6 Cryptomorphisms

We have already mentioned that there are many different, but equivalent, ways of defining a matroid. These different axiom schemes are called *cryptomorphisms*. This chapter is dedicated to collecting and justifying some of them.

Throughout this chapter, E will be a finite set. For the sake of completeness, let us start by restating the basis and independence axioms for matroids. Let $\mathcal{B}$ and $\mathcal{I}$ be families of subsets of E. The basis axioms are as follows.

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 $(B_1 - x) \cup y \in \mathcal{B}$.

The independence axioms are as follows.

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 $I_2 \cup e \in \mathcal{I}$.

The orthodox path is to define a matroid to be a pair $(E, \mathcal{I})$, where $\mathcal{I}$ is a family satisfying **I1**, **I2**, and **I3**. Then the independent sets are the members of $\mathcal{I}$, and the bases are the maximal members of $\mathcal{I}$. This is the approach you will find in most matroid textbooks. In Section 1 we took a different approach, and defined a matroid to be a pair $(E, \mathcal{B})$, where $\mathcal{B}$ is a family satisfying **B1** and **B2**. Then the members of $\mathcal{B}$ are bases, and their subsets are the independent sets. Of course, these two different approaches are equivalent because of Theorem 1.7, which we restate here in a slightly different way.

Theorem 6.1. *Let E be a finite set. If $\mathcal{B}$ is a family of subsets of E satisfying* **B1** *and* **B2**, *and*

$$\mathcal{I} = \{I \subseteq E \colon I \subseteq B \text{ for some } B \in \mathcal{B}\},$$

then $\mathcal{I}$ satisfies **I1**, **I2**, *and* **I3**. *Conversely, if $\mathcal{I}$ is a family of subsets of E satisfying* **I1**, **I2**, *and* **I3**, *and $\mathcal{B}$ is the set of maximal members of $\mathcal{I}$, then $\mathcal{B}$ satisfies* **B1** *and* **B2**.

Therefore we are free to define matroids via bases or independent sets, as we wish.

Recall that a circuit of a matroid is a minimal dependent set. Let $\mathcal{C}$ be a family of subsets of E. The circuit axioms are as follows.

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 $\mathcal{C}$.

We now restate and prove Theorem 1.11.

Theorem 6.2. *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.*

Proof. Let $\mathcal{C}$ be the family of circuits of a matroid. Because the empty set is independent by **I1**, it cannot be a circuit. Therefore **C1** holds. **C2** holds because circuits are minimal dependent sets by definition.

Now we prove that **C3** holds. Let C_1 and C_2 be distinct circuits, and assume e is in $C_1 \cap C_2$. Suppose that $(C_1 \cup C_2) - e$ does not contain a circuit. Then it is independent. Since C_1 and C_2 are distinct circuits, neither one of them is contained in the other, by **C2**. Therefore there is some element f in $C_1 - C_2$. By the definition of a circuit, $C_1 - f$ is independent. Let I be a maximum-sized independent subset of $C_1 \cup C_2$ that contains $C_1 - f$. If $|I| < |(C_1 \cup C_2) - e|$, then by **I3**, there is an element in $(C_1 \cup C_2) - e$ that is not in I, that can be added to I to create a larger independent set. This contradicts the definition of I, so $|I| \geq |(C_1 \cup C_2) - e|$. However, f is not in I, because otherwise I contains the dependent set C_1, and this contradicts **I2**. Therefore $I \subseteq (C_1 \cup C_2) - f$, so $|I| \leq |(C_1 \cup C_2) - f| = |(C_1 \cup C_2) - e|$. This means that $|I| = |(C_1 \cup C_2) - e| = |(C_1 \cup C_2) - f|$, and therefore $I = (C_1 \cup C_2) - f$. But this set contains the circuit C_2, which is a contradiction as I is independent. Therefore **C3** holds.

For the converse, we let $\mathcal{C}$ be a family of subsets of the finite set E satistfying **C1**, **C2**, and **C3**. Let

$$\mathcal{I} = \{I \subseteq E \colon X \notin \mathcal{C} \text{ for all } X \subseteq I\}.$$

We want to show that $\mathcal{I}$ satisfies **I1**, **I2**, and **I3**.

