# Matroids and Greed

Will Dana

July 25, 2019

## 1 Why Matroids?

A matroid is a mathematical structure which captures, in a broad sense, the idea of "independent subsets" of a set. There are two key examples of this which appear in every talk in matroids (though they are far from the only ones):

**Example 1.** Let $E = \{e_1, \ldots, e_m\}$ be a finite collection of vectors in some ambient vector space $V$. Then certain subsets of these vectors will be linearly independent, and other subsets may not. We can look at this as a question of redundancy: if a subset of the vectors is linearly independent, then we can represent any other vector in their span as a linear combination of them in a unique way. On the other hand, if the subset is linearly dependent, then there are multiple redudant ways to express a vector in its span.

**Example 2.** Let $G$ be a graph, and let $E$ be the set of its edges. Then we'll say that the subset of $E$ is independent if it is a **forest**: it contains no cycles. (Note that this is different from being a tree, as the graph need not be connected.) Again, this is about avoiding redundancy: if a set of edges is independent, there is at most one way to get from any vertex to any other vertex, while if it contains a cycle, there can be multiple paths between two vertices.

We'll look at a few different ways of defining matroids: with each one, keep these two examples in mind.

## 2 How Matroids?

One of the characteristic features of matroids is that there are approximately two bazillion ways to define them—definitions that end up being essentially equivalent, though it's nontrivial to see exactly why. (Many mathematicians say that the definitions are "cryptomorphic", a word which sounds much cooler than it actually is.) Let's start off with this initial idea of independence.

## 2.1 Independent Sets

**Definition.** *A **matroid** consists of a finite*[1] *set $E$, called the **ground set**, together with a collection $\mathcal{I}$ of subsets of $E$, called **independent subsets**. These satisfy the following axioms:*

1. $\varnothing \in \mathcal{I}$.
2. *Every subset of an independent set is independent.*
3. *If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then there is some $e \in I_2 - I_1$ such that $I_1 \cup \{e\} \in \mathcal{I}$.*

*A subset which is not independent is called **dependent***[2][3].

Let's verify that Example 1 above satisfies these axioms. The first and second properties are essentially immediate. As for the third, suppose $I_1$ and $I_2$ are two sets of linearly independent vectors with $|I_2| > |I_1|$. The linear independence implies that $\dim(\mathrm{span}(I_1)) = |I_1|$, and likewise for $I_2$. If we could not add any element of $I_2$ to $I_1$ while keeping it independent, this would imply that every element of $I_2$ was in the span of $I_1$. But then we would have $\mathrm{span}(I_2) \subset \mathrm{span}(I_1)$, contradicting $\dim(\mathrm{span}(I_2)) > \dim(\mathrm{span}(I_1))$.

We say that a matroid obtained from a set of vectors as in Example 1 is a **linear matroid**.

**Exercise 1.** *Prove that the edge set of a graph, as presented in Example 2, forms a matroid. (Or just read on and we'll do it in at least two other ways.)*

## 2.2 Circuits

If you attempted the previous exercise, you may have seen that working with independent sets in a set of vectors is easier than working with independent sets in a graph. If we wanted to define matroids starting from the graph perspective rather than the linear algebra perspective, we might focus on what it means to be a cycle in a graph rather than a subgraph that lacks one. So that motivates our next definition.

**Definition.** *A **matroid** consists of a finite set $E$, called the **ground set**, together with a collection $\mathcal{C}$ of subsets of $E$, called **circuits**. These satisfy the following axioms:*

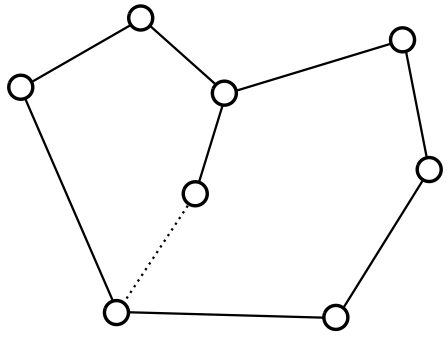
1. $\varnothing \notin \mathcal{C}$.
2. *No circuit properly contains another.*
3. *If $C_1, C_2$ are distinct circuits and $e \in C_1 \cap C_2$, then there is a circuit $C_3$ such that $C_3 \subset (C_1 \cup C_2) - \{e\}$.*

[1] Although there may not appear to be anything about these definitions that requires finiteness, the proper definition of infinite matroids is a point of contention. As we'll see, there are many different ways of defining matroids, and if you start allowing infinite sets these don't hang together as well.

[2] Or **nonindependent**.

[3] Or **unantinonindependent**.

