Chapter 1

Matroids

The underpinning of all our work are mathematical objects known as matroids. Though, as we've noted, they've been around since the 1930's, they're not, yet, household objects every mathematician knows. This is the shallowest scratch into the world of matroids, slanted heavily towards what's necessary for our problem at hand. There are many full books on matroids, for those curious to dig into more depth. We are partial to the treatment by Oxley's *Matroid Theory* [4].

We will build up to matroids by developing some intuition from more familiar, motivating mathematical objects. Then we will introduce the definition(s) of matroids and introduce the characteristic polynomial. We will wrap up this chapter by stating the Heron-Rota-Welsh conjecture.

1.1 Linear Algebra Done Hastily

When the vague notion of independence is mentioned in a mathematical context, we expect that minds wander to *linear* independence. A central concept to the field of linear algebra, this is likely the vast majority's first introduction to the topic. Happily, this mirrors, closely enough, the initial development of matroids. The patterns that emerge viewing the independence of collections of vectors will, quite directly, inspire the first of our definitions of a matroid.

1.1.1 Linear Independence

First, let us recall the definition of linear independence.

Definition 1.1 (Linear Independence)**.** Given a finite set of vectors $\{v_1, v_2, \ldots, v_k\} \subseteq F^n$, for some field F, the set of vectors is called *linearly independent* if the only solution to the linear combination

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k = 0$$

is $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$. Otherwise, we say the set is *linearly dependent*.

While this is a familiar definition to many of us, it will be illustrative to all to take a more concrete example. We'll define the vectors $a = (1, 0, 0), b = (0, 1, 0), c = (0, 0, 1)$, and $d = (1, 1, 0)$. Then we have the set $E = \{a, b, c, d\} \subseteq \mathbb{R}^3$.

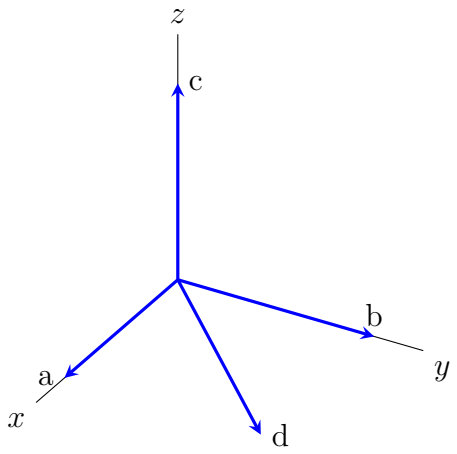


Figure 1.1: The collection of vectors in E

The observant will note that this of course cannot be linearly independent, and indeed we can confirm by showing the linear combination

$$1a + 1b + 0c + (-1)d = 0.$$

But now, a fun little game we could play, at least by our personal reckoning of fun, is to find all subsets of E that *are* linearly independent. For example, consider $\{c, d\} \subseteq E$.

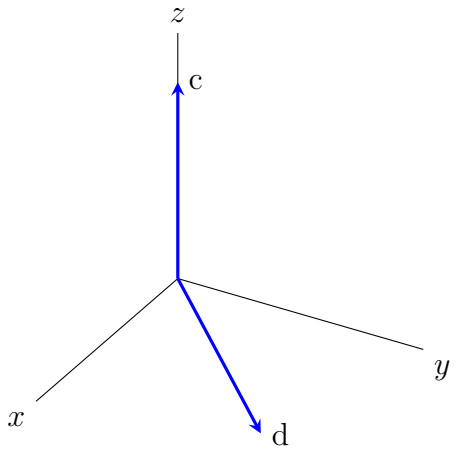


Figure 1.2: A linearly independent subset of E

Take a look to confirm there is no nonzero linear combination of our elements that gives us the 0-vector. Given the relatively small number of elements, it would not take too long to identify every possible subset of E_V that is linearly independent; for the impatient however, they are precisely

$$\big\{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a, b, c\}, \{a, c, d\}, \{b, c, d\}\big\}.$$

For the impatient *and* untrusting, we suggest that the only thing really necessary to check here is that each 3-element set is linearly independent and that there are no other possible 3-element sets in E that are linearly independent.

As a point of pure notation, the above list is ugly. We are going to be working with sets of this form so much in this paper that, in order to avoid a shortage of curly brackets, we will introduce a more tidy notation. Going forward, we will write the elements of the internal sets adjacent to each other to represent the set containing them; for example we will write the set $\big\{\{a,b\},\{a,b,d\}\big\}$ as $\{ab,abd\}$. Thus, we will more compactly identify the linearly independent subsets of E as

$$\{\emptyset, a, b, c, d, ab, ac, ad, bc, bd, cd, abc, acd, bcd\}.$$

Now that we have this collection, this leads to our next totally fun and normal activity. Namely, looking for patterns amongst these independent sets.

1.1.2 Noteworthy Properties of Linearly Independent Subsets

We suspect that those with some knowledge of linear algebra will immediately be ready to note that the largest independent subsets of E_V have 3 elements. And, sure enough, that is true! But this is more a property of the vector space, $\mathbb{R}^3$ in this case, that we're pulling the vectors from than some intrinsic relationship or property of the subsets. We'd like to call attention to some properties that may be less obvious (or so obvious one forgets they're even there). First, something entirely uninteresting.

Property 1.1 (The empty set is an independent subset)**.** For any finite collection of vectors, E, in vector space,

$$\emptyset \subseteq E$$

and $\emptyset$ is linearly independent.

That $\emptyset$ is linearly independent is what we call vacuously true. That is to say, it's true mostly as a quirk of how we define linear independence. Since we can't form a non-zero linear combination that gives the 0-vector, because there are *no* elements at all, it can't be linearly dependent. But then if it's not linearly dependent, it has to be independent. Proof by being pedantic, really the heart of mathematics if one thinks about it. Next, a property that will surprise no one who has taken a linear algebra class, but is worth making explicit.

Property 1.2 (Any subset of a linearly independent set is itself linearly independent)**.** For any linearly independent set of vectors, I, in vector space, if

$$I' \subseteq I,$$

then I' is linearly independent.

Recall we suggested that in order to check that our list of independent subsets of E_V was correct, it was sufficient to just check the subsets with the most elements. This property tells us that if we've figured out the maximal subsets, then filling in the rest is just a matter of taking subsets of those. One may even begin to see the specter of combinatorics lurking. This property falls out easily from our definition. If no non-zero linear combination of vectors in a set gives us the 0-vector, then using fewer vectors isn't going to change that. Finally, we have a more subtle property.