The condition **C1** shows that $\emptyset \notin \mathcal{C}$, so the empty set contains no member of $\mathcal{C}$. Therefore $\emptyset \in \mathcal{I}$, and **I1** is satisfied. If $I_1 \subseteq E$ contains no member of $\mathcal{C}$, then clearly no subset of I_1 contains a member of $\mathcal{C}$. Therefore all subsets of I_1 are contained in $\mathcal{I}$, and **I2** is satisfied.

Now we suppose that I_2 and I_1' are members of $\mathcal{I}$, and that $|I_2| < |I_1'|$, but **I3** fails for this pair. There is at least one member of $\mathcal{I}$ contained in $I_1' \cup I_2$ that is strictly larger than I_2 (since I_1' is such a subset). Amongst all such subsets, assume that I_1 has been chosen so that $I_1 \cap I_2$ is as large as possible. If I_2 were contained in I_1, then we would be able to extend I_2 by a single element in $I_1 - I_2$ and remain in $\mathcal{I}$. Since the element in $I_1 - I_2$ is also in $I_1' - I_2$, this contradicts our assumption that **I3** fails for I_1' and I_2, so $|I_2 - I_1| > 0$. Let e be an element in $I_2 - I_1$.

Since $|I_1| > |I_2|$, the set $I_1 - I_2$ is non-empty. We claim that for any $f \in I_1 - I_2$, the set $(I_1 \cup e) - f$ contains a member of $\mathcal{C}$. Let $f \in I_1 - I_2$. Now $(I_1 \cup e) - f$ is contained in $I_1' \cup I_2$, and is strictly larger than I_2. Furthermore, it meets I_2 in one more element (namely e) than I_1 does. Therefore $(I_1 \cup e) - f$ does not belong to $\mathcal{I}$, or else our choice of I_1 is contradicted. Thus $(I_1 \cup e) - f$ contains a member of $\mathcal{C}$, as claimed.

Let f_1 be any element in $I_1 - I_2$, so $(I_1 \cup e) - f_1$ contains a member, C_1, of $\mathcal{C}$. If $C_1 \cap (I_1 - I_2)$ is empty, then C_1 is contained in I_2, and this contradicts our assumption that $I_2 \in \mathcal{I}$. Therefore, there is some element f_2 in $C_1 \cap (I_1 - I_2)$. As $f_2 \in I_1 - I_2$, there is some member of $\mathcal{C}$ contained in $(I_1 \cup e) - f_2$. Let us call this member C_2. Note that both C_1 and C_2 contain e, for otherwise one of C_1 or C_2 is contained in I_1, which contradicts the fact that I_1 is in $\mathcal{I}$. Moreover, C_1 and C_2 are distinct, for C_2 cannot contain f_2 as it is contained in $(I_2 \cup e) - f_2$, and f_2 was chosen so that it belongs to C_1. Now **C3** says that there is a member of $\mathcal{C}$ contained in $(C_1 \cup C_2) - e$. But $(C_1 \cup C_2) - e$ is contained in I_1, and this contradicts the fact that I_1 is in $\mathcal{I}$. Therefore **I3** holds.

We have shown that $\mathcal{I}$ is the family of independent sets of a matroid M. We complete the proof by showing that $\mathcal{C}$ is the family of circuits of M. Note that $X \subseteq E$ is dependent in M if and only if it is not in $\mathcal{I}$, which means that X contains a member of $\mathcal{C}$. Therefore X is a circuit of M if and only if it is minimal with respect to containing a member of $\mathcal{C}$. It is clear that this is true if and only if X is itself a member of $\mathcal{C}$. Thus $\mathcal{C}$ is exactly the family of circuits of M, as required. □

Next we consider the rank function. Recall that if M is a matroid and X is a subset of $E(M)$, then $r(X)$ is the cardinality of a maximum-sized independent subset of X. The rank axioms are the following conditions on a function r from subsets of E to the integers.

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 $X, Y \subseteq E$.

Now we restate and prove Theorem 1.16.

Theorem 6.3. *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 the 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 $r(I) = |I|$.*

Proof. Let r be the rank function of the matroid M. Since $r(X)$ is the cardinality of a subset of X, it certainly satisfies **R1**. If $Y \subseteq X$, then any independent subset of Y is also an independent subset of X. This implies that **R2** holds.

