Matroid Theory

Alec Zabel-Mena

Text - Welsh, Dominic J. Matroid Theory

Chapter 1

Fundamental of Matroid Theory.

1.1 Definitions

We go over some fundamental definitions and theorems for matroids.

Definition 1.1.1 (The Independence Axioms)**.** We define a **matroid** M to be a set S, called the **ground set**, together with a collection $\mathcal{I} \subseteq 2^S$ of subsets of S which we call **independent sets** to such that;

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

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

(I2) If $X, Y \in \mathcal{I}$ such that $|Y| < |X|$, then ther is an $x \in X \backslash Y$ such that $Y \cup x \in \mathcal{I}$. (Augmentation)

There is one immediate example for a matroid.

Example 1.1.1. Let V be a finite vector space and let $\mathcal{I}$ be the collection of all linearly independent subsets of vectors of V. Clearly $\emptyset \in V$, and if U is linearly independent, and $W \subseteq U$, then W is also linearly independent; so inheretence is satisfied.

Now let U and W be linearly independent subspaces with $\dim U < \dim W$ and take $w \in W \backslash U$, then $w \notin \operatorname{span} U$, then for vectors $u_1, \ldots, u_n \in U$, and scalars $\alpha_1, \ldots, \alpha_n, b$, take

$$\alpha_1 u_1 + \cdots + \alpha_n u_n + bw = 0$$

if $b \neq 0$, then

$$w = (-\frac{\alpha_1}{b})u_1 + \cdots + \alpha_n u_n$$

putting $w \in \operatorname{span} U$, a contradiction. Hence $U \cup w$ is also linearly independent, and we have that $\mathcal{I}$ forms a matroid on V.

We define some additional concepts, all of which can be used in the definition of a matroid.

Definition 1.1.2. A **base** of a matroid M is a maximally independent subset of S. We denote the collection of bases of M by $\mathcal{B}$. We say a subset of S is **spanning** in M if it contains a base.

Definition 1.1.3. We define the **rank function** of a matroid to be the map $\text{rank} : 2^S \to \mathbb{Z}$ defined by

$$\text{rank}\, A = \max\{|X| : X \in \mathcal{I} \text{ and } X \subseteq A\} \tag{1.1}$$

We define the **rank** of the matroid to be $\text{rank}\, M = \text{rank}\, S$. We say $A \subseteq S$ is **closed**, or a **flat**, or a **subspace** of M if for all $x \in S\backslash A$, $\text{rank}\, A \cup x = \text{rank}\, A + 1$, and we say x **depends** on A.

Definition 1.1.4. We define the **closure operator** of a matroid to be the map $\text{cl} : 2^S \to 2^S$ defined such that $\text{cl}\, A$is the set of all elements which depend on A; that is

$$\text{cl}\, A = \{x \in S\backslash A : \text{rank}\, A \cup x = \text{rank}\, A\}. \tag{1.2}$$

Definition 1.1.5. A **dependent set** of a matroid is a subset $D \subseteq S$ which is not independent; this is $D \notin \mathcal{I}$. A **circuit** of a matroid is a minimally dependent set, and we denote the collection of all circuits as $\mathcal{C}$.

Now one thing that makes matroids so interesting, is that they can be axiomatically defined in various ways. We can not only define them in terms of independence, bu also in terms of bases, circuits, rank, and closure. We give the theorems below that establish the axioms.

Theorem 1.1.1 (The Base Axioms)**.** *A nonempty collection $\mathcal{B}$ of subsesets of a set S forms a set of bases of a matroid M on S if, and only if for:*

(B1) $B_1, B_2 \in \mathcal{B}$*, and* $x \in B_1\backslash B_2$*, there is a* $y \in B_2\backslash B_1$ *such that* $(B_1 \cup y)\backslash x \in \mathcal{B}$*.*

Theorem 1.1.2 (The Circuit Axioms)**.** *A nonempty collection $\mathcal{C}$ of subsesets of a set S forms a set of circuits of a matroid M on S if, and only if:*

(C1) If $Y \in \mathcal{C}$ *and* $X \neq Y$*, then* $X \not\subseteq Y$*.*

(C2) If $C_1, C_2 \in \mathcal{C}$ *are distinct, and* $z \in C_1 \cap C_2$*, then there is a circuit* $C_3 \in \mathcal{C}$ *such that* $C_3 \subseteq (C_1 \cup C_2)\backslash z$*. (The Circuit Elimination Axiom)*

Theorem 1.1.3 (The First Rank Axioms)**.** *Let S be a set. A map* $\text{rank} : 2^S \to \mathbb{Z}$ *is the rank function of a matroid on S if and only if for* $X \subseteq S$ *and* $y, z \in S$

(R1) $\text{rank}\, \emptyset = 1$*.*

(R2) $\text{rank}\, X \leq \text{rank}\, X \cup y \leq \text{rank}\, X + 1$*.*

(R3) If $\text{rank}\, X \cup y = \text{rank}\, X \cup z = \text{rank}\, X$*, then* $x \cup y \cup z = \text{rank}\, X$*.*

Theorem 1.1.4 (The Second Rank Axioms)**.** *Let S be a set. A map* $\text{rank} : 2^S \to \mathbb{Z}$ *is the rank function of a matroid on S if and only if for* $X, Y \subseteq S$

(R′1) $0 \leq \text{rank}\, X \leq |X|$*.*

(R′2) If XY*, then* $\text{rank}\, X \leq \text{rank}\, Y$

(R′3) $\operatorname{rank} X \cup Y + \operatorname{rank} X \cap Y \leq \operatorname{rank} X + \operatorname{rank} Y$.