Property 1.3 (The "independence augmentation" property)**.** Let $I = \{v_1, v_2, \ldots, v_m\}$ and $J = \{u_1, u_2, \ldots, u_n\}$ be linearly independent sets in a vector space, such that $m < n$. Then there exists a $k \in [n]$ such that the set

$$I \cup u_k = \{v_1, v_2, \ldots, v_m, u_k\}$$

is linearly independent.

In other words, we can always find an element of a larger independent set to include in a smaller one that will leave the (new, augmented) set independent. Going back to our running example, consider the sets acd and ab. Then $c \in acd$ is such an element, and we confirm that $ab \cup c = abc$ is indeed linearly independent. This property is not immediately obvious, though may be believable to those who have done a proof based linear algebra class.

These are the three properties of linearly independent sets we wish to highlight here. We could use these properties alone to motivate the first definition of a matroid. However, we have one more detour before we get to matroids proper. There is another area where independence arises quite naturally, and it will be useful to know going forward.

1.2 Graphic Content

The next place our intuition building journey takes us is the world of graphs. Graph theory was the other motivator of matroids, so we too shall delve in. While we tried to not assume too much, we did, secretly, expect the average reader would feel comfortable enough with linear algebra. Graphs, on the other hand we will quickly build up from scratch and develop a notion of independence. Luckily, this is actually a fairly short process.

1.2.1 What a Graph Is

Not to be confused with the graph of a function or whatever it is business analysts put in shareholder presentations, graphs for us are essentially a collection of points, called vertices, and lines between them, called edges. There are quite a few definitions of graphs, each allowing for slightly different properties, but for our purposes, we can use a rather basic definition.

Definition 1.2 (Graph)**.** A *graph* is a pair of sets $G = (V, E)$, where V is a set of objects known as vertices and

$$E \subseteq \big\{\{x, y\} \mid x, y \in V\big\}$$

is a set of edges.

A brief aside for our friends who actually care about graphs; the definition here is for an *undirected simple graph permitting loops*. The treatment of graphs and their relation to matroids in this paper extends easily enough for most other graphs because, as far as matroids are concerned, this kind of graph carries pretty much all the information necessary. Indeed, we will see soon enough that even allowing loops is an unnecessary flourish. We again recommend Oxley [4] for the serious graph theorist's entry into matroids.

For the rest of us, this definition may feel rather opaque. Here, an example and corresponding picture should help immensely. Let $V = \{v_1, v_2, v_3, v_4\}$ be a vertex set. Now we must define edges between vertices. For later convenience, we will name these edges. Let $a = \{v_1, v_2\}$, $b = \{v_2, v_3\}$, $c = \{v_3, v_4\}$, and $d = \{v_1, v_3\}$,; then let $E = \{a, b, c, d, e\}$ be our edge set. Recall that, for example, c represents an edge, or connection, between the vertex v_3 and the vertex v_4. With both those pieces, we have the graph $G = (E, V)$. The corresponding picture of our graph is below.

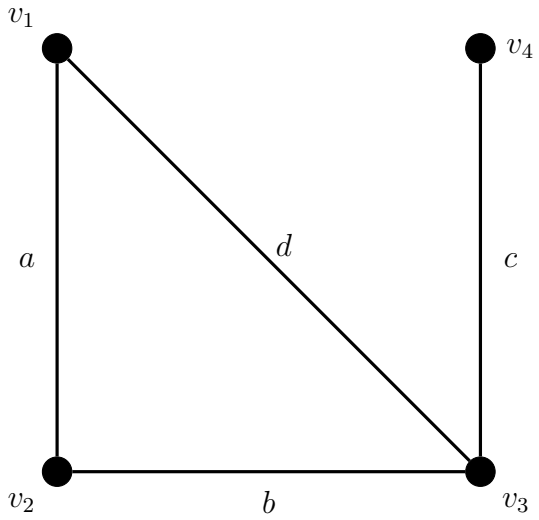


Figure 1.3: Our example graph G

Now that we know what a graph is, it's time to figure out what "independence" could possibly mean.

1.2.2 Independence in the Realm of Graphs

The first thing to note is that we will define independence on the set of edges of a graph; that is, for some graph $G = (V, E)$, an independent set will be some subset $I \subseteq E$, meeting some criteria we'll discuss below. What then would it mean for a set of edges to be independent? Well, if we take some subset of the edges, we restrict which vertices are accessible via those edges. But there might still be redundant edges. Could we remove additional edges from our set and still be able to reach all the same vertices? The answer to that determines if a set of edges is independent, when we can't make our collection of edges any smaller without disconnecting a vertex, or dependent, when we can.

To formalize this we will need to learn a few graph theoretic terms. First, we need the notion of a walk.

Definition 1.3 (Walk)**.** Given a graph $G = (V, E)$, a *walk* is an alternating sequence of vertices and edges

$$(v_1, e_1, v_2, e_2, v_3, \ldots, e_{k-1}, v_k),$$

where each $v_i \in V$, $e_j \in E$ and $v_i \in e_i$ and $v_{i+1} \in e_i$

Intuitively, a walk starts at some vertex and then follows an edge to another, connected vertex then continues to follow edges to vertices until ending at some vertex. If we put our finger on a vertex and trace along edges to another vertex, we've defined a walk. Now that we have a walk, we may define a cycle.

Definition 1.4 (Cycle)**.** A *cycle* is a walk

$$(v_1, e_1, v_2, e_2, v_3, \ldots, e_{k-1}, v_k),$$

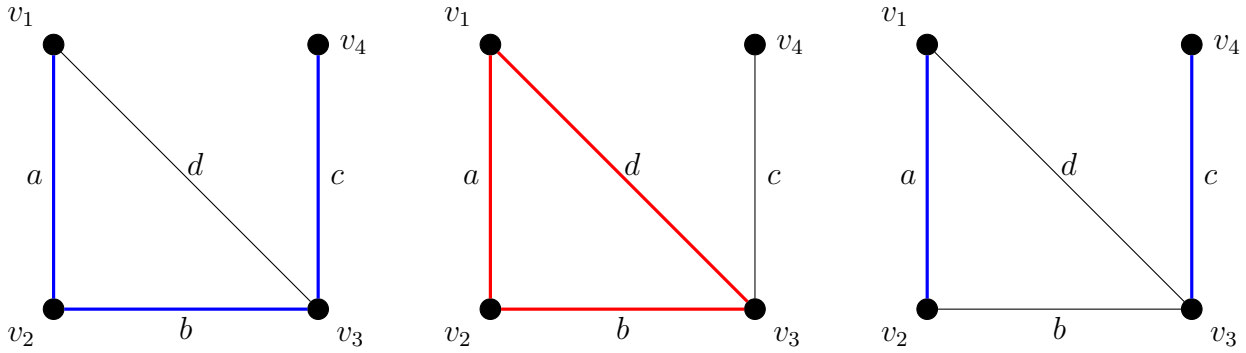
where $v_1 = v_k$ and $v_i \neq v_j$ when $i \neq j$ otherwise.