Next we prove that **R3** holds. Let X and Y be arbitrary subsets of $E(M)$. Let B be a maximum-sized independent set in $X \cap Y$, so that $|B| = r(X \cap Y)$. Now let B' be a maximum-sized independent set contained in $X \cup Y$ such that B' contains B. We claim that $|B'| = r(X \cup Y)$. If not, then there is an independent set I contained in $X \cup Y$ that is larger than B'. But **I3** then implies that there is an element e in $I - B'$ such that $B' \cup e$ is independent. However $B' \cup e$ is contained in $X \cup Y$, and contains B. Moreover, it is larger than B', so our choice of B' is contradicted. Therefore B' is a maximum-sized independent set contained in $X \cup Y$, and hence $r(X \cup Y) = |B'|$.

We now divide B' into three parts. Let B_1 be the intersection of B' with $X \cap Y$, let B_X be the intersection of B' with $X - Y$, and let B_Y be the intersection of B' with $Y - X$. We claim that $B_1 = B$. Certainly B is contained in B_1, since B is contained in the intersection of B' with $X \cap Y$. If B_1 is not equal to B, then B_1 is larger than B, and this contradicts our choice of B, since B_1 is independent (on account of it being a subset of B') and contained in $X \cap Y$. Therefore $B_1 = B$, so $|B_1| = r(X \cap Y)$.

Now

$$\begin{aligned} r(X \cup Y) + r(X \cap Y) &= |B'| + |B_1| = (|B_X| + |B_1| + |B_Y|) + |B_1| \\ &= (|B_X| + |B_1|) + (|B_Y| + |B_1|) = |B' \cap X| + |B' \cap Y|. \end{aligned}$$

As $B' \cap X$ is independent and contained in X it follows that $|B' \cap X| \leq r(X)$. Similarly, $|B' \cap Y| \leq r(Y)$. Therefore **R3** holds.

For the converse, we let r be a function taking the subsets of E to integers, and we assume that **R1**, **R2**, and **R3** hold. Let

$$\mathcal{I} = \{I \subseteq E \colon r(I) = |I|\}.$$

We will show that $\mathcal{I}$ satisfies **I1**, **I2**, and **I3**.

By **R1**, $0 \leq r(\emptyset) \leq |\emptyset| = 0$, so $r(\emptyset) = 0 = |\emptyset|$. Therefore the empty set belongs to $\mathcal{I}$, and **I1** is satisfied. Suppose that I_1 belongs to $\mathcal{I}$ and that I_2 is a subset of I_1. By applying **R3** we see that

$$\begin{aligned} r(I_2) + r(I_1 - I_2) &\geq r(I_2 \cup (I_1 - I_2)) + r(I_2 \cap (I_1 - I_2)) \\ &= r(I_1) + r(\emptyset) \\ &= |I_1|, \end{aligned}$$

using that $r(I_1) = |I_1|$, as I_1 is in $\mathcal{I}$, and $r(\emptyset) = 0$. So $r(I_2)+r(I_1-I_2) \geq |I_1|$. By applying **R1** we see that

$$|I_1| = |I_2| + |I_1 - I_2| \geq r(I_2) + r(I_1 - I_2) \geq |I_1|.$$

Therefore equality holds, so $|I_2| + |I_1 - I_2| = r(I_2) + r(I_1 - I_2)$, implying

$$|I_2| - r(I_2) = r(I_1 - I_2) - |I_1 - I_2|.$$

Now **R1** implies that the left side of the last equation is non-negative, and the right side is non-positive. Therefore both sides are zero, so $|I_2| = r(I_2)$. Therefore I_2 belongs to $\mathcal{I}$, so **I2** is satisfied.

To prove that **I3** is satisfied, we assume otherwise, and let I_1 and I_2 be members of $\mathcal{I}$ such that $|I_2| < |I_1|$, but $I_2 \cup e \notin \mathcal{I}$ for every element $e \in I_1 - I_2$. Now let e be an arbitrary element in $I_1 - I_2$, so $r(I_2 \cup e) \neq |I_2 \cup e|$. By **R1**, $r(I_2 \cup e)$ does not exceed $|I_2 \cup e|$, so $r(I_2 \cup e) < |I_2 \cup e|$. Equivalently, $r(I_2 \cup e) + 1 \leq |I_2 \cup e|$. Since $I_2 \in \mathcal{I}$, we have $|I_2| = r(I_2)$. So, using **R2**,

$$|I_2| + 1 = r(I_2) + 1 \leq r(I_2 \cup e) + 1 \leq |I_2 \cup e| = |I_2| + 1.$$

As equality holds, we deduce that $r(I_2 \cup e) = r(I_2)$ for any element $e \in I_1 - I_2$. Now Proposition 5.5 shows that $r(I_2) = r(I_2 \cup (I_1 - I_2)) = r(I_1 \cup I_2)$. Using **R2** and the fact that both I_1 and I_2 are in $\mathcal{I}$, we see that

$$|I_1| = r(I_1) \leq r(I_1 \cup I_2) = r(I_2) = |I_2| < |I_1|.$$

Now we have a contradiction, so **I3** holds.

