1 Introduction

Matroids are abstract mathematical objects, like groups and topological spaces. Groups arise when we consider symmetries. Topologies arise when we think about continuity. Matroids are the abstract objects that we arrive at when we think about notions of dependence. There are notions of dependence in many different areas of mathematics, and matroids underlie many of these various ideas. We will start by thinking about geometric dependence.

Imagine a finite set of points E, arranged in the Euclidean plane $\mathbb{R}^2$ as shown in Figure 1.

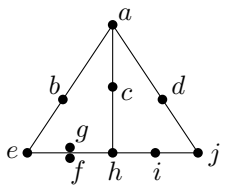

Figure 1: A collection of points in $\mathbb{R}^2$.

We have placed the points f and g next to each other, to indicate that they are in the same location. (Technically, this means that E is a *multiset* of points. We will make multisets formal later.) Let X be a three-element subset of E. We will say that X is a *basis* if there is no line of the plane (that is, a 2-dimensional affine subspace) that contains all the points in X; otherwise, X is not a basis. The plural of basis is *bases*. Therefore, in this example, $\{b, c, d\}$, $\{a, e, h\}$, and $\{c, f, i\}$ are bases, whereas $\{a, c, h\}$, $\{e, f, j\}$, and $\{f, g, d\}$ are not bases.

Geometric drawings such as in Figure 1 are essential for developing matroid intuition. We will see many examples. There are some important things we can note straight away:

(i) If three points are not explicitly shown on a line, then we do not assume them to be collinear. So in Figure 1, you might think that b, c, and d, are close to being on a line, but because this line is not explicitly drawn, we take them to be non-collinear.

(ii) We never draw a line that contains only two points. So for example, we have not drawn the line that contains b and h.

Exercise 1.1. Show that if B_1 and B_2 are bases in a geometric diagram and x is in $B_1 - B_2$, then there is some element $y \in B_2 - B_1$ such that $(B_1 - x) \cup y$ is a basis.

Remark. Note that if X and Y are sets, then we write $X - Y$ to denote the set difference $\{x \in X : x \notin Y\}$. (Often, this is instead written as $X \setminus Y$, but in matroid theory $X - Y$ is more common, so we follow that approach.) It is also standard in matroid theory to write x instead of $\{x\}$ to denote the set containing the single element x. ♢

The previous example described the bases in a collection of points in 2-dimensional space. We can extend this idea of bases to other dimensions. Let E be a finite set of points in $\mathbb{R}^3$. Let X be a four-element subset of E. We say that X is a *basis* if there is no plane (a 3-dimensional affine subspace) that contains X; otherwise, X is not a basis. For example, in Figure 2, $\{a, b, f, g\}$, $\{d, f, g, h\}$, and $\{b, c, f, h\}$ are bases. On the other hand, $\{a, b, c, d\}$, $\{a, b, g, h\}$, and $\{e, f, g, h\}$ are not bases.

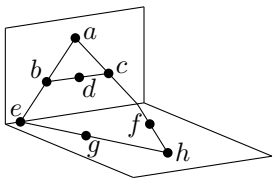

Figure 2: A discrete collection of points in $\mathbb{R}^3$.

Here are some further important points about geometric diagrams:

(iii) Three points that are on a line, along with any other point not on that line, lie on a common plane. So for example $\{a, b, e\}$ lies on a plane with any other point.

(iv) Any two lines that meet lie in a common plane. The line spanned by a and c and the line spanned by f and h meet, so those lines are contained in a common plane. This means that $\{a, c, f, h\}$ is not a basis.

In this 3-dimensional context, the property in Exercise 1.1 holds again: if B_1 and B_2 are bases, and $x \in B_1 - B_2$, then for some element $y \in B_2 - B_1$, $(B_1 - x) \cup y$ is a basis.

Finally, let us think about a discrete configuration of points on the real line $\mathbb{R}$. In this context, we are interested in a subset X of size two. If the two

points in X have different locations on the line, then X is a basis; otherwise, X is not a basis. In Figure 3, $\{a, e\}$ and $\{b, f\}$ are bases, while $\{b, c\}$ and $\{f, d\}$ are not bases.

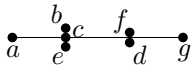

Figure 3: A discrete collection of points in $\mathbb{R}$.

Essentially, a matroid is an abstract structure that captures the property described in Exercise 1.1. With this motivation in hand, we give our first definition of matroids.