Let's verify that Example 2 above satisfies these axioms. The first is certainly true, and the second is true because any proper subgraph of a cycle is just a path (or union of paths). The third is best seen with a picture:



Note that when we remove one of the edges in which the two cycles shown overlap, we can find a cycle in the graph that remains, essentially by starting around one cycle and switching to the other one when we encounter the removed edge.

We say that a matroid obtained from a graph as in Example 2 is a **graphic matroid**.

What is the relationship between these two definitions? In a graph, a set of edges is dependent precisely when it contains a circuit. So in general, we can say that an independent set should be a subset containing no circuit; while a circuit should be a minimal dependent set. And in fact, under this dictionary, the two definitions we gave are equivalent.

**Theorem 1.** *1. The minimal dependent sets of a matroid satisfy the circuit axioms.*

*2. The subsets of a matroid containing no circuit satisfy the independent set axioms.*

*Proof.* Exercise. □

## 2.3 Bases

In a vector space, we like independent sets in general, but the best ones are bases. In a (connected) graph, general forests are okay, but we're often really interested in spanning trees. What both of these have in common is that they are maximal independent sets. In both of them, the idea of no redundancy that motivates independent sets is complemented by an idea of spanning: with a basis in a set of vectors, we can generate all of the other vectors, and with a spanning tree of a graph, we can reach every vertex.

**Proposition 1.** *All bases of a matroid have the same size.*

*Proof.* Suppose instead that $B_1$ and $B_2$ are bases such that $|B_1| < |B_2|$. Then we can add an element from $B_2$ to $B_1$ and make a larger independent set, contradicting its maximality. □

We say that the size of any basis is the **rank** of the matroid. For a collection of vectors, this is the dimension of their span. For a connected graph, this is one less than the number of vertices.

In any other subject, we might be happy just with defining bases in terms of independent sets. This being matroid theory, we have to turn it into a definition.

**Definition.** *A **matroid** is a finite set $E$, called the **ground set**, together with a collection $\mathcal{B}$ of subsets of $E$, called **bases**. These satisfy the following axioms:*

1. *$\mathcal{B}$ is nonempty.*
2. *If $B_1, B_2 \in \mathcal{B}$, and $x \in B_1 - B_2$, then there exists $y \in B_2 - B_1$ such that $(B_1 - \{x\}) \cup \{y\}$ is in $\mathcal{B}$.*

**Exercise 2.** *1. Prove that the maximal independent sets of a matroid according to our first definition satisfy the basis axioms.*

*2. Prove that the subsets of the bases of a matroid according to our most recent definition satisfy the independence axioms.*

## 2.4 Other Things

There are many other angles from which we can look at matroids, each of which lends itself to a definition (although we won't go into detail here)

- Just as we defined rank of a matroid above, we can define the rank of any subset of a matroid to be the size of the largest independent subset contained in it. This is analogous to taking the dimension of the span of a collection of vectors. We can define matroids in terms of axioms satisfied by the rank function.
- We just looked at the dimension of the span of a set of vectors, but how do we capture the notion of span itself? The idea is to define the **closure** of a subset $A$ to be the collection of all $e \in E$ such that $\mathrm{rank}(A \cup \{e\}) = \mathrm{rank}(A)$. That is, we are adding all the elements which are dependent with everything in $A$: in the context of a colleciton of vectors, the closure of a subset consists of all the vectors from our set which lie in the span of our subset. We can define matroids in terms of axioms satisfied by the closure operator.
- The closure operator tells us how to get from a set of elements to their span, but we might be more interested in the particular sets that result from the span—so we define a **flat** of a matroid to be a subset $F$ which is equal to its own closure. In the linear setting, this corresponds to taking the subset of vectors which are contained in a particular subspace. The flats form a poset (in fact, a lattice) under containment, and we can define matroids in terms of axioms satisfied by the lattice of flats.

The value of having these different definitions is that if we spot any one of these different structures in the wild, and we see that it satisfies the appropriate set of axioms, we then know that the rest of the matroid package comes with.

**Exercise 3.** *Choose any two of independent sets, circuits, bases, rank function, closure operator, and flats. Describe how we define each one in terms of the other.*

# 3 Representability

We haven't really looked at examples beyond linear and graphic matroids. And this is an even less diverse collection of examples than it seems, because graphic matroids are actually linear.

