Matroid Theory

Alec Zabel-Mena
Text - Oxley, James . Matroid Theory

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 1. 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.

Definition 2. 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**.

Example 1.1. Let E be a finite set. Then $M = (E, \mathcal{I})$ is a matroid if, and only if:

(1) $\mathcal{I} \neq \emptyset$.

(2) Inheritance holds.

(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 (I_3).

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

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

Example 1.2. (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:

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

The collection of dependent sets are:

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

The minimal dependent sets of M on A is:

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

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.

Definition 3. 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 4. 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 1.1.1 (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 1.1.2. *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.*

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

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 5. 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 1.3. (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.

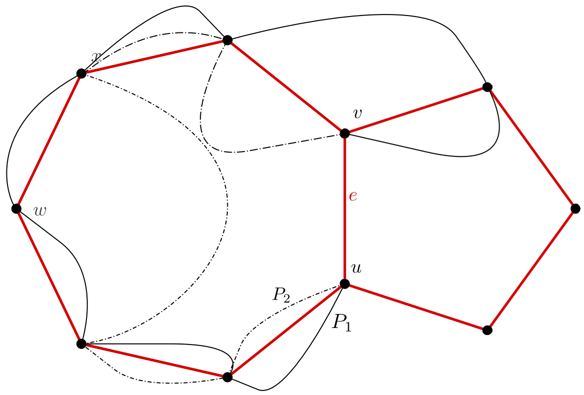

Figure 1.1: The cycle matroid corresponding to the graph G of example 1.2. Path P_1 is indicated by a solid line, and path P_2 indicated by a dotted line.

(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

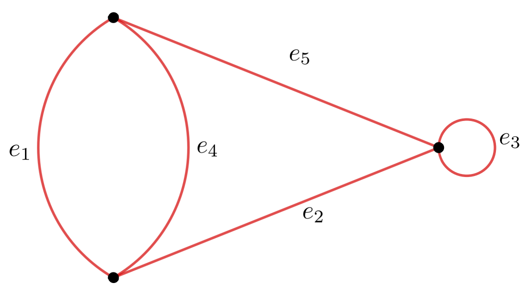

Figure 1.2:

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'.

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

Definition 6. 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 7. 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 8. 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 1.4. (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 1.1.3. *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. $\square$

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. $\square$

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 9. 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.

1.2 The Base Axioms.

Bibliography

[1] *Matroid Theory*. second ed.