Theorem 1.1.5 (The Closure Axioms)**.** *Let S be a set. A map $\operatorname{cl} : 2^S \to 2^S$ is the closure operator of a matroid on S if and only if for $X, Y \subseteq S$, and $x, y \in S$*

(S1) $X \subseteq \operatorname{cl} X$.

(S2) If $Y \subseteq X$, then $\operatorname{cl} Y \subseteq \operatorname{cl} X$.

(S3) $\operatorname{cl} X = \operatorname{cl}(\operatorname{cl} X)$.

1. *If $y \notin \operatorname{cl} X$ and $y \in \operatorname{cl}(X \cup x)$, then $x \in \operatorname{cl}(X cupy)$.*

We defer their proofs to the relevant sections.
We can already provea fact about matroids.

Proposition 1.1.6. *If an element of a matroid belongs to every base, then it can belong to no circuit of the matroid.*

Proof. Let M be a matroid and let $\mathcal{B}$ be the collection of all bases of M, $\mathcal{C}$ the collection of all circuits of M, and $\mathcal{I}$ the collection of all independent sets of M. Take $x \in X = \bigcap_{B \in \mathcal{B}} B$ and suppose that $x \in C$ for $C \in \mathcal{C}$. By theorem 1.1.1, we have that $X \neq \emptyset$, moreover since $x \in C$, $C \subseteq X$, i.e $C \in \mathcal{B}$. mow notice that since C is a circuit, it is dependent, so $C \notin \mathcal{I}$, but we have that $C \in \mathcal{B}$ which makes it a base, and hence independent; so $C \in \mathcal{I}$, a contradiction. □

Definition 1.1.6. We say that two matroids M_1 and M_2 on S_1 and S_2 respectively are **isomorphic** if there is a $1-1$ map $\phi : S_1 \to S_2$ of S_1 onto S_2 such that if $X \subseteq S_1$ is independent in M_1, then $\phi(X) \subseteq S_2$ is independent in M_2. We write $M_1 \simeq M_2$ to denote isomorphism.

Example 1.1.2. We list all nonisomorphic matroids on a set of n elements for $n = 1, 2, 3$.

$\underline{n = 1}$ For $S = \{1\}$, we have $M_1 = \emptyset$ and $M_2 = 2^S$. There are $2^1 = 2$ matroids on S.

$\underline{n = 2}$ On $S = \{1, 2\}$we have

$$\begin{aligned} M_1 &= \emptyset \\ M_2 &= \{\emptyset, \{1\}\} \\ M_3 &= \{\emptyset\{1\}, \{2\}\} \\ M_4 &= \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} = 2^S \end{aligned}$$

there are $2^2 = 4$ matroids on S

$\underline{n=3}$ For $S=\{1,2,3\}$ we have

$$
\begin{aligned}
M_1 &= \emptyset \\
M_2 &= \{\emptyset,\{1\}\} \\
M_3 &= \{\emptyset\{1\},\{2\}\} \\
M_4 &= \{\emptyset,\{1\},\{2\},\{1,2\}\} \\
M_5 &= \{\emptyset,\{1\},\{2\},\{3\}\} \\
M_6 &= \{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\}\} \\
M_7 &= \{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\}\} \\
M_8 &= \{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\} = 2^S
\end{aligned}
$$

There are $2^3 = 8$ matroids on S.

Now one might be tempted to generalize that there are a total of 2^n matroids on a given n element set, however a quick check for $n=4$ concludes that that is not the case.

$\underline{n=4}$ For $S=\{1,2,3,4\}$ we have

$$
\begin{aligned}
M_1 &= \emptyset \\
M_2 &= \{\emptyset,\{1\}\} \\
M_3 &= \{\emptyset\{1\},\{2\}\} \\
M_4 &= \{\emptyset,\{1\},\{2\},\{1,2\}\} \\
M_5 &= \{\emptyset,\{1\},\{2\},\{3\}\} \\
M_6 &= \{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\}\} \\
M_7 &= \{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\}\} \\
M_8 &= \{\emptyset,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\} \\
M_9 &= \{\emptyset,\{1\},\{2\},\{3\},\{4\}\} \\
M_{10} &= \{\emptyset,\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\}\} \\
M_{11} &= \{\emptyset,\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\},\{2,3\}\} \\
M_{12} &= \{\emptyset,\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\} \\
M_{13} &= \{\emptyset,\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},\{1,2,3\}\} \\
M_{14} &= \{\emptyset,\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},\{1,2,3\},\{1,2,4\}\} \\
M_{15} &= \{\emptyset,\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},\{1,2,3\},\{1,2,4\}\{1,3,4\}\} \\
M_{16} &= \{\emptyset,\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},\{1,2,3\},\{1,2,4\}\{1,3,4\}, \\
&\quad \{2,3,4\}\} \\
M_{17} &= \{\emptyset,\{1\},\{2\},\{3\},\{4\},\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\},\{1,2,3\},\{1,2,4\}\{1,3,4\}, \\
&\quad \{2,3,4\},\{1,2,3,4\}\} = 2^S
\end{aligned}
$$

Notice that $S=\{1,2,3,4\}$ has $17 = 2^4+1$ matroids.