We have shown that $\mathcal{I}$ is the family of independent sets of a matroid M. We now need to show that the rank function of M is r. Let X be an arbitrary subset of E, and let s be the rank of X in M. We'll show that $s = r(X)$. Now s is the cardinality of a maximum-sized member I of $\mathcal{I}$ that is contained in X. So $s = |I| = r(I)$, as $I \in \mathcal{I}$.

If x is an arbitrary element of $X - I$, then $I \cup x$ is not in $\mathcal{I}$, because I is a maximum-sized member of $\mathcal{I}$ contained in X. Therefore $r(I \cup x) \neq |I \cup x|$. By **R2**, we deduce that $r(I \cup x) < |I \cup x|$, or equivalently $r(I \cup x) + 1 \leq |I \cup x|$. Again, using **R2**, we see

$$|I| + 1 = r(I) + 1 \leq r(I \cup x) + 1 \leq |I \cup x| = |I| + 1.$$

As equality holds throughout, we deduce that $r(I) = r(I \cup x)$. Since x was chosen arbitrarily from $X - I$, we can apply Proposition 5.5 and deduce that $s = r(I) = r(I \cup (X - I)) = r(X)$, as required. $\square$

We will state (without proof) three more axiom schemes for matroids. First of all, we can characterise matroids via the closure operator. Let cl be a function that takes the subsets of E to subsets of E, and consider the following properties.

CL1. $X \subseteq \mathrm{cl}(X)$ for all $X \subseteq E$.

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

CL3. $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$ for all $X \subseteq E$.

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

We saw, as Theorem 6.4, that the closure operator of a matroid satisfies **CL1**–**CL4**. In fact, the next theorem shows that for any set E and function from subsets of E to subsets of E satisfying **CL1**–**CL4**, the function is the closure operator of a matroid on E.

Theorem 6.4. *Let M be a matroid, and let* cl *be its closure operator. Then* cl *satisfies* **CL1**, **CL2**, **CL3**, *and* **CL4**. *Conversely, assume E is a finite set and* cl *is a function taking subsets of E to subsets of E. If* cl *satisfies* **CL1**, **CL2**, **CL3**, *and* **CL4**, *then it is the closure operator of a matroid M on ground set E, and the independent sets of M are precisely the subsets $I \subseteq E$ such that $e \notin \mathrm{cl}(I - e)$ for every $e \in I$.*

We can also axiomatise matroids via flats. Let $\mathcal{F}$ be a family of subsets of E. Consider the following properties of $\mathcal{F}$.

F1. $E \in \mathcal{F}$.

F2. If $F_1, F_2 \in \mathcal{F}$, then $F_1 \cap F_2 \in \mathcal{F}$.

F3. If $F \in \mathcal{F}$, and $\{F_1, \ldots, F_n\}$ are the minimal members of $\mathcal{F}$ that properly contain F, then $(F_1 - F, \ldots, F_n - F)$ is a partition of $E - F$.

Theorem 6.5. *Let M be a matroid, and let $\mathcal{F}$ be its family of flats. Then $\mathcal{F}$ satisfies* **F1**, **F2**, *and* **F3**. *Conversely, assume E is a finite set and $\mathcal{F}$ is a family of subsets of E. If $\mathcal{F}$ satisfies* **F1**, **F2**, *and* **F3**, *then it is the family of flats of a matroid M on ground set E, and the independent sets of M are exactly the subsets $I \subseteq E$ such that for every element $e \in I$, there is a set $F \in \mathcal{F}$ such that $I - e \subseteq F$ and $e \notin F$.*

We now consider yet another characterisation of matroids. This characterisation differs from those we have seen so far in that it has an algorithmic flavour. One attractive feature of this characterisation is that it highlights why matroids naturally arise in combinatorial optimisation.