Definition 1.2. A *matroid* is a pair $(E, \mathcal{B})$, where E is a finite set, and $\mathcal{B}$ is a family of subsets of E obeying the following axiom:

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

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

Thus we can see matroids as being abstractions of discrete collections of points in space. The members of $\mathcal{B}$ are called *bases*. We say that E is the *ground set* of the matroid $(E, \mathcal{B})$. If M is a matroid, then we write $E(M)$ to denote the ground set of M, and $\mathcal{B}(M)$ to denote its set of bases. Figures 1, 2, and 3 are what we call *geometric representations* of matroids.

What does this have to do with 'dependence'? One can think of a basis as a maximal 'independent' set, so a set of points is 'independent' if and only if it is contained in a basis. Many texts on matroid theory choose to start with the notion of independent sets, and define a matroid using this notion. This viewpoint is equivalent; we will return to it a bit later on.

Proposition 1.3. *Let M be a matroid. The members of $\mathcal{B}(M)$ have the same size.*

Proof. Assume that the result is false. Let B_1 and B_2 be bases such that $|B_1| > |B_2|$, and assume that among all such bases, we have chosen B_1 and B_2 so that $|B_1 \cap B_2|$ is as large as possible. Because B_1 is larger than B_2, there is an element, x, in $B_1 - B_2$, and hence there is an element $y \in B_2 - B_1$ such that $B_1' = (B_1 - x) \cup y$ is in $\mathcal{B}$. Now B_1' and B_2 are bases, and $|B_1'| = |B_1| > |B_2|$, but $B_1' \cap B_2 = (B_1 \cap B_2) \cup y$, so this contradicts our choice of B_1 and B_2. □

Uniform matroids. For our first example of a family of matroids, let E be a finite set of size n, and let r be an integer satisfying $0 \leq r \leq n$. Let

$$\mathcal{B} = \{B \subseteq E \colon |B| = r\}.$$

It is very easy to check that $\mathcal{B}$ is non-empty and satisfies axiom **B2**. Therefore $(E, \mathcal{B})$ is a matroid, denoted by $U_{r,n}$. Any matroid of this type is known as a *uniform matroid*. Figure 4 contains a geometric representation of the uniform matroid $U_{3,6}$. This representation works in exactly the same way as the one in Figure 1: because no line in the plane contains three points in the collection, every three-element subset is a basis.

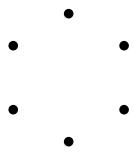

Figure 4: A geometric representation of $U_{3,6}$.

Although the uniform matroids are not complicated, they play an important role. The uniform matroid $U_{0,0}$ is sometimes called the *empty matroid*.

Isomorphisms. Note that matroids with different ground sets cannot be equal. So it seems that we have an infinite number of matroids that could be called $U_{r,n}$, corresponding to an infinite number of possible ground sets. We avoid this problem by introducing the notion of matroid isomorphism. If $M_1 = (E_1, \mathcal{B}_1)$ and $M_2 = (E_2, \mathcal{B}_2)$ are matroids, where $\mathcal{B}_1$ and $\mathcal{B}_2$ are families that obey **B1** and **B2**, then an *isomorphism* from M_1 to M_2 is a bijection $\psi \colon E_1 \to E_2$ such that a subset $B \subseteq E_1$ belongs to $\mathcal{B}_1$ if and only if $\psi(B) = \{\psi(b) \colon b \in B\}$ belongs to $\mathcal{B}_2$. In this case, M_1 and M_2 are *isomorphic*. We denote this by writing $M_1 \cong M_2$. So, rather than denoting a unique matroid, $U_{r,n}$ denotes an isomorphism class of matroids. We will often blur the distinction between a matroid and the class of matroids that are isomorphic to it.

Sparse paving matroids.

Exercise 1.4. Let E be a finite set, and let r be an integer such that $0 < r < |E|$. Let $\mathcal{C}$ be a collection of r-element subsets of E such that if C_1 and C_2 are distinct members of $\mathcal{C}$, then $|C_1 \cap C_2| < r - 1$. Let $\mathcal{B}$ be the family of

r-element subsets that are not in $\mathcal{C}$. That is, $\mathcal{B} = \{B \subseteq E \colon |B| = r,\ B \notin \mathcal{C}\}$. Prove that $\mathcal{B}$ is the family of bases of a matroid.