We conclude the section with an additional axiomatic definition for a matroid. This definition relies on the concept of an "independence function", which was postulated and shown by Rado.

Definition 1.1.7 (The Independence Function Axioms)**.** A map $f : 2^S \to \mathbb{Z}/2\mathbb{Z}$ on the set of finite sequences of elements of S is an **independence function** if for any $n \in \mathbb{Z}^+$ and sequences $\{x_i\}_{i=1}^n, \{y_i\}_{i=1}^{n+1}$ of S the folowing hold:

(IF1) $f(\emptyset) = 1$

(IF2) f is decreasing.

(IF3) f is commutative, i.e. for any permutation $i \to \alpha i$ of $\{1, \ldots, n\}$

$$f(\{x_i\}) = f(\{x_{\alpha i}\}) \tag{1.3}$$

(IF4) f is non reflexive, i.e. $f(x, x) = 0$ for all $x \in S$.

(IF5) f is distributive; that is

$$f(\{x_i\})f(\{y_i\}) \leq \sum_{i=1}^{n+1} f(\{x_i\}, y_i) \tag{1.4}$$

Theorem 1.1.7. *Let S be a set and $f : 2^S \to \mathbb{Z}/2\mathbb{Z}$ be an independence function. Define $\mathcal{I}$ to be the collection of sequences finite $\{x_i\}_{i=1}^n$ of S such that $f(\{x_i\}) = 1$. Then $\mathcal{I}$ forms a matroid on S. Conversely, if M is a matroid on S with independence set $\mathcal{I}$, then there is a map $f : 2^S \to \mathbb{Z}/2\mathbb{Z}$ satisfying the independence function axioms.*

Proof. Clearly $\emptyset \in \mathcal{I}$ since $f(\emptyset) = 1$ by definition. Now let $X = \{x_i\}_{i=1}^m \in \mathcal{I}$ and $Y = \{x_j\}_{j=1}^n \subseteq X$, with $n \leq m$. Since f is decreasing, we have that $f(X) \leq f(Y)$; now if $f(Y) = 0$ then $x_j = x$ for all $1 \leq j \leq n$ by the nonreflexivity of f. Then $f(X)f(Y) \leq \sum_{i=1}^{n+m} f(X, x_i) = 0$ by nonreflexivity again, implying that $f(X) = 0$ which cannot happen. So $f(Y) = 1$.

Now take $X = \{x_i\}_{i=1}^m, Y = \{y_i\}_{i=1}^n \in \mathcal{I}$ with $n < m$ so that $|Y| < |X|$. Take $X \backslash Y$, then since f is distributrive, we have $f(Y)f(X\backslash Y) \leq \sum_{i=1}^{n+1} f(Y, x_i)$ (if $x_i \in Y$ we reduce to nonreflexivity), and since $f(X) = 1$ and $f(Y) = 1$, then $\sum f(Y, x_i) = 1$ for if not we get nonreflexivity leading to the previous contradictions; thus $f(Y, x_i) = 1$. Therefore $\mathcal{I} = \{X \subseteq S : f(X) = 1\}$ defines a matroid over S.

Conversely, suppose we habe a matroid $M = (S, \mathcal{I})$, and define the map $f : 2^S \to \mathbb{Z}/2\mathbb{Z}$ By $f(X) = \begin{cases} 1 & \text{, if } X \in \mathcal{I} \\ 0 & \text{, if } X \notin \mathcal{I} \end{cases}$, we wish to show that f is an independence function on M.

Clearly $f(\emptyset) = 1$. Now for $X \in \mathcal{I}$ and $Y \subseteq X$, $Y \in \mathcal{I}$, so we have that $f(X) = f(Y) = 1$, moreover since $|Y| \leq |X|$, by augmentation, $f(Y \cup x) = 1$ for $x \in \cup XY$, and if this not the case, we get $f(Y \cup x) = 0$. In either cases we have $f(Y \cup x) \leq f(Y)$, so f is decreasing. It is also clear to see that f is commutative.

Now take $f(X \cup x)$ for $x \in X$ (we are generalizing reflexivity), then $f(X \cup x) \leq f(X)$. Now if $f(X \cup x) = 1$, we have a contradiction in the agumentation property, so that cannot happen; hence f is nonreflexive.

Lastly, we see by the deacreasing of f, and by augmentation that for $X = \{X_i\}_{i=1}^{n}, Y = \{y_i\}_{i=1}^{n+1} \in \mathcal{I}$, and summing the augmentations $f(X \cup y_i)$ for all $y_i \in Y$, we get

$$f(X)f(Y) \leq \sum_{i=1}^{n+1} f(X \cup y_i)$$

and so f is distributive, which makes it into an independence function. □

1.2 Examples

We define some matroids, and observe the properties of a peculiar one.

