcal{C} = \mathcal{C}' \cup \{X \subseteq E : |X| = r + 1 \text{ and } X \text{ contains no circuit of } \mathcal{C}'\}$$

Theorem 1.4.12. *if* G *is a graph then* H *is a hyperplane of* $M(G)$ *if, and only if* $E(G) \backslash H$ *is a minimal set of edges such whose removal fro m* G *increases the number of connected components.*

Proof. □

Theorem 1.4.13. *Let* E *be a set. Then the mapping* $r : 2^E \to \mathbb{N}$ *is the rank function for a matroid* M *on* E *if, and only if the following are satisfied:*

(R′1) $r(\emptyset) = 0$.

(R′2) If $X \subseteq E$ *and* $x \in E$*, then* $r(X) \leq r(X \cup x) \leq r(X) + 1$.

(R′3) If $X \subseteq E$*, and* $x, y \in E$ *such that* $r(X \cup x) = r(X \cup y) = r(X)$*, then* $r(X \cup x \cup y) = r(X)$.

Proof. Suppose first that r is the rank function of the matroid M. Then we see that $r(\emptyset) = 0$, and by the corollary to lemma 1.3.1, that $r(X) \leq r(X \cup x) \leq r(X) + 1$, whenever $X \subseteq E$, and $x \in E$.

Now suppose that X is a subset of E, and that $x, y \in E$, such that $r(X \cup x) = r(X \cup y) = r(X)$. This makes $x, y \in \operatorname{cl} X$, hence we have that $x \cup y \subseteq \operatorname{cl} X$, so we get that $r(X \cup x \cup y) = r(X \cup (x \cup y)) = r(X)$. So the rank function of a matroid satisfies $(R'1) - (R'3)$.

Conversely suppose that $r : 2^E \to \mathbb{N}$ is a mapping of subsets of E satisfying $(R'1) - (R'3)$. Then by $(R'1)$ and $(R'2)$ we get that $0 \leq r(X) \leq |X|$. Now suppose that $X \subseteq Y$, then $0 \leq r(X) \leq |X|$, and $0 \leq r(Y) \leq |Y|$, and $|X| \leq |Y|$ then $0 \leq r(Y) - r(X) \leq |Y| - |X|$, thus we get that $r(X) \leq r(Y)$. □

With the inclusion of the notion of rank and closure in a matroid, we have two more equivalent definitions as can be verified by the theorems above. The equivalence of the independence, rank, and closure axiomes can be seen in figure 1.5, and the equivalence of the rank and closure axioms to the base and circuit axioms can be verified by the transitivity of the two diagrams in figures 1.5 and 1.8. This gives us already a total of 5 *equivalent definitions of what a matroid is.*

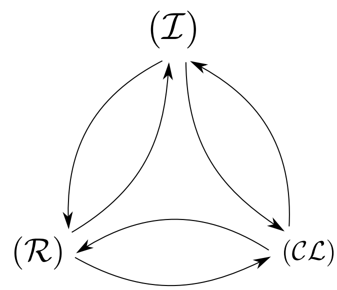


Figure 1.8: The equivalence of matroids defined by the independence $(\mathcal{I})$, rank $(\mathcal{R})$, and closure $(\mathcal{CL})$ axioms.

We can make one more definition for a matroid.

Definition. Let M be a matroid on a set E. We define the **nullity** of a set X of M to be:

$$\operatorname{nul} X = |X| - \operatorname{rank} X$$

One could define a matroid in terms of the nullity of its sets, however, doing so shows that the axiom system for nullity is precisely that for rank functiions. This makes the nullity of a matroid M a rank function.

1.5 Geometric Representations of Matroids of Small Rank.

Definition. Let V be a vector space over a field F of dimension m, a set of vector $\{v_1, \ldots, n_k\}$, not all necessarily distinct, is called **affinely dependent** if there exists scalars $a_1, \ldots, a_k \in F$, not all 0 such that

$$a_1 v_1 + \cdots + a_k v_k = 0$$

and

$$a_1 + \cdots + a_k = 0$$

We call $\{v_1, \ldots, v_k\}$ **affinely independent** if they are not affinely dependent.

We present one lemma on affine independence without proof.