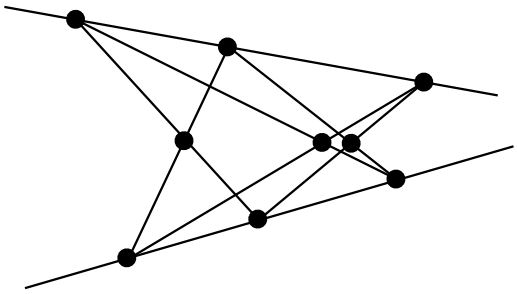
Given a graph $G$ with vertices indexed $1, \ldots, n$, we construct a set of vectors $v_e \in \mathbb{R}^n$ associated to its edges as follows. For each edge, choose an orientation (it doesn't particularly matter which). Then to the edge which goes from $i$ to $j$, associate the vector which is $-1$ in the $i$th component, $1$ in the $j$th component, and $0$ in all others.

**Exercise 4.** *Show that the vectors $v_{e_1}, \ldots, v_{e_n}$ are linearly independent if and only if the subgraph formed by $e_1, \ldots, e_n$ does not contain a cycle.*

Here are some other examples of matroids which are not-very-secretly linear matroids:

- A hyperplane arrangement. Given a collection of $n-1$-dimensional subspaces (hyperplanes) in some $n$-dimensional vector space, we can say that a subset of $k$ of them is dependent if their intersection has dimension greater than $n-k$ (so that some of the hyperplanes impose redundant conditions). But if we represent each hyperplane by its defining equation, and define vectors using the coefficients of these equations, we get an equivalent linear matroid.
- A collection of points in space. Say that some subset of the points is dependent if they all lie in a lower-dimensional subspace than expected (for example, 3 or more points in the plane being collinear). If we look at this from the point of view of projective geometry, where points are represented by 1-dimensional subspaces of a space one dimension higher, the vectors spanning those subspaces form an equivalent linear matroid.

Is matroid theory just linear algebra in disguise? Not at all! The diagram below depicts the **non-Pappus matroid**: its ground set consists of the 9 highlighted points, and a set is dependent if it has at least 4 elements or consists of the 3 points on one of the lines shown.



Why can't this be realized as a linear matroid? Because of the classical theorem of projective geometry known as **Pappus' theorem**, which says that if 6 points are arranged in the fashion shown on the top and bottom lines in the above figure, and 3 more points are obtained as the intersections in the middle of the figure, then those 3 points must also lie on a line. Roughly, if we attempt to realize the non-Pappus matroid over a field, it will force the middle 3 points to be a dependent set as well.

**Exercise 5.** *Verify that the non-Pappus matroid is, in fact, a matroid.*

The situation gets even subtler than this. Consider the **uniform matroid** $U_{2,4}$, on the ground set $\{1, 2, 3, 4\}$, in which the independent sets are precisely those with 2 or fewer elements. Then this matroid has rank 2, so if we represent it as a linear matroid, it can be realized as a set of 4 vectors in a 2-dimensional space. Since any two of the vectors are independent, we know the 4 vectors must be distinct and nonzero.

This is perfectly doable—unless we're working over the field $\mathbb{F}_2$, where a two-dimensional vector space has only 3 distinct nonzero elements! So the field our vector spaces are defined over actually affects which matroids can be realized as linear. In general, we say that a matroid is **representable over a field** $K$ if it can be realized by a set of vectors over that field. The question of which fields matroids are representable over is actually quite complicated and the subject of active research.

This then raises the question: if matroid theory *isn't* just linear algebra in disguise, why did we adopt a system of axioms that allows things like the non-Pappus matroid to slip through in the first place[4]? As we'll see in the next section, the definition we chose has an important and practical characterizing property.

[4]One answer to this questions is "actually coming up with a system of axioms that screens out non-representable matroids would be extremely complicated and maybe also impossible". Vámos wrote an article on this issue with the lovely title of "The Missing Axiom of Matroid Theory Is Lost Forever"

# 4 Greedy Algorithms Are, For Lack of a Better Word, Good

Here is a problem that arises naturally in contexts involving graphs. Assign to every edge $e$ of your graph a real number $w(e)$, its weight. Then for any spanning tree, we define its weight to be the sum of the weights of its edges. The problem is to find a spanning tree of minimal weight. If we interpret the weight of an edge as a cost, this is essentially asking: how can we bind the whole graph together as efficiently as possible?

In matroid language, the problem becomes: if we assign a weight $w(e)$ to each element $e$ of the ground set, how can we find a basis of minimal total weight? The most straightforward approach is to use a **greedy algorithm**: at each step, look at all the elements we can add to our basis-in-progress without making it dependent, and pick the one with the smallest weight.

It's not at all obvious that this should work—adding elements to our basis prevents other elements from being added later, and we could hypothetically miss out on a more optimal combination of elements this way. But despite not planning ahead at all to correct this, the algorithm does work!