Proposition 1.2.1. *Let S be a set with $|S| = n$ and define $\mathcal{I} = \{X \subseteq S : |X| \leq k\}$ for $k \leq n$. Then S is a matroid on S.*

Proof. Clearly $\emptyset \in \mathcal{I}$, and if X is independent, and $Y \subseteq X$, then $|Y| \leq |X| \leq k$, hence $Y \in \mathcal{I}$.

Now take $Y, X \in \mathcal{I}$ with $|Y| < |X|$. Now if $|Y| + 1 = |X| = k$, the result is clear. Otherwise, choose an $x \imath X \backslash Y$, then since $|Y| < k$, $|Y \cup x| \leq k$, and hence is independent. □

Definition 1.2.1. We call the matroids on a set S, generated by the collection $\mathcal{I} = \{X \subseteq S : |X| \leq\}$ the **uniform matroid** of rank k on S; and we denote it $U_{k,n}$.

We discuss some properties of the uniform matroid.

Corollary. *$\mathcal{B}(U_{k,n}) = \{X \subseteq S : |X| = k\}$ and $\mathcal{C}(U_{k,n}) = \{X \subseteq S : |X| = k + 1\}$*

Proof. If $B \in \mathcal{I}(U_{k,n})$ is a base, then $|B| \leq k$ and by the maximality of B for any $x \in S \backslash B$, $B \cup x \notin \mathcal{I}$, i.e. $|B \cup x| = |B| + 1 > k$. It follows that $|B| = k$. Likewise by the same reasoning we see by the minimality of any circuit $C \in \mathcal{C}$ that $|C| = k + 1$ □

Remark. Since any base, and any dependent set in $U_{k,n}$ has size $\geq k$, it is easy to see that any set A with $|A| \geq k$ is spanning in $U_{k,n}$.

Corollary. *For any $A \subseteq U_{k,n}$* $\operatorname{rank} A = \begin{cases} |A|, & \text{if } |A| \leq k \\ k, & \text{if } |A| > k \end{cases}$ *and* $\operatorname{cl} A = \begin{cases} A, & \text{if } |A| < k \\ S, & \text{if } |A| \geq k \end{cases}$

Proof. By definition, we have that $\operatorname{rank} A = \max\{|X| : X \subseteq A, |X| \leq k\}$. Now if A is independent, then $\operatorname{rank} A = A$. If A is dependent, well since every dependent set of $U_{k,n}$ is spanning, choose a base $B \subseteq A$. Then $\operatorname{rank} A = \operatorname{rank} B = k$.

Now by the closure axioms, $A \subseteq \operatorname{cl} A \subseteq S$. Suppose that $|A| < k$, and take $x \in \operatorname{cl} A$, then $\operatorname{rank} A \cup x = \operatorname{rank} A = |A|$, thus $x \in A$, so $\operatorname{cl} A = A$. Now if $|A| \geq k$, then for any $x \in S \backslash A$, $\operatorname{rank} A \cup x = \operatorname{rank} A \geq k > |A|$, this puts $x \in \operatorname{cl} A$, and bu consequence $S \subseteq \operatorname{cl} A$. Therefore $\operatorname{cl} A = S$. □

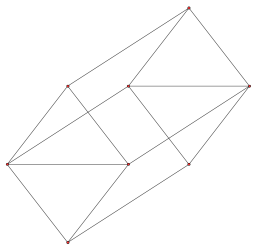

Figure 1.1: The Vámos Matroid.

Corollary. $\operatorname{rank} U_{k,n} = k$.

In the example 1.1.1 of section 1.1, we showed that a collection of linearlt independent subsets of vectors of a vector space forms a matroid over that vector space.

Definition 1.2.2. Let V be a finite vector space, and let M be the matroid on V formed by taking all linearly independent subsets of vectors of V. We call a matroid isomorphic to M **vectorial** over V, or **representable** over V.

Proposition 1.2.2. *The rank of a vectorial matroid is the dimension of the vector space that it is isomorphic to.*

Proof. Since $\dim V = |B|$, where B is a basis of linearly independent vectors of V, it is easy to see that $\operatorname{rank} M = \dim V$. □

Example 1.2.1. Consider $U_{2,4}$ and $\mathbb{F}_2$ as a vector space. One can see that $U_{2,4}$ is not vectorial over $\mathbb{F}_2$, for consider the subspace in $V_{\mathbb{F}_2}$ represented by the matrix $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ which is linearly dependent, hence any circuit of $V_{\mathbb{F}_2}$ has size at most 2, and since the circuits of $U_{2,4}$ have size exactly 3, there exists no map wich preserves circuits.

What about $\mathbb{F}_3$? We have $\operatorname{rank} U_{2,4} = 2 < \dim V_{\mathbb{F}_3} = 3$, so consider a subspace of $\dim = 2$ in $V_{\mathbb{F}_3}$. We see that for any $2 \times n$ matrix $M_{2\times n}$ that $\operatorname{cl} M_{2\times n} = V_{\mathbb{F}_3}$ (since adding any vector does not change the rank). So there is some matroid on $V_{\mathbb{F}_3}$ isomorphic to $U_{2,4}$, hence $U_{2,4}$ is vectorial over $\mathbb{F}_3$.