Lemma 1.5.1. *A set $\{v_1, \ldots .v_k\}$ of vectors (not necesarily distinct) of a vector space V of dimension m is affinely dependent if the set of vectors $\{(1, v_1), \ldots, (1, v_k))\}$ is linearly dependent in the vector space F^{m+1}.*

Corollary. *$\{v_1, \ldots, v_k\}$ is affinely independent if $\{(1, v_1), \ldots, (1, v_k))\}$ is linearly independent.*

Lemma 1.5.2. *Let V be a vector space of dimension m over a field F, and let E be the set of vectors of V, not all necesarily distinct. If $\mathcal{I}$ is the collection of all subsetets of E which are affinely independent, then E together with $\mathcal{I}$ forms a matroid.*

Proof. By lemma 1.5.1, we have that $M = M[A]$ where A is the $(m+1) \times n$ matrix over F whose columns are $(1, v_i)^T$.

Alternatively, if we prove this directly by definition, we see that $\emptyset \in \mathcal{I}$, since $\emptyset$ is affinely independent. Moreover, if $\{v_1, \ldots, v_k\}$, is affinely independent, then $a_1v_1 + \cdots + a_kv_k$ with $a_1 + \cdots + a_k = 0$ implies that $a_i = 0$ for each $1 \leq i \leq k$, then indexing $1 \leq j \leq i$, we get that the subset $\{u_1, \ldots, u_j\}$ of $\{v_1, \ldots, v_k\}$ is also affinely independnet.

Now suppose that $U = \{u_1, \ldots, u_k\}$, and $V = \{v_1, \ldots, v_n\}$ are affinely independnet, with $k > n$, so that $|U| < |V|$. Then by definition, we have that

$$a_1v_1 + \cdots + a_kv_k = 0, \qquad a_1 + \cdots + a_k = 0$$

implies $a_i = 0$ for ech $1 \leq i \leq k$, and

$$b_1u_1 + \cdots + b_nu_n = 0, \qquad b_1 + \cdots + b_n = 0$$

implies $b_j = 0$ for ech $1 \leq j \leq n$

Then choose a vector $v_i \in V \backslash U$, so that $v_i \neq u_j$ for all u_j of U. Then we find that:

$$(b_1u_1 + \cdots + b_nu_n) + a_iv_i = 0, \qquad (b_1 + \cdots + b_n) + a_i = 0$$

Since $v_i \in V$, $a_i = 0$, so that the set $U \cup v_i$ is also affinely independent. Therefore E forms a matroid having $\mathcal{I}$ as its collection of independent sets. □

Example 1.17. (1) Let $E = \{(0,0), (1,0), (2,0), (0,1), (0,2), (1,1)\}$ Of $\mathbb{R}^2$, and consider the affine matroid on E We find that this matroid can be represented by the geometric figure in figure 1.9 below.

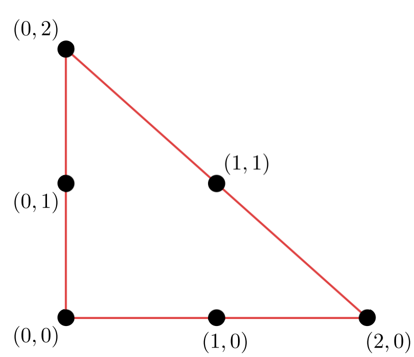


Figure 1.9: An affine matroid of rank 3.

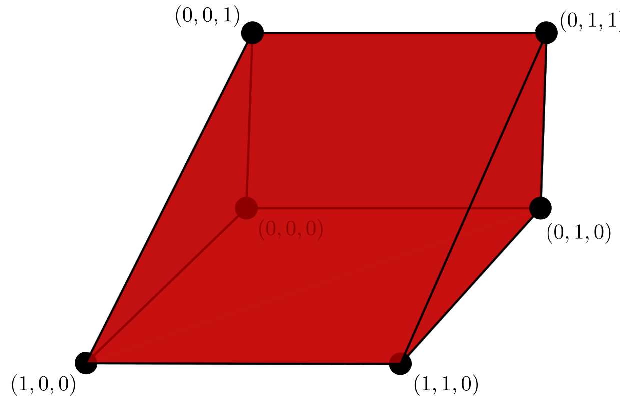


Figure 1.10: A rank 4 affine matroid in $\mathbb{R}^3$.