Further, we say a set of edges *contains a cycle* if there is a cycle whose edges are contained in the set.

That is, a cycle is a walk that starts and ends at the same place and otherwise passes through unique vertices. Given the notion of independence we began to motivate above, hopefully the utility of defining a cycle is apparent. Any subset of edges that contains a cycle must be dependent, as we can always remove the last edge from the walk and still have all the same vertices connected. With this, our definition of independence can finally be formalized.

Definition 1.5 (Independence (of edges of a graph))**.** Let $G = (V, E)$ be a graph. Then a subset of edges $I \subseteq E$ is *independent* if it does not contain a cycle.

Let us immediately take to our example for this section to consider some possible sets of edges.



(a) Independent: the set of edges $\{a, b, c\}$ does not contain a cycle

(b) Dependent: The edges in $\{a, b, d\}$ contain a cycle

(c) Independent: The edge set $\{a, c\}$ does not contain a cycle. It's not necessary for all vertices to be connected

Figure 1.4: Some examples of independent/dependent sets of edges

Now that we've got some practice under our belt, it's time to play our favorite game again. Given our example graph, $G = (V, E)$, we want to identify the set of all possible independent vectors. A few moments of tracing paths along the graph, hunting for cycles, will reveal that from our set of edges $E = \{a, b, c, d\}$, the independent subsets are precisely

$$\{\emptyset, a, b, c, d, ab, ac, ad, bc, bd, cd, abc, acd, bcd\}.$$

This should look familiar! Suspiciously so, even. The independent subsets are the same as those we found in our collection of vectors. Clearly then all the properties of linearly independent subsets we showed above also hold in this example. Indeed, this is not just a quirk of our example. Given any graph, the independent subsets of the edge set will obey the same properties as the linearly independent subsets of a set of vectors. It was the reoccurrence of these properties across different mathematical objects that inspired the creation of matroids.

1.3 Matroids, Finally

Matroids were initially developed by Hassler Whitney in the paper *On the Abstract Properties of Linear Dependence* [9]. The introduction of Whitney's paper parallels our journey so far, covering, much more succinctly, shared properties of linear independence and independence of graph edges. He then goes on to introduce several equivalent definitions of a matroid.

An interesting feature of matroids is just how many definitions exist. Plenty more have been added since the several introduced by Whitney, and any one of these definitions can be taken axiomatically and from them any other definition may be derived. However, it can be extremely non-obvious that a given definition is equivalent to some other. The path between the various axiomatizations can be so difficult to see that they have been affectionately called *cryptomorphic* to one another.

We will primarily be concerned with two axiomatizations, one based on the notion of independent sets and another based on what are called *flats*. The first definition follows closely from the background we've developed so far. This allows us to more easily define the terms and properties of matroids that we will need in the second definition. It is this second definition that will be of key importance for the following chapters, so it is important to develop it here.

1.3.1 Independent Set Axioms

The first definition of matroids should, again, look very familiar.

Definition 1.6 (Matroid — Independent Set Axioms)**.** A *matroid* is a pair $\mathcal{M} = (E, \mathcal{I})$, where E is a finite set, called the *ground set*, and $\mathcal{I} \subseteq 2^E$ is a collection of subsets of E, called the *independent sets*, with the following properties:

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

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

(I3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| \leq |I_2|$, then there exists some $e \in I_2 \setminus I_1$ such that $I_1 \cup e \in \mathcal{I}$.

They correspond precisely to the properties we identified in linearly independent subsets and that we saw again in independent edge sets. We can take this opportunity to define our now familiar examples as a matroid.

Example 1.1. We let the ground set $E = \{a, b, c, d\}$, and pick the independent sets to be

$$\mathcal{I} = \{\emptyset, a, b, c, d, ab, ac, ad, bc, bd, cd, abc, acd, bcd\}.$$

Coming as probably no surprise, this has the same independence relations as both our vector example and our graph example. We should confirm that $\mathcal{I}$ obeys the properties (I1)-(I3), but we already know that particular set must.

1.3.1.1 Aside: Representable Matroids

Given that we've already seen the example "matroid" arise twice in other contexts, it is natural to ask if we've gained anything new with matroids. If every matroid could just be studied as a finite collection of vectors and its independent subsets, we don't really have to go through the trouble defining a whole new object.

It turns out that this is not the case. A matroid that can arise from a finite set of vectors, like our example, is called *representable*. However, there are *unrepresentable* matroids. A lot of them in fact.

The distinction between representable and unrepresentable matroids has no bearing on the results of this thesis, but it's worth noting here. Our examples are representable, as it allows us to leverage some visual intuition, but everything we say here holds for all matroids.

1.3.2 The Uphill Path to Flats

A benefit of introducing the independence axioms first, we feel, is that they are readily interpretable. At least after developing a bit of intuition in the realm of linear independence. For much of the rest of our paper however, we won't be thinking of matroids in this form. We will need a formulation of matroids that use something called *flats*.

To get to this new definition of matroids, or even state what a flat is, we will have to build up our vocabulary surrounding matroids. Our goal here is to develop everything necessary to define a flat. The path there may seem rather wandering, we will introduce quite a few definitions here. But there are no shortcuts; each new definition builds on the last, until we have a nice tower of terms with which to use.

Given their history, matroids borrow a lot of terminology from linear algebra and graph theory. For the most part, their meaning is related to that in the original context, so it can be a useful starting point. Still, it is not necessary to have heard of them before; these definitions exist perfectly fine on their own in the world of matroids, as we shall see.

We use the independent set axioms to these terms and state properties, but we could have started with any of the axioms and developed all these terms. It's actually quite a fun exercise to develop parallel definitions from different starting axioms.