Proposition 1.2.3. *If M is a vectorial matroid and the elements $\{x_1, \ldots, x_n\}$ form a circuit, then $\{x_1, \ldots, x_n\}$ is linearly dependent when considered as vectors.*

Proof. If M is vectorial, then it is isomorphic to some matroid M' over a vector space V. Then for a cicuit of M, $\{x_1, \ldots, x_n\} \to \{v_1, \ldots, v_n\}$ is a circuit in the vector space V, thus $\{v_1, \ldots, v_n\}$ is linearly dependent. To complete the proof we just take the map to be the identity map. □

Example 1.2.2. Let $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$ represented in the following geometry of figure 1.2. Take $\mathcal{C}$ to be the set of all planes on S which are coplanar; notice that any plane in $\mathcal{C}$

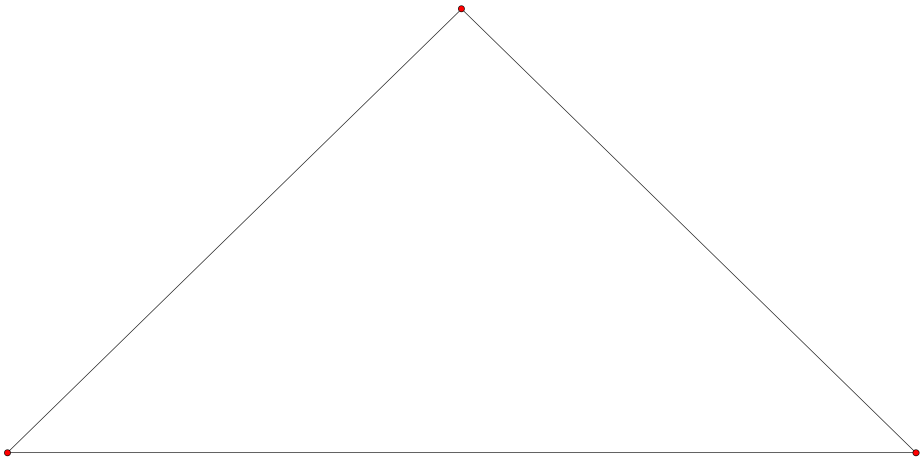

Figure 1.2: The complete graph K_3.

is minamal (removing an element removes its planarity), and also notice that if P_1 and P_1 are distinct planes in $\mathcal{C}$, they are coplanar, so take a point $z \in P_1 \cup P_2$, then there is indeed a plane $P_3(P_1 \cup P_2)\backslash z$ that is also coplanar. hence $\mathcal{C}$ is the set of circuits of a matroid. We call this matroid the **Vámos matroid** and denote it V_8.

Proposition 1.2.4. *The Vámos matroid is not vectorial over any vector space.*

Proof. Suppose that V_8 is indeed vectorial on a vector space V. Then there is a matroid M on V isomorphic to V_8; thus V has as bases linearly independent sets of 4 vectors, hence $\operatorname{rank} V_8 = \dim V = 4$. Then for any 4 elements of V_8 maps to a set of 4 vectors of V. Then for a circuit of V_8, take $\{p_1, p_2, p_3, p_4\} \to \{v_1, v_2, v_3, v_4\}$ which makes $\{v_1, v_2, v_3, v_4\}$ into a circuit of V, hence $\{v_1, v_2, v_3\}$ is a maximally independent set, and so is a base of B, thus we get $\dim\{v_1, v_2, v_3\} = \dim V = 3$, a contradiction; hence V_8 cannot be vectorial. □

Definition 1.2.3. Let G be a graph with edge set E, and let $X \in \mathcal{I}$ if and only if X contains no cycle of G. Then $\mathcal{I}$ is a collection of independent sets of a matroid, which we call the **cycle matroid** on G and denote it $M(G)$.

We defer the proof that the cycle is indeed a matroid for when we talk about matroids on graphs.

Example 1.2.3. The complete graph K_3 has as it's cycle matroid the matroid $U_{2,3}$ see figure 1.2.

We now talk about matroids arising from algebra. we give some proofs, but these matroids will be discussed when appropriate.

Definition 1.2.4. Let F be a field and K be an extension of F. We call a subset $\{x_1, \ldots, x_k\} \subseteq K$ of K **algebraically dependent** if there is a polynomial f with coefficients in F such that $f(x_1, dots, x_k) = 0$. Otherwise we say they are **algebraically independent**.

Theorem 1.2.5. *Let F be a field, K an extension of F, and let $S \subseteq K$ be finite. For any $X \subseteq S$, let $X \in \mathcal{I}$ if and only if X is algebraically independent. Then $\mathcal{I}$ forms a matroid over S..*

Proof. Clearly $\emptyset$ is algebraically independent. Now suppose that X is algebraically independent, and that YX. Then for every polynomial in X, $f \neq 0$. We have then there is a polyomial $g \in Y$ with $g \neq 0$ for which $f = g + h$ hence Y is algebraically independent.