(2) Consider the affine matroid on $\mathbb{R}^3$ with ground set $E = \{(0,0,0),(1,0,0),(1,1,0),(0,1,0),(0,1,1),(0,0,1)\}$. We can geometrically represent this matroid by a wedge in $\mathbb{R}^3$ as in figure 1.10 The only dependent sets of less than 5 points are the three 4-point planes of the wedge.

(3) Consider the 2×5 matrix:

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

Which defines a matroid $M[A]$ Labeling the columns of A as $E = \{1,2,3,4,5\}$, we can represent this matroid geometrically in the following figure 1.11. Here we represent the loops of $M[A]$ as graphical loops (elements adjecent to themselves in a graph), and we represent parallel elements by two tangent points.

Figure 1.11: The rank 2 matroid $M[A]$ on the matrix A.

Definition. Let E be a set and $\mathcal{L}$ the collection of lines inducing a geomtry on E. We call a subset X of $\mathcal{L}$ **geometrically** dependent if for any of the points of X, two are identical, three are colinear, four are coplanar, or there are 5 arbitrary points in space.

Theorem 1.5.3. *Affine dependence is equivalent to geometric dependence.*

Theorem 1.5.3 provides a way to represent matroids of small rank geometrically. However, not all geometric figures are matroids. Consider the next example.

Example 1.18. Consider the geometric figure in figure 1.13. On notion of dependnece in geometry is that a set of points are dependent if they are colinear. Thus the sets $\{1,2,3\}$ and $\{1,4,5\}$ are dependent lines. The dependent planes are $\{2,3,4,5\}$, $\{2,3,6,7\}$, and $\{4,5,6,7\}$. However, this diagram does not represent a matroid. For, suppose to the contrary. Let $X = \{1,2,3,6,7\}$, and $Y = \{1,4,5,6,7\}$, then we have $\operatorname{rank} X = \operatorname{rank} Y = 3$,

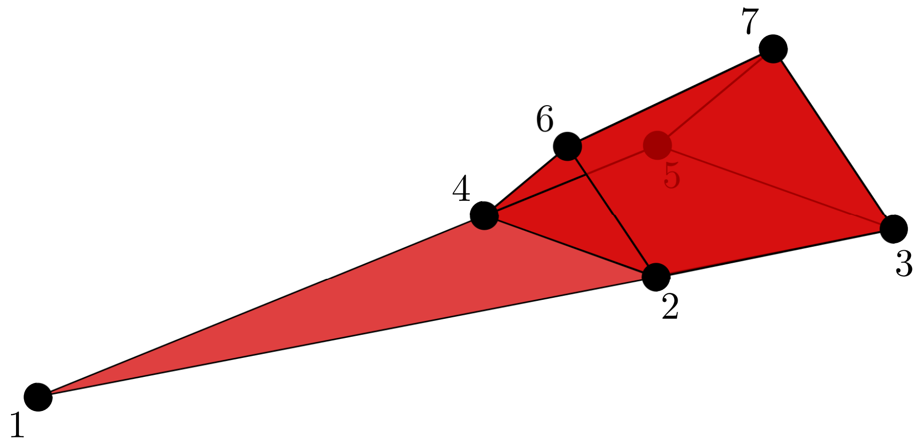


Figure 1.12: The Escher Figure.

and $\operatorname{rank}(X \cup Y) = 4$, so we must have $\operatorname{rank}(X \cup Y) + \operatorname{rank}(X \cap Y) \leq \operatorname{rank} X + \operatorname{rank} Y$, so that $\operatorname{rank}(X \cap Y) = \operatorname{rank}\{1, 6, 7\} \leq 2$. However, $\{1, 6, 7\}$ are noncolinear, and hence independent, so that $\operatorname{rank}(X \cap Y) = 3$, a contradiction. So to make figure 1.12 into a matroid, we would like to draw a line inbetween 1 and 7 so that $1 - 6 - 7$ are colinear, as shown in figure 1.13.