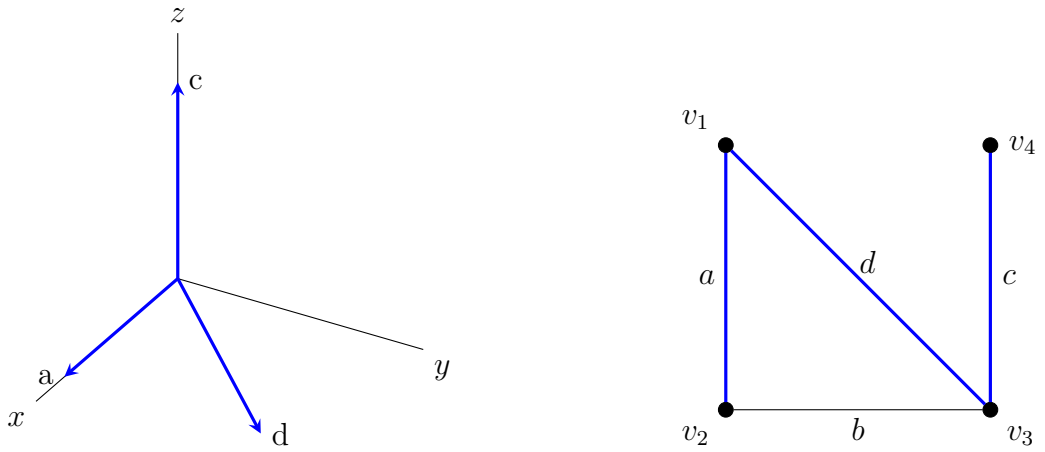
1.3.2.1 All Your Bases Belong to Matroid

First, we will finally address a pattern we've noted earlier, that the largest independent sets all seem to have the same number of elements, or, as we like to say in the business, the same *cardinality*. To do so we'll introduce the notion of a basis of a matroid.

Definition 1.7 (Basis)**.** Given a matroid $\mathcal{M} = (E, \mathcal{I})$, an independent set $B \in \mathcal{I}$ is a *basis* of $\mathcal{M}$ if

$$B \cup e \notin \mathcal{I}$$

for all $e \in E \setminus B$. That is to say, a basis B is a maximally independent subset of E with respect to set inclusion.



(a) A basis in linear algebra is a minimal spanning set (b) A basis of graph is a spanning tree

Figure 1.5: The set $\{acd\}$ is a basis of M, which we can view in the vector and graph setting

For those recalling their linear algebra, yes, this does have the very useful property we expect from something called a basis.

Proposition 1.1. *All bases of a matroid contain the same number of elements.*

Proof. Let B_1 and B_2 be two bases of $\mathcal{M}$. It must be the case that $|B_1| < |B_2|$, $|B_1| > |B_2|$, or $|B_1| = |B_2|$. Let's assume that $|B_1| < |B_2|$. Then since $B_1, B_2 \in \mathcal{I}$, we may use the property (I3) of matroids. There exists some $b \in B_2 \setminus B_1$ such that $B_1 \cup b \in \mathcal{I}$. This is a contradiction with our definition of a basis, since adding any element not already in B_1 should make it dependent.

We have then that $|B_1| \geq |B_2|$, but assuming the case $|B_1| > |B_2|$, we will arrive at a contradiction by the same steps as above. Thus, $|B_1| = |B_2|$, and we conclude that all bases of $\mathcal{M}$ have the same number of elements. □

As we see in the examples in figure 1.5, a basis has a very literal interpretation in the context of vector spaces and graphs. If pressed for an intuition of a basis in the more general matroid setting, we'd say that they give us an idea of "how much" (in)dependence is going on amongst the elements ground set; likely accompanied by us literally waving our hands through the air. If our matroid has 1000 elements in its ground set, but its bases only have size 3, then there must be a lot of dependence amongst all those elements of the ground set. However vague the idea, it would be very useful to be able to quantify "how much" independence is going on in any subset $X \subseteq E$ of a matroids ground set.

1.3.2.2 Rank and Closure

Indeed, this is an important enough property to get its own name, the *rank*. The rank of any subset of ground elements is simply the size of the largest independent subset.

Definition 1.8 (Rank)**.** Let $\mathcal{M} = (E, \mathcal{I})$ be a matroid. The *rank function* is the map

$$\begin{aligned} \mathrm{rk}_{\mathcal{M}} \,:\, 2^E &\to \mathbb{Z}_{\geq 0} \\ X &\mapsto |Y| \end{aligned}$$

where $Y \subseteq X$, $Y \in \mathcal{I}$, and there is no $Y \subsetneq Y' \subseteq X$ such that $Y' \in \mathcal{I}$. That is to say, the rank of any subset X is the size of the largest independent set contained in X.

We write $\mathrm{rk}_{\mathcal{M}}(E)$ as $\mathrm{rk}_{\mathcal{M}}(\mathcal{M})$, and is called the *rank* of $\mathcal{M}$.

Unless we are in imminent danger of confusion, we will notate $\mathrm{rk}_{\mathcal{M}}(X)$ as just $\mathrm{rk}(X)$. In the land of linear algebra, the rank corresponds to the dimension spanned by the vectors. Just as adding more vectors into a linear span won't necessarily increase the dimension spanned, increasing the number of your elements in your subset will not necessarily increase the rank. For instance, in our running example we see that $\mathrm{rk}(ab) = \mathrm{rk}(abd) = 2$. The rank of the matroid itself will be, as we showed above, the size of any basis of the matroid.

This notion that we can add more elements to a subset without changing its rank leads, at last, to the final preliminary definition.

Definition 1.9 (Closure)**.** Given a matroid $\mathcal{M} = (E, \mathcal{I})$, the *closure operator* is a function

$$\begin{aligned} \mathrm{cl}_{\mathcal{M}} \,:\, 2^E &\to 2^E \\ X &\mapsto \{e \in E \mid \mathrm{rk}(X \cup e) = \mathrm{rk}(X)\}. \end{aligned}$$

For any $X \subseteq E$, we call $\mathrm{cl}(X)$ the closure of X. Adittionally, taking closures is idempotent, so $\mathrm{cl}(X) = \mathrm{cl}\big(\mathrm{cl}(X)\big)$.

Again we will write the closure operator as $\mathrm{cl}(X)$ almost exclusively. If a basis captures how much "independence" is in a set of elements, the closure of a subset generates a set that is as "dependent" as possible for a given rank (using the elements of that initial set). One might ask if there is anything special about these sets that are as big as they can be with respect to closure. A very insightful question, if we do say so ourselves.

1.3.3 Our Flag Means Totally-Ordered Subsets of the Lattice of Flats

If you didn't notice our subtle hint above, it may come as a surprise that sets that are as "big" or "dependent" as possible for a given rank are precisely flats.