Any matroid of the type described in Exercise 1.4 is known as a *sparse paving matroid*. In addition, if E is a finite set, and $\mathcal{B}$ is either $\{\emptyset\}$ or E, then $(E, \mathcal{B})$ is a sparse paving matroid. Note that $\mathcal{B} = \{\emptyset\}$ is not forbidden by the axiom **B1**, since $\mathcal{B}$ contains exactly one set (the empty set), and therefore $\mathcal{B}$ is not empty.

Exercise 1.5. Verify that every uniform matroid is a sparse paving matroid.

Independent sets, circuits, and rank. As we have mentioned, the definition of a matroid that we started with is not the one most commonly found at the beginning of a matroid theory textbook. We now pivot to the other definition.

Definition 1.6. Let M be a matroid. A subset of $E(M)$ is *independent* in M if it is a subset of a basis. A set that is not independent is *dependent*. We use $\mathcal{I}(M)$ to denote the family of independent sets of the matroid M.

Because the bases of M are equicardinal by Proposition 1.3, it follows that no basis is properly contained in another. Therefore the bases of M are exactly the maximal independent sets. (Meaning that a subset is a basis if and only if it is independent, but is not properly contained in any independent set.)

Assume that E is a finite set, and that $\mathcal{I}$ is a collection of subsets of E. Consider the following conditions on $\mathcal{I}$.

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 and I_2 are in $\mathcal{I}$, and $|I_2| < |I_1|$, then there is an element $e \in I_1 - I_2$ such that $I_2 \cup e \in \mathcal{I}$.

Property **I3** is sometimes called the *augmentation* or *independence extension* axiom.

Theorem 1.7. *Let M be a matroid, and let $\mathcal{I}$ be its family of independent sets. Then $\mathcal{I}$ satisfies* **I1**, **I2**, *and* **I3**. *Conversely, assume that E is a finite set and $\mathcal{I}$ is a family of subsets of E. If $\mathcal{I}$ satisfies* **I1**, **I2**, *and* **I3**, *then $\mathcal{I}$ is the family of independent sets of a matroid M, and the bases of M are exactly the maximal members of $\mathcal{I}$.*

Proof. Let M be a matroid on the ground set E. Let $\mathcal{B}$ and $\mathcal{I}$ be the families of bases and independent sets of M, respectively. First we show that $\mathcal{I}$ satisfies **I1**, **I2**, and **I3**. By **B1**, $\mathcal{B}$ is non-empty, so M has at least one basis. The empty set is a subset of this basis, so the empty set is independent, and hence **I1** is satisfied.

Let $I \in \mathcal{I}$. Then I is contained in a maximal independent set B. For any $I' \subseteq I$, we also have $I' \subseteq B$, so I' is independent. Hence **I2** is also satisfied.

Assume that **I3** fails, so there are members, I_1 and I_2, of $\mathcal{I}$ such that $|I_2| < |I_1|$, and $I_2 \cup e \notin \mathcal{I}$ for every element $e \in I_1 - I_2$. Since I_2 belongs to $\mathcal{I}$, it is contained in some basis B_2. Similarly, I_1 is contained in a basis B_1. Suppose that B_1 and B_2 have been chosen so that $B_1 \cap B_2$ is as large as possible. If there is some element x that is in $(I_1 \cap B_2) - I_2$, then $x \in I_1 - I_2$, and $I_2 \cup x$ belongs to $\mathcal{I}$ (since it is a subset of B_2). But this contradicts our assumption that **I3** fails. Therefore every element of $I_1 \cap B_2$ belongs to I_2, which means that

$$I_1 - B_2 = I_1 - I_2. \tag{1.1}$$

Next we assume that there is an element $x \in B_1 - (I_1 \cup B_2)$. Then x is in $B_1 - B_2$. By **B2**, there is an element $y \in B_2 - B_1$ such that $(B_1 - x) \cup y$ belongs to $\mathcal{B}$. But $(B_1 - x) \cup y$ contains I_1, and it intersects B_2 in one more element than B_1 does. Therefore our choice of B_1 and B_2 is contradicted. This implies that $B_1 - (I_1 \cup B_2)$ is empty, and this means that $B_1 - B_2 = I_1 - B_2$. Equation (1.1) now shows that