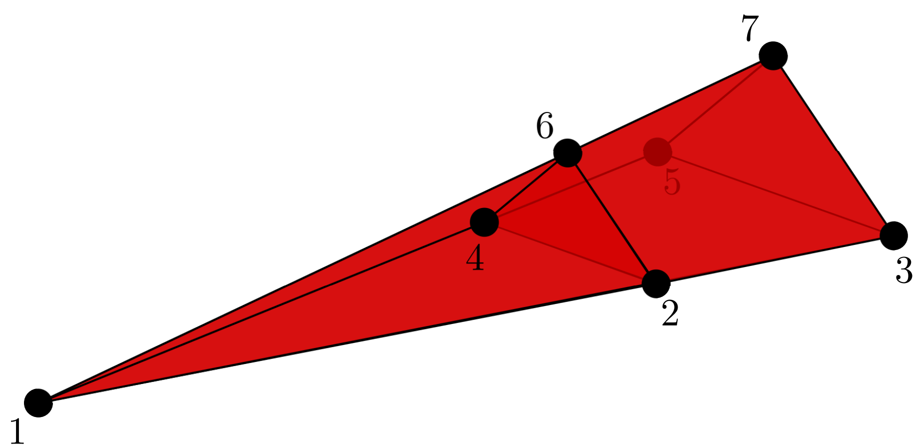


Figure 1.13: The Escher matroid.

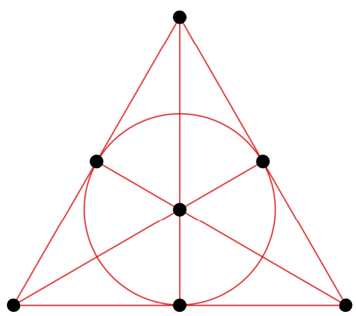
We call the matroid in figure 1.13 the **Escher matroid**. Notice that the rank of this matroid is 4.

The next result gives a way of identifing when geometric figures represent matroids of rank at most 4*, provided that any two distinct lines in the figure meet in at most one point.*

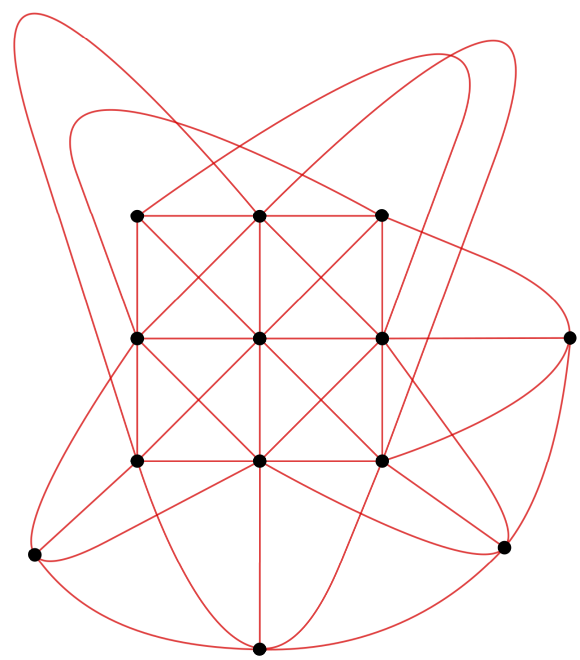
Lemma 1.5.4. *Let E be a set and $\mathcal{L}$ a collection of subsets of E each having atleast* 3 *elements, and such that every two distinct members of $\mathcal{L}$ intersect at atmost one element. Let $\mathcal{I}$ be the collection of subsets X of E having atleast* 3 *elements, such that no member of $\mathcal{L}$ contains on elements of X. Then E together with $\mathcal{I}$ forms a simple matroid M of rank* $\operatorname{rank} M \leq 3$*, whose rank* 1 *flats are the one element subsets of E, and whose rank* 2 *flats are* *the members of $\mathcal{L}$ together with all two element subsets Y of E such that no member of $\mathcal{L}$ contains Y.*

Corollary. *Every simple matroid of* rank ≤ 3 *arises this way.*

Example 1.19. Condsider the 7 and 13 point figures of the projective geometries $PG(2,2)$ and $PG(2,3)$. By lemma 1.5.3, we get that $PG(2,2)$ and $PG(2,3)$ form rank $= 3$ matroids. Specifically, we call $PG(2,2)$, which is the smallest such projkective geometry, the **Fano plane**, and hence call the matroid on $PG(2,2)$ the **Fano matroid**.