We begin by discussing a well-known optimisation problem on graphs. Let $G = (V, E)$ be a connected graph and let w be a function from E into $\mathbb{R}$. We call w a *weight function* on G, and for all $X \subseteq E(G)$, we define the *weight* of X to be $\sum_{x \in X} w(x)$. We are interested in the problem of finding a minimum-weight spanning tree of G. For instance, an n-vertex graph G could represent n towns to be linked by a railway network, where the weight of an edge is the cost of adding a direct link between the two towns corresponding to the edge's ends. In this case, a minimum-weight spanning tree corresponds to the cheapest railway network that links all n towns.

One well-known solution to this problem is *Kruskal's algorithm*. This algorithm proceeds as follows. Initially, set $S = \emptyset$, where S represents a potential solution that will be constructed incrementally. Order the edges E from minimum weight to maximum weight. Then, proceed by considering these edges one by one, in order, adding an edge e to S if it does not introduce a cycle; that is, if $G[S \cup e]$ is a forest. When $|S| = n - 1$, then $G[S]$ is a spanning tree, which is output as a solution.

Kruskal's algorithm is an instance of a so-called "greedy algorithm", as it greedily selects, to include in the solution, whichever edge appears to be the best choice at that point in time. In other words, it makes a locally optimal choice, that may or may not be globally optimal. It turns out that this greedy approach does indeed give a globally optimal solution for the problem of finding a minimum-weight spanning tree. In fact, the success of the greedy algorithm depends on whether the underlying structure is a matroid.

The minimum-weight spanning tree problem is a particular instance of a more general optimisation problem. Let $\mathcal{I}$ be a collection of subsets of a finite set E, where $\mathcal{I}$ satisfies **I1** and **I2**. As before, let w be a function from E into $\mathbb{R}$, which we call the *weight function*, and define the *weight* of X to be $\sum_{x \in X} w(x)$, where $w(\emptyset) = 0$. The *optimisation problem* for $(\mathcal{I}, w)$ is to find a maximal member B of $\mathcal{I}$ of maximum weight. We call B a *solution* to this problem.

The *greedy algorithm* for the pair $(\mathcal{I}, w)$ proceeds as follows:

1. Set $I := \emptyset$.
2. While there is an element $e \in E - I$ such that $I \cup e$ is in $\mathcal{I}$, then choose such an element e' of maximum weight, set $I := I \cup e'$, and repeat.
3. Output I.

Given an instance of the minimum-weight spanning tree problem on a graph G with weight function w, by letting $\mathcal{I}$ be the forests of G, we see that this problem is just the optimisation problem $(\mathcal{I}, -w)$. Observe that Kruskal's algorithm is then just the greedy algorithm on $(\mathcal{I}, -w)$.

The greedy algorithm is evidently an efficient algorithm for an optimisation problem, provided it does indeed give us an optimal solution. The next theorem implies that, given a matroid M, the greedy algorithm on $(\mathcal{I}(M), w)$ is optimal, for any weight function $w : E(M) \to \mathbb{R}$. In particular, it follows that Kruskal's algorithm is an optimal algorithm for the minimum-weight spanning tree problem.

Let $\mathcal{I}$ be a family of subsets of a finite set E, and consider the following property:

G1. For all weight functions $w : E \to \mathbb{R}$, the greedy algorithm finds a maximal member of $\mathcal{I}$ of maximum weight.

It turns out that for any matroid M, the family of independent sets of M satisfy **G1**. This may be somewhat surprising, but what is even more surprising is that the greedy algorithm fails to give an optimal solution for everything else.

Theorem 6.6. *Let $\mathcal{I}$ be a collection of subsets of a finite set E. Then $\mathcal{I}$ is the family of independent sets of a matroid on ground set E if and only if $\mathcal{I}$ satisfies* **I1**, **I2**, *and* **G1**.

Another well-known efficient algorithm for finding a minimum-weight spanning tree is *Prim's algorithm.* We will not describe this algorithm here, but it also employs a greedy-type strategy, which turns out to be optimal. However, the optimality of this algorithm is not explained by the fact the underlying structure is a matroid, but because it is a more general structure known as a *greedoid.* Every matroid is a greedoid but the converse is not true: for a greedoid, only a weaker version of **I2** needs to hold.