$$B_1 - B_2 = I_1 - I_2. \tag{1.2}$$

Next we assume that there is an element $x \in B_2 - (I_2 \cup B_1)$. Then x is in $B_2 - B_1$, so by **B2**, there is an element $y \in B_1 - B_2$ such that $(B_2 - x) \cup y$ belongs to $\mathcal{B}$. But $I_2 \subseteq (B_2 - x) \cup y$, and $(B_2 - x) \cup y$ intersects B_1 in one more element than B_2. This contradicts our choice of B_1 and B_2, so $B_2 - (I_2 \cup B_1)$ is empty. This means that $B_2 - B_1 = I_2 - B_1$. Since $B_2 - B_1 = I_2 - B_1 \subseteq I_2 - I_1$, we see that

$$|B_2 - B_1| \leq |I_2 - I_1|. \tag{1.3}$$

Now B_1 and B_2 have the same size by Proposition 1.3, so $|B_1 - B_2| = |B_2 - B_1|$. By applying Equations (1.2) and (1.3), we see that

$$|I_1 - I_2| = |B_1 - B_2| = |B_2 - B_1| \leq |I_2 - I_1|.$$

Therefore

$$|I_1| = |I_1 \cap I_2| + |I_1 - I_2| \leq |I_1 \cap I_2| + |I_2 - I_1| = |I_2|,$$

and we have a contradiction to our original assumption that $|I_2| < |I_1|$. Thus **I3** is satisfied, and this completes the first half of the proof.

For the converse, we let E be a finite set, and we let $\mathcal{I}$ be a collection of subsets of E. We assume $\mathcal{I}$ satisfies **I1**, **I2**, and **I3**. Let $\mathcal{B}$ be the collection of maximal members of $\mathcal{I}$. Then each $B \in \mathcal{B}$ is a member of $\mathcal{I}$ and, since **I2** holds, every subset of B is also in $\mathcal{I}$. Moreover, if I is in $\mathcal{I}$, then I is a subset of a maximal member of $\mathcal{I}$, which is to say I is a subset of a member of $\mathcal{B}$. This demonstrates that the members of $\mathcal{I}$ are exactly the subsets of the members of $\mathcal{B}$. Therefore, if $\mathcal{B}$ is the family of bases of a matroid M, then $\mathcal{I}$ is the family of independent sets of M. Now, to complete the proof we need only show that $\mathcal{B}$ satisfies **B1** and **B2**.

Because the empty set is in $\mathcal{I}$, there is at least one member of $\mathcal{I}$, so there is at least one maximal member of $\mathcal{I}$. Therefore $\mathcal{B}$ is non-empty, so **B1** holds. Next we claim that the members of $\mathcal{B}$ have the same cardinality. Suppose this is not the case, so there are members $B_1, B_2 \in \mathcal{B}$ such that $|B_2| < |B_1|$. Since B_1 and B_2 are members of $\mathcal{I}$, **I3** implies that there is an element $e \in B_1 - B_2$ such that $B_2 \cup e$ is in $\mathcal{I}$. This contradicts the fact that B_2 is a maximal member of $\mathcal{I}$. This proves that the members of $\mathcal{B}$ have the same cardinality.

Next we prove that **B2** holds. Let B_1 and B_2 be members of $\mathcal{B}$, and let x be an element in $B_1 - B_2$. As $|B_1| = |B_2|$, it follows that $|B_1 - x| < |B_2|$. Now B_1 is in $\mathcal{I}$, so $B_1 - x$ is also in $\mathcal{I}$, by **I2**. By **I3**, there is an element $y \in B_2 - (B_1 - x)$ such that $(B_1 - x) \cup y$ is in $\mathcal{I}$. Note that $y \neq x$, since $x \notin B_2$ but $y \in B_2$. Therefore y is in $B_2 - B_1$. Also, $|(B_1 - x) \cup y| = |B_1|$. Since maximal members of $\mathcal{I}$ have the same cardinality, we deduce that $(B_1 - x) \cup y$ is a maximal member of $\mathcal{I}$, and hence a member of $\mathcal{B}$. Therefore **B2** holds.□

From Theorem 1.7 we see that we could have defined a matroid via the statements **I1**, **I2**, and **I3** just as easily as via the statements **B1** and **B2**. From now on we will often not specify which axiom scheme we are using to define a matroid.

In fact, there are many more axioms schemes that could be used to define matroids. We will note two of these schemes here.

Definition 1.8. Let M be a matroid. A subset of $E(M)$ is a *circuit* in M if it is a minimal dependent set. That is, $C \subseteq E(M)$ is a circuit if it is dependent and all of its proper subsets are independent. We use $\mathcal{C}(M)$ to denote the family of circuits of the matroid M.