$PG(2,2)$



$PG(2,3)$

Figure 1.14: The Fano matroid on the Fano plane together with the matroid on $PG(2,3)$.

Theorem 1.5.5. *Let M be a matroid on a set E having a subset X that is both a circuit and ahyperplane. Let $\mathcal{B}$ be the collection of bases of M, and $\mathcal{B}' = \mathcal{B} \cup \{X\}$, then $\mathcal{B}'$ is the set of bases of a matroid M' on E. Moreover, if $\mathcal{C}$ is the set of circuits of M, then M' has the following as its set of circuits:*

$$\mathcal{C}' = (\mathcal{C} \backslash X) \cup \{X \cup e : e \in E \backslash X\}$$

There are also necessary and sufficient conditios on which a geometry actually represents a matroid of rank ≤ 4.

Theorem 1.5.6. *A set E together with a collection of lines inducing a geometry on E is a simple matroid of rank at most 4 if and only if the following hold:*

(1) Any two distinct lines meet in at most one point.

(2) Any two distinct planes meeting at more than one point do so in a line.

(3) Any two distinct lines meeting at a point do so in at most one point, and lie on a common plane.

(4) Any line not lying on a plane intersects the plane in at most one point.

Example 1.20. Consider the geometric figures P, and P' of figure 1.15. We call the matroid on P a **Papus** matroid, while P' is non-Papus they both obey law 1.5.9, and hence are geometric representations of matroids of rank $= 3$. The Papus matroid P is a representable matroid, while the non-Papus matroid P' is nonrepresentable. A "smallest" matroid can be derived with this property from the affine space $AG(3, 2)$.

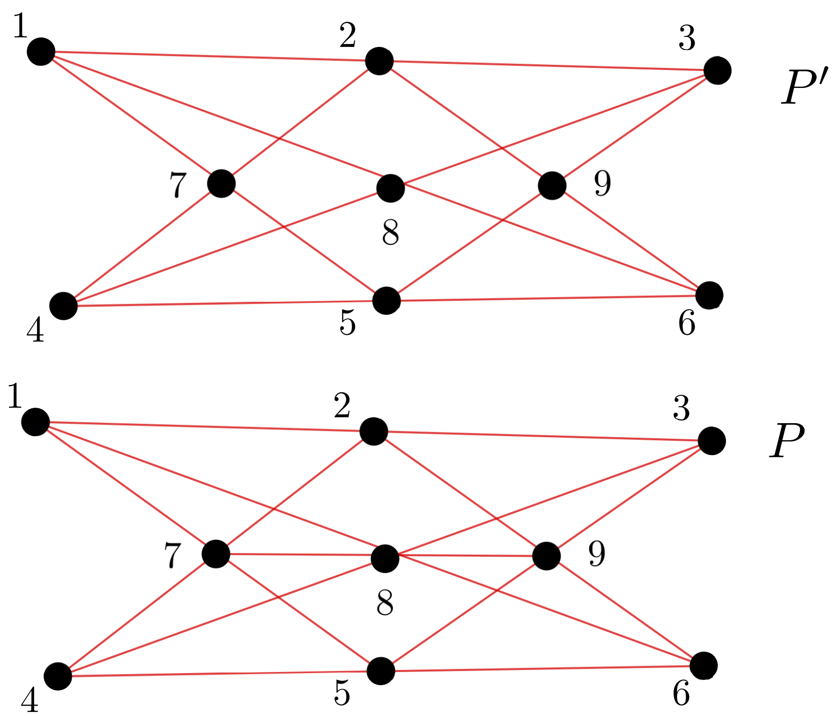


Figure 1.15: P' is a non-Papus matroid, and P is a Papus matroid.

It turns out most of the matroids represented here belong to a specific class of matroids which we define below.

