Matroid Theory

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

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.

(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:

$$\{3\} \qquad \{1,4\} \qquad \{1,2,5\} \qquad \{2,4,5\}$$

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 1.3(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. □

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 $IC_1 \cup C_2$ 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.

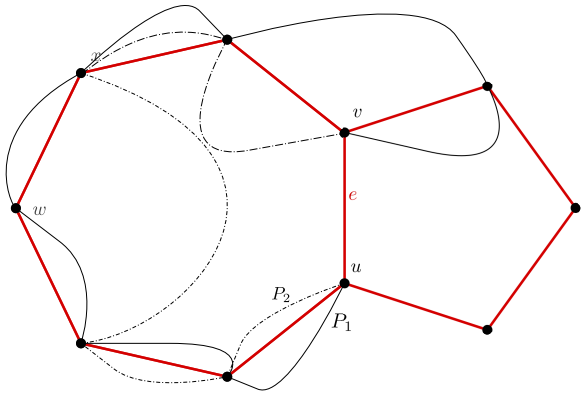

Figure 1.1: The cycle matroid corresponding to the graph G of example 1.2. Path P_1 is indicated by a solid line, and path P_2 indicated by a dotted line.

(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

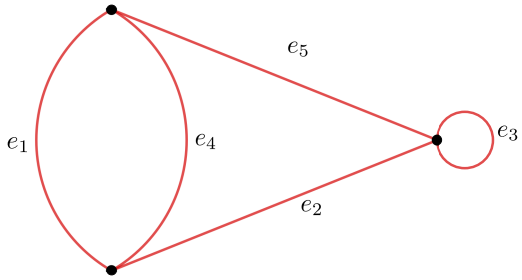

Figure 1.2:

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:

$$\{1,2,4\} \qquad \{1,3,5\} \qquad \{2,3,6\} \qquad \{4,5,6\}$$
$$\{1,4,3,6\} \qquad \{1,5,2,6\} \qquad \{2,4,3,5\}$$

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 $(0 \dots 0)^T$. 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.

Definition. Let G be a set with bi-parition (X, Y). We defiine a **matching** from elements of X to subsets of Y to simply be a map $\mu : X \to 2^Y$. We then say that a subset $U \subseteq Y$ can be **matched** to X if there exists a matching $\mu : X \to U$.

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 with elements of X. Then $M = (Y, \mathcal{I})$ forms a matroid.*

Proof. Notce that $\emptyset \in \mathcal{I}$, and can be matched to elements of X with no matching. Likewise, if I_1 is a subset of Y that can be matched to elements of X, then there is a matching $\mu : X \to I_1$. Now if $I_2 \subseteq I_1$, then I_2 can also be matched to elements of X by restricting the image of μ, i.e. taking $\mu : X \to I_2$.

Now, let $I_1, I_2 \in \mathcal{I}$. That is, they can be matched to elements of X via the matchings $\mu : X \to I_1$ and $\eta : X \to I_2$. Now, suppose that $|I_1| < |I_2|$ Then, taking $e \in I_2 \backslash I_1$, form the matching $\lambda : X \to I_1 \cup e$ by the rule $\lambda(I_1) = \mu(I_1)$ and $\lambda(e) = \nu(e)$. Then $I_1 \cup e$ can be matched to X via . Thus $I_1 \cup e \in \mathcal{I}$, making $(Y, \mathcal{I})$ 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 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 1.8. (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.

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

Example 1.9. (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:

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

(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 1.10. (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 $M(A) \simeq U_{2,4}$.

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 defininig 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.

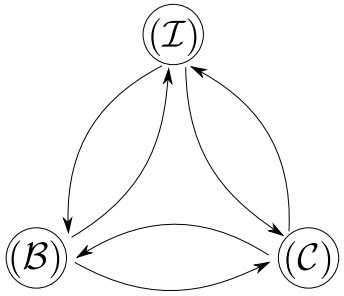

Figure 1.3: The implication digraph of $(\mathcal{I})$, $(\mathcal{B})$, and $(\mathcal{C})$.

1.3 The Rank of a Matroid.

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.