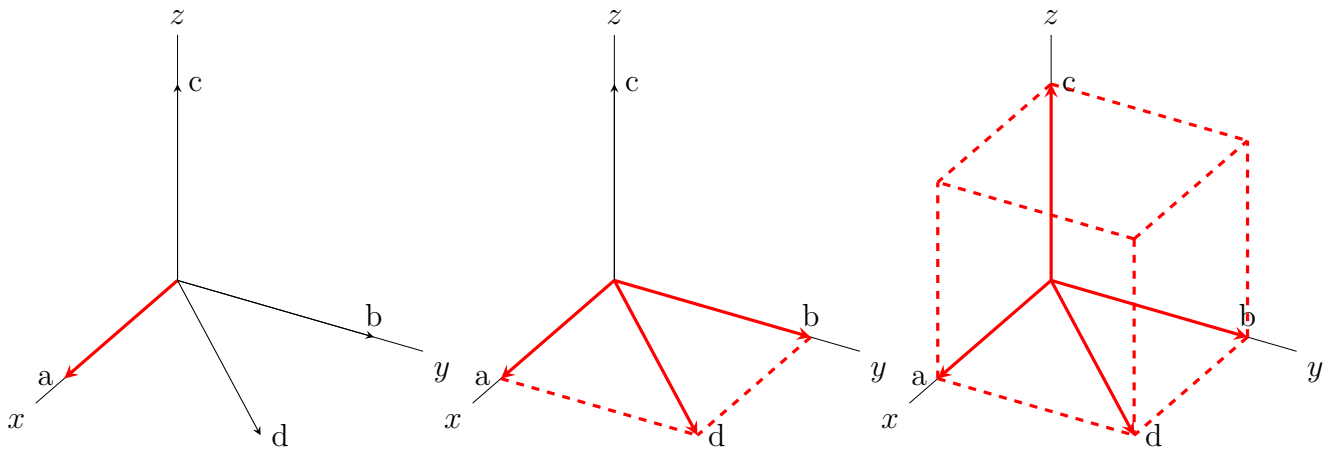
Definition 1.10 (Flat)**.** Given a matroid $\mathcal{M} = (E, \mathcal{I})$ and subset $X \subseteq E$, if

$$X = \mathrm{cl}(X),$$

then X is a *flat* of $\mathcal{M}$.

What if instead of independent sets, we collect all the flats of a matroid. In our running example, we could start applying the closure opreator left and right until we collect the set

$$\mathcal{F} = \{\emptyset, a, b, c, d, abd, ac, bc, cd, abcd\}.$$



(a) Rank 1: The single element a is a flat

(b) Rank 2: Note ab is not a flat, but abd is

(c) Rank 3: The matroid itself is rank 3, so the flat of this rank is the whole ground set, $abcd$

Figure 1.6: Examples of flats of rank 1, 2, and 3 in our example matroid M, viewed as vectors

Since flats are maximal with respect to rank, they naturally divide up by rank; i.e.

$$\begin{aligned}\mathcal{F}_0 &= \{\emptyset\}\\ \mathcal{F}_1 &= \{a, b, c, d\}\\ \mathcal{F}_2 &= \{abd, ac, bc, cd\}\\ \mathcal{F}_3 &= \{abcd\},\end{aligned}$$

where everything in $\mathcal{F}_k$ has rank k. When laid out like this we may begin to note some interesting patterns. Indeed, just like independent sets have some useful properties, so do the set of flats.

Proposition 1.2 (Properties of Flats)**.** *Let $\mathcal{M} = (E, \mathcal{I})$, be a matroid. Then the set*

$$\mathcal{F} = \{X \subseteq E \mid X = \mathrm{cl}(X)\}$$

is the set of flats of $\mathcal{M}$, and $\mathcal{F}$ has the following properties:

(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 $F_1, F_2, \ldots, F_k \in \mathcal{F}$ are the minimal flats such that each $F_i \subsetneq F$, then the sets $F_1 \setminus F$, $F_2 \setminus F$, $\ldots$, $F_k \setminus F$ partition $E \setminus F$.

Further, let E be any ground set and $\mathcal{F} \subseteq 2^E$ be a collection of subsets of the ground set such that properties (F1)–(F3) hold. Define

$$\mathrm{cl}^* \,:\, 2^E \to 2^E$$

such that $\mathrm{cl}^*(X) = F$ for some flat $F \in \mathcal{F}$ where $X \subseteq F$ and there is no $F' \in \mathcal{F}$ such that $X \subseteq F' \subsetneq F'$. Then $\mathcal{M} = (E, \mathcal{F})$ is a matroid with independent set

$$\mathcal{I} = \{I \subseteq E \mid I_1 \subsetneq I_2 \subseteq I,\, \mathrm{cl}^*(I_1) \neq \mathrm{cl}^*(I_2)\}\,.$$

Let's unpack this proposition, as flats are a bit more difficult than independent sets as a foundation of matroids. Property (F1) says that the ground set, E, is a flat. This follows directly from the fact that the closure of a basis has to be every element of the ground set, since you can't ever get a higher rank than a basis.

The second property (F2) says that the set of flats is closed under intersection; i.e. the elements shared between any two flats is a flat itself. This follows from the properties of closure and a bit of set theory; it's a fun little exercise to prove.

The last property, (F3), looks more intimidating than it is. In essence, if you take a flat, F (with $F \neq E$, since no flats have higher rank than E), then for every element *not* in F you're going to find it in a flat that is one rank higher. This shouldn't be too surprising, since if an element, let's call it x, is not in F, then $\mathrm{cl}(F \cup x)$ will have to have a higher rank than F. That this *partitions* $E \setminus F$ just means that each $e \in E$ that's not in F is going to appear in exactly one flat one rank higher (specifically the flat $\mathrm{cl}(F \cup e)$).

Finally, the proposition asserts that if we start with a ground set and then a collection of subsets of that ground set that meet all three properties (F1)–(F3), then that is sufficient to characterize a matroid. That is, we could take (F1)–(F3) as another axiomatization of a matroid. A recommended exercise would be to reconstruct all the definitions in the preceding section starting with just these axioms.

These properties actually impart a very interesting structure on the set of flats that we will now explore.

1.3.3.1 The Lattice of Flats

First, we recall, or learn here and now, that any collection of subsets of a set form a partially ordered set.