Let M be a matroid with ground set E. Notice that a subset of E is dependent if and only if it contains a circuit. The bases of M are exactly

the maximal subsets of E that do not contain any circuit. If $\{e\}$ is a circuit of the matroid M, then e is known as a *loop*. Similarly, a circuit of size two is known as a *parallel pair*. A *parallel class* is a subset P of E such that every pair of elements in P is a parallel pair, and P is maximal with respect to this property. When drawing a geometric representation of a matroid, we place parallel elements adjacent to each other. We place loops in a box to one side.

Exercise 1.9. Characterise the circuits of uniform and sparse paving matroids.

Exercise 1.10. If C is a circuit of a matroid, then every proper subset of C is independent. Give an example of a matroid with an independent set that is not contained in any circuit.

Let E be a finite set, and let $\mathcal{C}$ be a family of subsets of E. Consider the following properties:

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 are distinct members of $\mathcal{C}$ and $e \in C_1 \cap C_2$, then $(C_1 \cup C_2) - e$ contains a member of $\mathcal{C}$.

Property **C3** is sometimes referred to as the *circuit-elimination* axiom.

Theorem 1.11. *Let M be a matroid, and let $\mathcal{C}$ be its family of circuits. Then $\mathcal{C}$ satisfies* **C1**, **C2**, *and* **C3**. *Conversely, assume that E is a finite set and $\mathcal{C}$ is a family of subsets of E. If $\mathcal{C}$ satisfies* **C1**, **C2**, *and* **C3**, *then it is the collection of circuits of a matroid M, and the independent sets of M are exactly the subsets of E that do not contain any member of $\mathcal{C}$ as a subset.*

Next we state a very useful property of circuits.

Proposition 1.12. *Suppose that I is an independent set of a matroid M, and that $I \cup e$ is dependent for some element $e \in E(M) - I$. Then $I \cup e$ contains a unique circuit, and this circuit contains e.*

Proof. Since $I \cup e$ is dependent, it certainly contains a circuit. Any circuit in $I \cup e$ contains e, for otherwise I contains a circuit, which contradicts the fact that it is independent. Assume $I \cup e$ contains two distinct circuits, C_1 and C_2. Then $e \in C_1 \cap C_2$, so **C3** tells us that $(C_1 \cup C_2) - e$ contains a circuit. But $(C_1 \cup C_2) - e$ is contained in I, so we have a contradiction. □

We note one more method for axiomatising matroids.

Definition 1.13. Let M be a matroid. The *rank function* of M is the function r_M that takes any subset $X \subseteq E(M)$ to the number

$$\max\{|I|\colon I \subseteq X,\ I \text{ is independent in } M\}.$$

When there is no ambiguity as to the matroid in question, we write $r(X)$ rather than $r_M(X)$.

Equivalently, $r(X)$ is the size of a maximal independent set contained in X. Notice that a subset of $E(M)$ is independent in M if and only if its cardinality is equal to its rank. The rank of a matroid, denoted $r(M)$, is the size of a basis in that matroid. Note that $r(M) = r(E(M))$. Geometric representations of rank-2, rank-3, and rank-4 matroids are collections of points on a line, plane, and in 3-dimensional space, respectively.

Exercise 1.14. Characterise bases, independent sets, and circuits, using only the rank function.

Exercise 1.15. Let M be a matroid and let X be a subset of $E(M)$. Show that if I and I' are maximal independent subsets of X, then $|I| = |I'|$.

Let E be a finite set, and let r be a function taking subsets of E to the integers. Consider the following properties of r.

R1. $0 \leq r(X) \leq |X|$ for all $X \subseteq E$.

R2. $r(Y) \leq r(X)$ for all $X, Y \subseteq E$ such that $Y \subseteq X$.

R3. $r(X) + r(Y) \geq r(X \cup Y) + r(X \cap Y)$ for all $X, Y \subseteq E$.

Property **R3** is known as *submodularity*.

Theorem 1.16. *Let M be a matroid, and let r be its rank function. Then r satisfies* **R1**, **R2**, *and* **R3**. *Conversely, assume E is a finite set and r is a function taking subsets of E to integers. If r satisfies* **R1**, **R2**, *and* **R3**, *then it is the rank function of a matroid M, and the independent sets of M are exactly the subsets, $I \subseteq E$, satisfying $r(I) = |I|$.*

There are many many other schemes for axiomatising matroids. We will see some more of them in the future. We will prove Theorems 1.11 and 1.16 in Section 6.