Now suppose that $X = \{x_1, \ldots, x_k\}$ and $Y = \{y_1, \ldots, y_m\}$ are algebraically independent, with $m < k$, so that $|Y| < |X|$. Now for every polynomial in X, f, $f(x_1, \ldots, x_k) \neq 0$, and for every polynomial g in Y, $g(y_1, \ldots, y_m) \neq 0$. Now we can find a polynomial f_1 in X such that $f = f_1(x_i) + f_2(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$, where $f_1(x_i) \neq 0$, for $x_i \in X \backslash Y$ (if $X \cap Y = \emptyset$, then choose any x_i), then $f_1 \neq 0$ and $g \neq 0$ implies that $f(x_i) + g(y_1, \ldots, y_m) \neq 0$, then we see that $Y \cup x_i$ is also algebraically independent, whc=ich completes the proof. □

Definition 1.2.5. Let F be a field, K a field extension of F, and $S \subseteq K$ be finite. The collection of all algebraically independent subsets of S form a matroid on S. We call these matroids **algebraic**.

Definition 1.2.6. We call an element of Euclidean d-space, $x \in \mathbb{R}^d$ **affinely dependent** on a subset $\{x_1, \ldots, x_r\} \subseteq \mathbb{R}^d$ if there exist real numbers λ_i for $1 \leq i \leq r$ such that:

$$\sum \lambda_i = 1 \tag{1.5}$$

and

$$x = \sum \lambda_i x_i \tag{1.6}$$

We call a subset $X \subseteq \mathbb{R}^d$ **affinely independent** if no element $x \in X$ is affinely dependent on $X \backslash x$.

Theorem 1.2.6. *Let $S \subseteq \mathbb{R}^d$. Then the collection of all affinely independent subsets of S form a matroid on S.*

Proof. Clearly $\emptyset$ is affinely indipendent, trivially. Let X be affinely independent, and let $Y \subseteq X$. Then for $x \in X$ and $\{x_1, \ldots, x_r\} \subseteq X$ with $x \neq x_i$ for $1 \leq i \leq r$, there are no real nubers λ_i for which $\sum \lambda_i = 1$ and $x = \sum \lambda_i x_i$. Now if $x \in Y$, take $\{y_1, \ldots, y_s\} \subseteq \{x_1, \ldots, x_r\}$ and we are done. Now take $y \neq x \in Y$, and again take $\{y_1, \ldots, y_s\} \subseteq \{x_1, \ldots, x_r\}$ and where $y \neq y_j$ for $1 \leq j \leq s$. Now if there are realnumbers γ_j for which $\sum \gamma_j = 1$ and $y = \sum \gamma_j y_j$, then by inclusion, we can find addition γ_i for which $x = \sum \gamma_i x_i$, a contradiction; so Y must also be affinely independent.

Now let X and Y be affinely independent with $|Y| < |X|$, then for $y \in Y$ and $x \in X$ and $\{x_1, \ldots, x_r\}$, $\{y_1, \ldots, y_s\}$ (not necessarily disjoint) with $x_i \neq x$ and $y_j \neq y$ for $1 \leq i \leq r$ and $1]leqj \leq s$, there are no real numbers λ_i and γ_j for which $\sum \lambda_i = \sum \gamma_j = 1$ and $x = \sum \lambda_i x_i$ and $y = \sum \gamma_j y_j$. Now if there is indeed a λ_i and $x_i \notin \{y_1, \ldots, y_s\}$ for which $y = \lambda_i x_i + \sum \gamma_i y_i$, that would imply that we can find real numbers λ_i for which $x = \sum \lambda_i$ which cannot happen. Thus $Y \cup x_i$ must be affinely independent. □

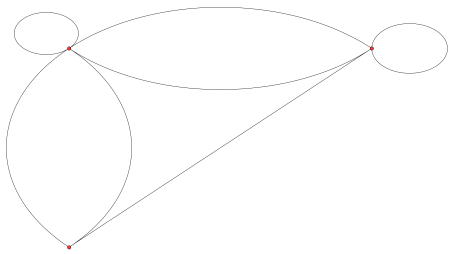

Figure 1.3: The graph G has 2 loops and 4 parallel elements.
fig:1.3

Definition 1.2.7. Let J be an abelian torsion group. An element $g \in J$ is called **dependent** if for elements $g_1, \ldots, g_n \in J$ and integers $m \neq 0, k_1, \ldots, k_m$ we have

$$mg = k_1 g_1 + \cdots + k_n g_n. \tag{1.7}$$

A subset $Y \subseteq J$ is **independent** if there is no $y \in Y$ for which y is dependent on $Y \backslash y$.

We defer the proof of this theorem.

1.3 Loops and Parallel elements.

Definition 1.3.1. We define a **loop** of a matroid to be an element $x \in S$ for which $\{x\}$ is a dependent set. We say that two elements $x, y \in S$ are parallel if $\{x, y\}$ is dependent, and they are both not loops.

Example 1.3.1. Let M be the cycle matroid of the graph G in figure **??** has 2 loops which we label x_1 and x_2, and 4 parallel elements which we label y_1, y_2 and z_1, z_2.

We have the following proposition on loops.

Proposition 1.3.1. *[label=(0)]*

1. *x is a loop if and only if $x \in \operatorname{cl} \emptyset$.*
2. *If x is a loop and $x \in A$, then A is dependent.*
3. *If x is a loop then $x \in \operatorname{cl} A$ for all $A \subseteq S$.*
4. *x is a loop if and only if $\{x\}$ is a circuit.*
5. *x is a loop if and only if it cannot be contained in any base.*

Proof. [label=(0)]
If x is a loop, then $\{x\}$ is dependent and since $\operatorname{rank} \emptyset = 0$, we have $\operatorname{rank} \emptyset \cup \{x\} = \operatorname{rank} \emptyset = 0$, so $x \in \operatorname{cl} \emptyset$. Conversely if $x \in \operatorname{cl} \emptyset$, then $\operatorname{rank} \emptyset \cup \{x\} = \operatorname{rank} \emptyset = 0$, and since $x \in S$, $\{x\}$ is dependent.