Definition 1.11 (Partially Ordered Set)**.** A *partially ordered set*, often called a poset, is a pair $(P, \preceq)$, where P is a set of elements, and $\preceq$, is a relation between some, but not necessarily all, of the elements of P with the following properties:

i. $a \preceq a$,

ii. if $a \preceq b$ and $b \preceq a$, then $a = b$,

iii. if $a \preceq b$ and $b \preceq c$, then $a \preceq c$,

for all $a, b, c \in P$.

With the definition in hand, we can verify that $(\mathcal{F}, \subseteq)$ is a partially ordered set, where $\mathcal{F}$ is the set of all flats of a matroid. But we can do even better than that. Some posets have an even stronger structure, called a lattice.

Definition 1.12 (Lattice)**.** A partially ordered set $(L, \preceq)$ is a *lattice* if there exist binary operations

$$\vee \, : \, L \times L \to L,$$

called a *join*, and

$$\wedge \, : \, L \times L \to L,$$

called a *meet*, such that for any two elements $a, b \in L$,

i. the join $a \vee b$ is an element of the lattice such that $a \preceq a \vee b$ and $b \preceq a \vee b$, and for any element $c \in L$ such that $a \preceq c$ and $b \preceq c$ it's the case that $a \vee b \preceq c$,

ii. the meet $a \wedge b$ is an element of the lattice such that $a \wedge b \preceq a$ and $a \wedge b \preceq b$, and for any $c \in L$ such that $c \preceq a$ and $c \preceq b$ then we have $c \preceq a \wedge b$.

If you've never seen this definition before, it can be a bit heavy on symbols, but once we ground it in our set of flats it won't be too bad. First though, we must establish that the set of flats does indeed form a lattice.

Proposition 1.3 (The Collection of Flats Form a Lattice)**.** *Let $\mathcal{M}$ be a matroid and $\mathcal{F}$ be the set of all flats of $\mathcal{M}$. Then $(\mathcal{F}, \subseteq)$ is a lattice, with the operations*

$$F_1 \wedge F_2 = F_1 \cap F_2$$
$$F_1 \vee F_2 = \mathrm{cl}(F_1 \cup F_2)$$

for any $F_1, F_2 \in \mathcal{F}$.

Proof. It is sufficient to show that $\mathcal{F}$ is a meet-semilattice and that $\mathcal{F}$ has a maximal element.

To show that F is a meet-semilattice, we must prove that the meet operation is well-defined. Let $F_1, F_2 \in \mathcal{F}$ be flats. Then from property (F2), $F_1 \cap F_2$ is a flat. Naturally, for any $F_3 \in \mathcal{F}$ such that $F_3 \subseteq F_1$ and $F_3 \subseteq F_2$, then $F_3 \subseteq F_1 \cap F_2$. Thus, the meet operation is well-defined.

The maximal element of $\mathcal{F}$ is, trivially, the ground set, E, itself which is a flat by property (F1). A meet-semilattice with a maximal element is a lattice, and so $\mathcal{F}$ forms a lattice. □

Now we can talk about a lattice of flats. To motivate this, let us once again consider our example matroid. It is, if not traditional, convenient to structure a lattice graphically in a *Hasse diagram*.

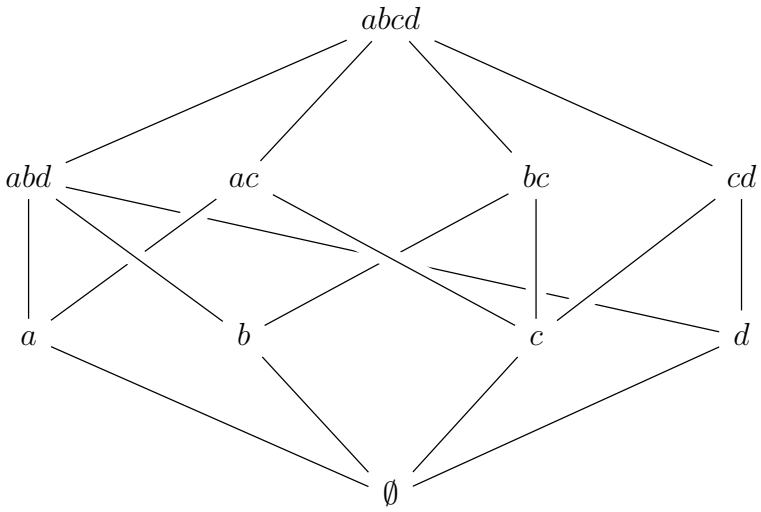


Figure 1.7: The Hasse diagram of flats of our example matroid M

When reading a Hasse diagram, if we have two entries x and y, with a line connecting them and x is higher on the page than y, we say x *covers* y. This corresponds to the relation $y \preceq x$. In the lattice of flats, each level corresponds to a rank, starting at the bottom, which is rank 0. If F_1 covers F_2, then $F_2 \subset F_1$. All of those properties in the definition of the lattice just mean that taking the intersection of two flats, or the closure of the union of two flats, will uniquely identify another element of the lattice (connected by lines to your original two entries).

When considering a matroid in terms of flats, one often sees $\mathcal{M} = (E, \mathcal{L})$ in lieu of $\mathcal{M} = (E, \mathcal{F})$ as a reminder that the set of flats forms a lattice. We will follow that convention going forward as well.

This lattice structure is key to the construction of our objects of interest in the following chapters, as we will soon see. The final definition we need from matroids are called flags, and they are, basically, just reasonable collections of flats.

1.3.3.2 Flags

Given a matroid $\mathcal{M} = (E, \mathcal{L})$, let $\mathcal{L}^*$ be the set of proper flats of $\mathcal{M}$; i.e. all flats with rank greater than 0 and not including E. Since *every* lattice of flats always has 1 element of rank 0 as a minimal element and E as the unique maximal element, $\mathcal{L}^*$ is just the interesting bits of $\mathcal{L}$.

Definition 1.13 (Flag)**.** If $\mathcal{M} = (E, \mathcal{L})$ is a matroid, then a *flag* is a totally ordered subset $\mathscr{F} \subseteq \mathcal{L}^*$ of the proper flats of a matroid,

$$\mathscr{F} = \{F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_k\} \subseteq \mathcal{L}^*.$$

If $\operatorname{rk}(\mathcal{M}) = r + 1$, then a flag $\mathscr{F} = \{F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_r\}$ is a *maximal* flag of $\mathcal{M}$.

Flags are, then, just collections of flats where you can nest all the flats; a little set theoretic *matryoshka*. On the Hasse diagram, a flag will have at most one element from each

rank and there will be a strictly increasing path of lines between all elements of the flag. Maximal flats will be those that take you along a path on the Hasse diagram from rank 1 all the way up to the rank right below that of the matroid itself, including something from every rank in between. One thing to remember is that for every flat F, $\mathscr{F} = \{F\}$ is, indeed, a flag.