**Theorem 2.** *The greedy algorithm produces a basis of minimal weight.*

*Proof.* Let $e_1, \ldots, e_r$ be the sequence of elements produced by the greedy algorithm, in the order they appear. Note that $w(e_1) \leq w(e_2) \leq \cdots \leq w(e_r)$.

Now let $f_1, \ldots, f_r$ be another basis, ordered such that $w(f_1) \leq w(f_2) \leq \cdots \leq w(e_r)$. We claim that $w(e_i) \leq w(f_i)$ for all $1 \leq i \leq r$, which will certainly imply that the total weight of the $e_i$ basis is less than or equal to that of the $f_i$ basis.

To see this, suppose the contrary, and let $j$ be the smallest index at which $w(f_j) < w(e_j)$. Then $I_1 = \{e_1, \ldots, e_{j-1}\}$ and $I_2 = \{f_1, \ldots, f_{j-1}, f_j\}$ are independent sets, with $|I_2| > |I_1|$. Thus there exists some $k$, $1 \leq k \leq j$ such that $\{e_1, \ldots, e_{j-1}, f_k\}$ is independent. On the other hand, $w(f_k) \leq w(f_j) < w(e_j)$, so our greedy algorithm shouldn't have chosen $e_j$ to add to $\{e_1, \ldots, e_{j-1}\}$. Rather, $f_k$ was a better choice, a contradiction. □

One (much better-known) consequence of this result is that we can produce minimal spanning trees this way. In that context, the greedy algorithm is known as **Kruskal's algorithm**.

But we can consider this greedy algorithm outside of just the context of a matroid. Suppose $E$ is a set and $\mathcal{I}$ is any collection of subsets such that any subset[5] of a member of $\mathcal{I}$ is also in $\mathcal{I}$, and suppose that every element $e \in E$ has a weight $w(e)$. Then we could again apply the greedy algorithm: build up a subset $B$ by starting with the empty set and repeatedly adding the edge of smallest weight which keeps our subset in $\mathcal{I}$, until we can't anymore. By our

[5]We could even drop this condition, but at that point using the greedy algorithm is kind of silly, since there may be independent subsets that can't be built up as a sequence of smaller sets at all.

stopping condition, $B$ is a maximal element of $\mathcal{I}$; but is it the smallest-weighted such element?

In fact, the answer is "precisely when $(E, \mathcal{I})$ is a matroid". So what we have here is yet another definition of matroids!

**Theorem 3.** *Let $E$ be a set and $\mathcal{I}$ a collection of subsets. Suppose that*

1. $\varnothing \in \mathcal{I}$
2. *Any subset of a set in $\mathcal{I}$ is also in $\mathcal{I}$.*
3. *The greedy algorithm produces a maximal member of $\mathcal{I}$ of minimal weight.*

*Then $(E, \mathcal{I})$ is a matroid.*

*Proof.* Suppose not. Then we can choose sets $I_1, I_2 \in \mathcal{I}$ such that $|I_2| > |I_1|$, but for every $e \in I_2 - I_1$, $I_1 \cup \{e\}$ is dependent. Now for some $0 < \epsilon < 1$, weight the elements as follows:

$$w(e) = \begin{cases} -1 & e \in I_1 \\ -1 + \epsilon & e \in I_2 - I_1 \\ 0 & \text{otherwise} \end{cases}$$

In this case, the greedy algorithm will start by picking all the elements of $I_1$; then, since it can't add any elements of $I_2 - I_1$ by assumption, it will fill this out to a maximal member of $\mathcal{I}$ by adding elements of weight 0. The resulting maximal member $B \in \mathcal{I}$ has weight $-|I_1|$.

On the other hand, we can add more elements to $I_2$ and fill it out to a maximal subset $B_2 \in \mathcal{I}$. Since our weights are negative, $w(B_2) < w(I_2)$, and

$$\begin{aligned} w(I_2) &= w(I_1 \cap I_2) + w(I_2 - I_1) \\ &= -|I_1 \cap I_2| - |I_2 - I_1| + \epsilon|I_2 - I_1| = -|I_2| + \epsilon|I_2 - I_1| \end{aligned}$$

By choosing $\epsilon$ sufficiently small, we can make this less than $-|I_1|$. This shows that the maximal member of $\mathcal{I}$ we got through the greedy algorithm was not optimal. □

In a way, this gives us another reason that the definition of matroid, and the particular aspects of independence we chose to prioritize in it, really are worth considering: they isolate a particular property that makes a greedy algorithm work.

# References

[1] Oxley, James. *Matroid Theory*, 2nd ed. Oxford University Press, 2011.