2. This is clear by definition and by (1).

3. If x is a loop and if A were independent, then that would make $\{x\}$ independent; absurd.

4. For $A \subseteq S$, since x is a loop, $\operatorname{rank} A \cup x = \operatorname{rank} A$, so $x \in \operatorname{cl} A$.

5. This is clear by definition.

6. This follows from the contrapositive of proposition 1.1.6.

□

Corollary. *A loop belongs to every flat.*

Proof. If x is a loop and F is an arbitrary flat, then $x \in \operatorname{cl} \emptyset \subseteq \operatorname{cl} F$, and we also have that $x \in \operatorname{cl} F$, thus $x \in F$. □

Corollary. *$\emptyset$ is a flat if and only if M has no loops.*

Proof. If $\emptyset$ is a flat, then for every $x \in S$, $\operatorname{rank} \emptyset \cup x = \operatorname{rank} \emptyset + 1$, thus there are no elements depending on $\emptyset$, thus there are no loops in M.

Conversely if there are no loops in M, and $\emptyset$ is not a flat, then there is some element in $x \in S$ for which $\operatorname{rank} \emptyset \cup x = \operatorname{rank} \emptyset$, thus $\{x\}$ is dependent, which makes x a loop; absurd. □

And the following proposition for parallel elements.

Proposition 1.3.2. *[label=(0)]*

1. *Distinct elements x and y are parallel if and only if $\{x, y\}$ is a circuit.*

2. *If x is parallel to y and y is parallel to z, then x is parallel to z.*

3. *If $x \neq y$, x is parallel to y if and only if $x \in \operatorname{cl} y$ and $y \in \operatorname{cl} x$, and they are both not loops.*

4. *If $x \in \operatorname{cl} A$ for $A \subseteq S$, and x is parallel to y, then $y \in \operatorname{cl} A$.*

5. *If A contains two parallel elements, then A must be dependent.*

Proof. [label=(0)]

If $x = y$, then x is a loop. Now if $x \neq y$ and x and y are parallel, then $\{x, y\}$ is dependent, and $\{x\}$ isn't a loop (hence it is independent), thus $\{x, y\}$ is minimally dependent. On the on the other hand, if $\{x, y\}$ is a circuit, then both $\{x\}$ and $\{y\}$ are independent, thus they are not loops, so x and y are parallel.

2. If x is parallel to y, then $\{x, y\}$ is dependent, and if y and z are parallel, then $\{y, z\}$ is also dependent. Then by the circuit elimination axiom, $\{x, y\}$ is dependent, and x and z are both not loops, hence they are parallel.

3. If x is parallel to y, then $\operatorname{rank}\{x,y\} = \operatorname{rank}\{y\}$ likewise $\operatorname{rank}\{x,y\} = \operatorname{rank} x$, thus $x \in \operatorname{cl}\{y\}$ and $y \in \operatorname{cl}\{x\}$; that they are both not parallel follows by definition.

4. If x depends on A, and x is parallel to y, then $\operatorname{rank} A \cup y = \operatorname{rank} A$, hence y also depends on A.

5. This is obvious by the inheritance axiom.

□

1.4 Independent Sets and Bases.

It is clear that if A is an independent set, then there is a base B for which $A \subseteq B$.

Theorem 1.4.1 (The Augmentation Theorem)**.** *Suppose that X and Y are independent in a matroid M, and that $|X| < |Y|$, then there is a $Z \subseteq X\backslash y$ such that $|X \cup Z| = |Y|$, and $X \cup Z$ is independent in M.*

Proof. Let Z_0 be such that for all $Z \subseteq X\backslash Y$, with $X \cup Z$ independent, $X \cup Z_0$ is maximally independent. Now if $|X \cup Z_0| < |Y|$, there is a $Y_0 \subseteq Y$ such that $|X \cup Z_0| < |Y_0|$, and since Y_0 is independent, by the augmentation axiom, there is a $y \in Y_0\backslash(X \cup Z_0)$ for which $X \cup Z_0 \cup y$ is independent. But $X \cup Z_0$ is maximal, a contradiction. □

Corollary. *Any two bases of a matroid on S have the same size, and $|B| = \operatorname{rank} S$ for any $B \in \mathcal{B}$.*

Proof. Suppose that there are bases $B_1, B_2 \in \mathcal{B}$ for which $|B_1| < |B_2|$. Then by the augmentation theorem, there is a $Z \subseteq B_2\backslash B_1$ for which $B_1 \cup Z$ is independent; but B_1 is maximally independent, which is a contradiction. Thus $|B_1| = |B_2|$ for any two bases $B_1, B_2 \in \mathcal{B}$. We also see that by the definition of rank, that $|B| = \operatorname{rank} S$ for any $B \in \mathcal{B}$. □

We can now give a proof of theorem 1.1.1.