1.3.3.3 Ṫis the Gift to Be Simple

If a serious matroid theorist is, for some inexplicable reason, subjecting themselves to this section, we feel the need to admit one simplifying assumption we intend to make (and have implicitly made with our example). Since we care primarily about the lattice structure of our matroid, we assume all of our matroids are *simple*.

For the rest of us, the non-serious, a brief explanation. A matroid is simple if it does not have any *loops*, elements in the ground set that have rank 0, or *parallel edges*, sets of elements that share identical independence relations. If this feels overly restrictive, worry not, for Oxley[4, p. 49] comes to our rescue.

Proposition 1.4 (Simplification Preserves Lattice Structure)**.** *For any matroid $\mathcal{M}$, there exists a unique, up to labeling, matroid* $\mathrm{si}(\mathcal{M})$*, called the* simplification of $\mathcal{M}$ *such that*

i. $\mathrm{si}(\mathcal{M})$ *is simple,*

ii. if $\mathcal{L}$ is the lattice of flats of $\mathcal{M}$ and $\mathcal{L}'$ is the lattice of flats of $\mathrm{si}(\mathcal{M})$*, then*

$$\mathcal{L} \cong \mathcal{L}'.$$

If we care mostly about the lattice of matroids, then we can take any matroid and find a simple matroid with an identical lattice structure. We'll see the main practical benefit of working with simple matroids in the next section. However, we also get convenience, we don't have to keep track of unnecessary letters, and aesthetics, the lattice diagrams look much nicer, as a bonus. If we take our matroid to be simple, then our lattice structure has the following properties.

Proposition 1.5 (Properties of the Lattice of Simple Matroids)**.** *Let $\mathcal{M} = (E, \mathcal{L})$ be a simple matroid. Then*

i. the empty set is the minimal, rank 0, element of $\mathcal{L}$,

ii. for every $e \in E$, there is unique rank 1 flat, F_e, such that $F_e = e$,

iii. for any flat $F \in \mathcal{L}$, if $e \in F$, then $F_e \subseteq F$,

iv. we can write any flat $F \in \mathcal{L}$ as a disjoint union of rank 1 flats; $F = \biguplus_{e \in F} F_e$.

If this seems like a lot, the big takeaway is that this promises that the very bottom of our lattice will always be the empty set, and that the rank 1 flats correspond to the elements of the ground set. For those coming in with lattice knowledge, the second two properties mean the lattice of a simple matroid is *atomic*. We can verify these properties in our example, M, which is a simple matroid.

That admission of simplification done, we have now learned everything we need about the construction of matroids. It's time to learn about some polynomials.

1.4 The Characteristic Polynomial

The conjecture by Heron, Rota, and Welsh, that we promise we are getting to, has to deal with the characteristic polynomial of a matriod. This is some polynomial we can cook up using the structure of a matroid, which is fair enough. But when presented on its own, it feels, at least to us, that it comes out of nowhere. Why anyone would make up this polynomial or why we'd start conjecturing about it is not at all clear.

So first, a little history back in the realm of graphs.

1.4.1 Coloring Graphs and the Chromatic Polynomial

Let us play another game. This time, pick a graph, G, like the one pictured below.

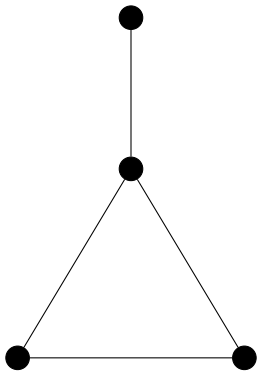


Figure 1.8: An example graph, G

Let's say we have three colors, and we want to color the vertices of the graph so that no two connected vertices have the same color. Such an arrangement of colors would be called a 3-coloring of G. It's not too hard to come up with some colors that work.

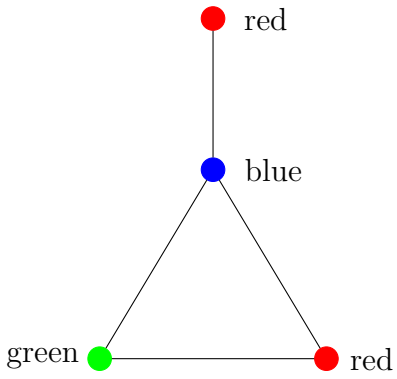


Figure 1.9: A 3-coloring of G

But now, suppose we wanted to know how many unique ways we could use those three colors to color the graph. This isn't too bad. We could just get out our markers and start coloring lots of graphs. Honestly, it sounds relaxing.

But now let's suppose we want to know how many ways we can use 1000 colors to color our little graph, or 10,000, or a billion. Since our set of markers only has 12 distinct colors, we will have to turn to math to solve this one.

The strategy is not too complicated, just pick a vertex and say how many colors we have to choose from, then find a connected vertex that hasn't been assigned a color yet, and say how many colors it is allowed to choose from. Repeat until we're out of vertices to label. Instead of picking a specific number, let's say we have n colors to choose from.

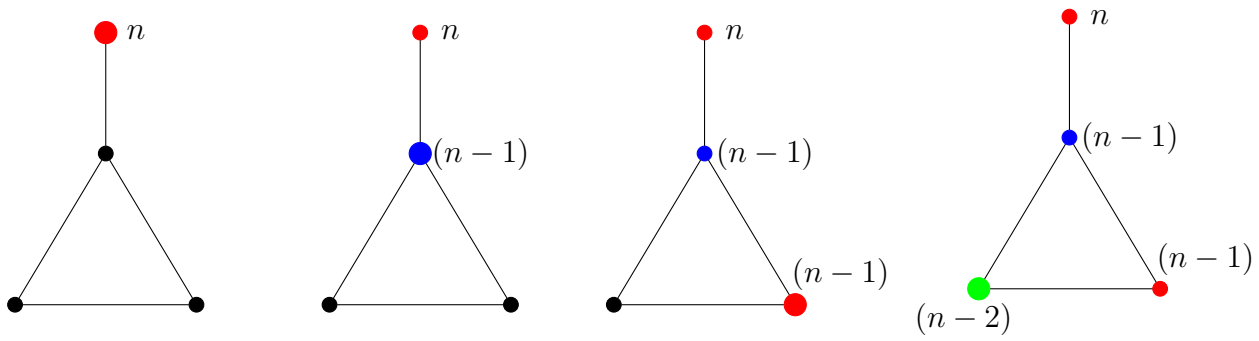


Figure 1.10: The process of figuring out the number of n-colorings of G; the choice of starting vertex doesn't matter, though that's not necessarily obvious

We then just have to multiply the number of possibilities together. For G, if we have n colors to choose from, there are $n(n-1)^2(n-2)$ different ways to arrange those colors on the graph. We've just discovered the *chromatic polynomial* of G. But there's nothing particularly special about our choice of graph, we will get something like this for any graph we come up with.