Theorem 1.5.7. *Let $E = \{t, x_1, y_1, \ldots, x_r, y_r\}$ for some $r \geq 3$. Let $\mathcal{C}_1 = \{\{t, x_i, y_i\} : 1 \leq i \leq r\}$, let $\mathcal{C}_2 = \{\{x_i y_i, x_j, /y_j\} : 1 \leq i \leq j \leq r\}$. Let $\mathcal{C}_3$ be the possibly empty collection of all $\{z_1, \ldots, z_r\}$ such that $z_i \in \{x_i, y_i\}$, and no two member of $\mathcal{C}_3$ has more than $r - 2$ points in common. Let $\mathcal{C}_4$ be the collection of all $(r+1)$-element subsets that do not contain members of $\mathcal{C}_2 \cup \mathcal{C}_3$. Then there is a matroid on E of rank r having $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4$ as its collection of circuits.*

Proof. We have that $\emptyset \notin \mathcal{C}$, as the only collection that can possibly be empty is $\mathcal{C}_3$. We also have by definition that no member of $\mathcal{C}$ can be a proper subset of another member of $\mathcal{C}$.

Now if $\mathcal{C}$ were the collection of circuits on M, then we have that $\operatorname{rank} M \leq r$,by definition of $\mathcal{C}_4$. On the otherhand, by the definition of $\mathcal{C}_3$, at most one of the subsets $\{y_1, \ldots, y_r\}$ and $\{y_1, \ldots, y_{r-1}, x_r\}$ is independent, so that $M \geq r$. This makes $\operatorname{rank} M = r$.

Now, let $C_1, C_2 \in \mathcal{C}$, and $e \in C_1 \cap C_2$. If $C_1, C_2 \in \mathcal{C}_1 \cup \mathcal{C}_2$, then the weak circuit elimination axiom is satisfied. Now, suppose then that $|C_1| \leq |C_2|$ and that $C_2 \in \mathcal{C}_3 \cup \mathcal{C}_4$. Then we have:

$$\begin{aligned} |(C_1 \cup C_2)\backslash e| &= |C_1 \cup C_2| - 1 \\ &= |C_1| + |C_2| - |C_1 \cap C_2| - 1 \\ &= |C_1 \backslash C_2| + |C_2| - 1 \end{aligned}$$

Since $|C_2| = r$ or $|C_2| = r + 1$, we must have that $|(C_1 \cup C_2)\backslash e| \geq r + 1$, or that $C_2 \in \mathcal{C}_3$ and that $|C_1 \backslash C_2| = 1$. In the first case, we get that there is a circuit $C \in \mathcal{C}$ contained in $(C_1 \cup C_2)\backslash e$. In the second case, we get that $C_2 \in \mathcal{C}_4$, making $|C_1| > |C_2|$, which contradicts our suposition, so only the first case is true. This makes the collection $\mathcal{C}$ into the collection of cirvuits of M. $\square$

Definition. A matroid M on a set E having as collection of circuits the collection $\mathcal{C}$ defined in theorem 1.5.7 an r**-spiked matroid** with **tip** t, and legs $L_i = \{t, x_i, y_i\}$ where $1 \leq i \leq r$. If $\mathcal{C}_3 = \emptyset$, then we call M a **free spike**. If $/M' = M \backslash t$ is also a matroid, then we call M' a **tipless** spiked matroid.

Theorem 1.5.8. *Let $r \geq 2$ be an integer. A matroid M is an r- spike with tip t if, and only if:*

(1) E is the union of the legs $L_1, \ldots, L_r$, each of which is a 3-element circuit containing t.

(2) For each $1 \leq k \leq r - 1$, the union of any k legs $L_1, \ldots, L_r$ has rank $k + 1$.

(3) $\operatorname{rank}(L_1 \cup \cdots \cup L_r) = r$.

Definition. Let M be a matroid. We call distinct elements e and f of M **clones** if there exists an isomorphism $\phi : M \to M$ of M onto itself such that $\phi : e \to f, f \to e$, and $\phi : g \to g$ for any g distinct from both e and f.

Bibliography

[1] *J. G. Oxley,* Matroid theory*. Oxford New York: Oxford University Press, 2011.*

[2] *D. J. A. Welsh,* Matroid theory*. Mineola, N.Y: Dover Publications, 2010.*

[3] *G. Gordon and J. McNulty,* Matroids: A geometric Introduction*. CB2 8BS, United Kingdom: Cambridge University Press, 2012.*

[4] *I. N. Herstein,* Topics in algebra*. New York: Wiley, 1975.*

[5] *D. Dummit and R. Foote,* Abstract algebra*. Hoboken, NJ: John Wiley & Sons, Inc, 2004.*