Proof of theorem 1.1.1. If $\mathcal{B}$ is the set of bases of a matroid, then we have that $\mathcal{B} \neq \emptyset$, since $\emptyset \in \mathcal{I}$. Now let $B_1, B_2 \in \mathcal{B}$, then by the augmentation theorem, there is a $y \in B_2$ for which $|(B\backslash x) \cup y| = |B_2|$, thus $y \in B_2\backslash B_1$.

Conversely, let $\mathcal{B}$ be a nonempty collection of subsets for which axiom $(B1)$ holds. Define $\mathcal{I}$ the be the colection of all subsets X of S for which $X \subseteq B \in \mathcal{B}$. Clearly $\emptyset \in \mathcal{I}$, and if $X \in \mathcal{I}$, and $Y \subseteq X$, then $Y \subseteq B \in \mathcal{B}$, so $Y \in \mathcal{I}$.

Now let $X, Y \in \mathcal{I}$ with $|X| < |Y|$, and choose $B_1, B_2 \in \mathcal{B}$ For $B_1\backslash b$, by the augmentation theorem, there is a $z \in B_2$ for which $(B_2\backslash b \cup z) \in \mathcal{B}$. if $z \in Y$, we are done. Otherwise consider $((B_1\backslash b)\cup z)\backslash b'$ then there is a $z' \in B_2$ for which $((B_1\backslash b)\cup z)\backslash b' \cup z' \in \mathcal{B}$, then if $z' \in Y$, we are done. If not, then continue, and by induction on $|B_1|$, and since $|B_1| > |B_1\backslash Y|$, after atmost $|B_1|$ steps, we will reach a member of Y. Thus the augmentation axiom is satisfied. That is $\mathcal{B}$ is the collection of bases of M. □

Theorem 1.4.2. *A collection $\mathcal{I}$ of subsets of a set S is th collection of independent sets of a matroid on S if and only if $\mathcal{I}$ satisfies:*

(I′1) $\emptyset \in \mathcal{I}$

(I′2) If $X \in \mathcal{I}$, *and* $Y \subseteq X$, *then* $Y \in \mathcal{I}$.

(I′3) If $A \subseteq S$, *then for any two maximal subsets* $Y_1, Y_2 \subseteq A$, *with* $Y_1, Y_2 \in \mathcal{I}$, $|Y_1| = |Y_2|$.

Proof. If $\mathcal{I}$ is the collection of independent sets, cleary $(I'1)$ and $(I'2)$ are satisfied. Now if $(I'3)$ fails, then there are maximal set $Y_1, Y_2 \in \mathcal{I}$ for which $|Y_1| < |Y_2|$, then by the augmentation axiom, there is a $y \in Y_2 \backslash Y_1$ for which $Y_1 \cup y \in \mathcal{I}$, which contradicts maximality.

Conversely, if $\mathcal{I}$ satisfies $(I'1)$, $(I'2)$ and $(I'3)$, then clearly $(I1)$ and $(I2)$ are satisfied. Now let $U, V \in \mathcal{I}$ with $|U| < |V|$, and let $A = U \cup V$. Since all maximal subsets of A have the same size, there is an $x \in A$ for which $|x \cup U| = |V|$, by the augmentation theorem. So $x \cup U \in \mathcal{I}$, and we are done. □

Remark. $(I'1)$ and $(I'2)$ are just axioms $(I1)$ and $(I2)$, so they are satisfied trivially. it is also worth noting that the augmentation theorem implies the augmentation axiom.

Example 1.4.1. Let B_1, B_2 be distinct bases of a matroid M. Since $|B_1| = |B_2|$, we can put the elements of B_1 into a $1-1$ correspondence with those of B_2, that is map $e \to \pi(e)$, then $\pi : B_1 \to B_2$ is $1-1$ onto B_2; thus by $(B1)$, and the augmentation theorem, for $e \in B_1$, take $\pi(e) \in B_2$. then $(B_2 \cup e) \backslash \pi(e) = (B_2 \backslash \pi(e)) \cup e$ is a base of M.

Proposition 1.4.3. *Let* B_1, B_2 *be bases of a matroid* M. *Then for any* $e \in B_1$, *there is an* $f \in B_2$ *such that* $(B_1 \backslash e) \cup f$ *and* $(B_2 \backslash f) \cup e$ *are bases of* M.

Proof. By $(B1)$ and the augmentation theorem, there is an $f \in B_2$ for which $(B_1 \cup f) \backslash e$ is a base. Note that $(B_1 \cup f) \backslash e = (B_1 \backslash e) \cup f$. Similarly we get that $(B_2 \backslash f) \cup e$ is also a base of M. □

Corollary. *If* B_1 *and* B_2 *are bases of* M, *and* $X_1 \subseteq B_1$, *then there is an* $X_2 \subseteq B_2$ *for which* $(B_1 \backslash X_1) \cup X_2$ *and* $(B_2 \backslash X_2) \cup X_1$ *are bases of* M.

Proof. Take X_2 oto be the set of all such f for which $(B_1 \backslash X_1) \cup X_2$ and $(B_2 \backslash X_2) \cup X_1$ are bases of M, for $e \in B_1$. That is take the map f which takes $e \to f$ by this rule. Thus we get the result by taking the image of f. □

1.5 The Rank function.