Proposition 1.6 (Chromatic Polynomial of a Graph)**.** *Let $\chi_G(n)$ be the number of n-colorings of graph G. Then the map*

$$z \mapsto \chi_G(z)$$

is a polynomial with integer coefficients, known as the chromatic polynomial *of G.*

For our purposes we will always expand our polynomials, so for our worked example above we have

$$\chi_G(z) = z^4 - 4z^3 + 5z^2 - 2z.$$

Early work in chromatic polynomials was done by none other than our good friend Whitney [10], and expanded on by the mathematician Tutte in his development of what we now call Tutte polynomials [7].

1.4.2 The Characteristic Polynomial of a Matroid

It was following in this work on chromatic polynomials that Gian-Carlo Rota, who you may recognize as usually sandwiched between Heron and Welsh, extended this concept to matroids [5]. To do this, Rota extended something called the *Möbius function* to lattices

(technically any locally finite poset), which for matroids means it uses the lattice structure of the flats. We present an equivalent definition that's easier to state, but with the downside that the relationship to the lattice is obfuscated.

Definition 1.14 (Characteristic Polynomial)**.** Let $\mathcal{M} = (E, \mathcal{L})$ be a matroid. Then the *characteristic polynomial* of $\mathcal{M}$ is given by

$$\chi_{\mathcal{M}}(z) = \sum_{X \subseteq E} (-1)^{|X|} z^{\mathrm{rk}(\mathcal{M}) - \mathrm{rk}(X)}.$$

You may notice that each term of the polynomial will have a power of z between 0 and $\mathrm{rk}(\mathcal{M})$. The Heron-Rota-Welsh conjecture is about the coefficients of this polynomial, specifically once we collect the terms.

Definition 1.15 (Whitney Numbers of the First Kind)**.** Let $\mathcal{M}$ be a matroid with characteristic polynomial

$$\begin{aligned}\chi_{\mathcal{M}}(z) &= \sum_{X \subseteq E} (-1)^{|X|} z^{\mathrm{rk}(\mathcal{M}) - \mathrm{rk}(X)} \\ &= \sum_{k=0}^{\mathrm{rk}(\mathcal{M})} (-1)^k w_k z^{\mathrm{rk}(\mathcal{M}) - k}.\end{aligned}$$

The unsigned portion of the coefficients $w_0, w_1, \ldots, w_{\mathrm{rk}(\mathcal{M})}$ are the *Whitney numbers of the first kind.*

We will return to these numbers very soon. Before that, a few interesting facts about the characteristic polynomial.

Proposition 1.7. *Let $\mathcal{M}$ be a matroid with a loop; that is some element $e \in E$ such that $\mathrm{rk}(e) = 0$. Then*

$$\chi_{\mathcal{M}}(z) = 0.$$

Getting to ignore these trivial characteristic polynomials is the concrete benefit for assuming we only deal in simple matroids. A loop makes the characteristic polynomial easy to calculate, just not at all interesting

Finally, we want to wrap up the graph connection. Since any graph can be represented by a matroid, and the characteristic polynomial is in some sense inspired by the chromatic polynomial, it would be natural to ask if there is a relation between them. And there is, in fact, a very nice one.

Proposition 1.8. *Let G be a graph and $\mathcal{M}(G)$ be the matroid that comes from G. Then*

$$\chi_G(z) = z^c \chi_{\mathcal{M}(G)}(z),$$

where c is the number of connected components of G.

For those who want more on the connections between these values, and how they relate to the more general Tutte polynomial, we found the overview given by Ardila [2] to be a great help.

1.5 The Heron-Rota-Welsh Conjecture

We now have all the knowledge of matroids necessary to state the Heron-Rota-Welsh conjecture. Developed and formalized by Heron [3], Rota [6], and Welsh [8], this was a conjecture about the coefficients of the characteristic polynomial of matroids. We say "was" because, as noted in the introduction, this has proven by Adiprasito, Huh, and Katz [1]. We're going to keep calling it a conjecture though.

First, a few definitions necessary to carefully state the conjecture.

Definition 1.16 (Unimodal)**.** A sequence of numbers $x_0, x_1, \ldots, x_k$ is called *unimodal* if there exists an index i such that

$$x_0 \leq x_1 \leq \cdots \leq x_i \geq \cdots \geq x_{k-1} \cdots x_k.$$

The values of a unimodal sequence get larger until a certain point, and after they start to decrease. Such a sequence is also known as *concave*, since the average of any two non-consecutive points in the sequence will be less than a point in between them; i.e. for a sequence $x_0, x_1, \ldots, x_k$ and $i < j < k$,

$$2x_j \geq x_i + x_k.$$

We can define an even stronger condition.

Definition 1.17 (Log-Concavity)**.** A sequence of numbers $x_0, x_1, \ldots, x_k$ is called *logarithmically concave*, or log-concave, if

$$x_i^2 \geq x_{i-1}x_{i+1}$$

for $0 < i < n$.

When all x_i are positive, log-concavity implies the sequence is also unimodal. This is the last piece of the puzzle.

Theorem 1.9 (Heron-Rota-Welsh Conjecture)**.** *Assume we have a matroid $\mathcal{M} = (E, \mathcal{L})$ of rank $r + 1$. If*

$$\chi_{\mathcal{M}}(z) = \sum_{k=0}^{\mathrm{rk}(\mathcal{M})} (-1)^k w_k z^{\mathrm{rk}(\mathcal{M})-k}$$

is the characteristic polynomial of $\mathcal{M}$, where $w_0, w_1, \ldots, w_r$ are the Whitney numbers of the first kind, then

$$w_i^2 \geq w_{i-1}w_{i+1}$$

for $0 < i < \mathrm{rk}(M)$.

That is, the absolute values of the coefficients of the characteristic polynomial of the matroid $\mathcal{M}$ are log-concave.

Since we want to show something about the characteristic polynomials of the matroid, we need a way to study it. To do so, we are going to find the characteristic polynomial in some unexpected places, and then leverage properties of those other settings.