What is a Matroid?

Matroids have become ubiquitous in modern mathematics, and a common selling point for matroids revolves around the many different ways to define them. Miraculously, these 'cryptomorphic axiomatizations' all turn out to give the same object.

Matroids are meant to generalize various mathematical objects. I'll give one definition, and then I'll discuss two such objects: graphs and vector spaces.

Some Set Terminology

The set $\{1,2,3\}$ is a *subset* of the set $\{1,2,3,4\}$, and we write this using the notation $\{1,2,3\} \subset \{1,2,3,4\}$. Further examples area $\{1,4\} \subset \{1,2,3,4\}$, and $\{\} \subset \{1,2,3,4\}$. This last set $\{\}$ is a special set we call the *empty set*, $\varnothing$, because it contains no elements. The empty set is a subset of every set.

The element 1 is in the set $\{1,2,3,4\}$, and we write this as $1 \in \{1,2,3,4\}$. The number of elements of a set A is written $|A|$, and for example $|\{1,2,3,4\}| = 4$.

Given two sets, A and B, the set of elements that are in B, but not in A, is written as $B \backslash A$. The set of elements in both A and B is written as $A \cup B$ ('A union B'). The set of elements in A or in B is written as $A \cap B$ ('A intersect B').

1 Independent sets

(If you know what a vector space is, you should think this definition as analogous to linear independence.) One definition of matroids uses *independent sets*. (The terminology comes from linear independence.) A *matroid*, M, defined by independent sets comes with two pieces. We call the first piece, E, the *ground set* of M. E is a collection of elements, and usually we will use the first n numbers $E = \{1, 2, \ldots, n\}$ for this collection.

The second piece of incormation is $\mathcal{I}$, the collection of *independent sets* of M. We write $M = (E, \mathcal{I})$ to record the two pieces of information Elements of $\mathcal{I}$ are subsets of E satisfying some properties, and we call the elements of $\mathcal{I}$ independent. I'll list these properties, and then translate them into English.

1. $\varnothing \in \mathcal{I}$
2. If $A \in \mathcal{I}$ and $B \subset A$, then $B \in \mathcal{I}$
3. If $A \in \mathcal{I}$, $B \in \mathcal{I}$ and $|B| > |A|$, then there is $b \in B \backslash A$ with $A \cup \{x\} \in \mathcal{I}$

Property 1 says that the empty set is independent. Property 2 says that any subset of an independent set is independent. Property 3 says that if you have two independent sets A and B with different sizes, you can take an element from the bigger one (B) and add it to the smaller one (A) to get a larger independent set. Let's do some examples.

1.1 Uniform Matroids

Let $E = \{1, 2, 3, 4\}$. Let $\mathcal{I} = \{\varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{12\}, \{13\}, \{14\}, \{23\}, \{24\}, \{34\}\}$. In words, all the zero, one, and two element subsets of E are independent. Let us check that $M = (E, \mathcal{I})$ is a matroid.

1. The empty set $\varnothing$ is in $\mathcal{I}$, so property 1 is satisfied.
2. The only subset of the empty set $\varnothing$ is itself, so every subset of any zero element set in $\mathcal{I}$ is in $\mathcal{I}$.

   The only subsets of $\{1\}$ are $\varnothing$ and $\{1\}$ itself. Both of these are in $\mathcal{I}$, so we are safe. Check the rest of the one element sets in $\mathcal{I}$ the same way.

   The only subsets of $\{1, 2\}$ are $\varnothing, \{1\}, \{2\}$, and $\{1, 2\}$. All of these are in $\mathcal{I}$, so we are still safe. Check the rest of the two element sets in $\mathcal{I}$ the same way.
3. Take $A = \varnothing$ and $B = \{1\}$. $1 = |B| > |A| = 0$, and we can add 1 to $\varnothing$ to get a larger independent set, so we are safe. Check the rest in the same way.

   Take $A = \varnothing$ and $B = \{1, 2\}$. Then we can add either 1 or 2 to $\varnothing$, so we are safe. Check the rest the same way.

   Take $A = \{1\}$ and $B = \{1, 4\}$. We can add 4 to A, so we are safe. Take $A = \{1\}$ and $B = \{2, 3\}$. We can add either 2 or 3 to A, so we are safe. Check the rest the same way.

After a lot of painful checking, we find that the M we defined above is actually a matroid. This matroid has another name: the *uniform matroid* $U_{2,4}$. The 4 refers to the size of E, and the 2 refers to the fact that every subset of E that has two or fewer elements is independent. In general, $U_{k,n}$ is a matroid with $|E| = n$ and every subest of E with k or fewer elements is independent.

In fact, the above checking was so painful that we never want to do it again. Unfortunately, if we want to prove that something is a matroid, then we are out of luck: we have to check these properties. However, you can get a computer to check it. (Sage has a great matroids package `http://doc.sagemath.org/html/en/reference/matroids/index.html`.)

Here is code that would check the same thing we did by hand above:

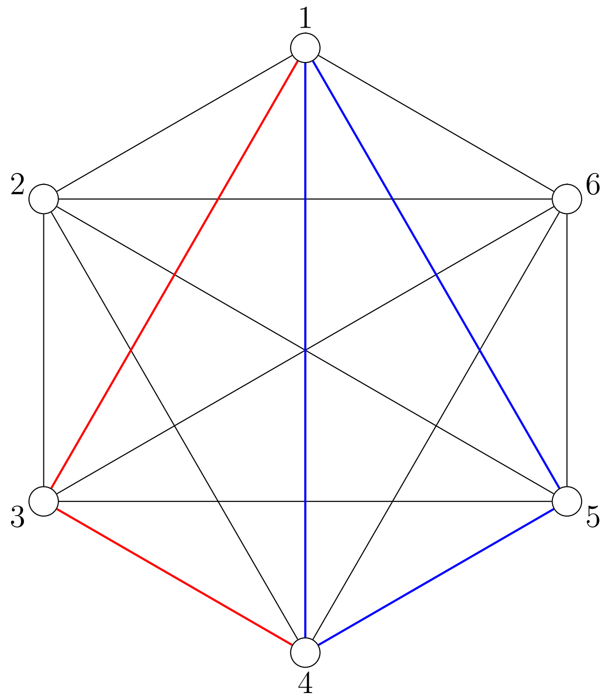
```
#test whether the E and I from above forms a matroid.
M = Matroid(groundset='1234',
independent_sets=['','1','2','3','4','12','13','14','23','24','34'])
M.is_valid() #return True is M is a matroid and False otherwise
M.is_isomorphic(matroids.Uniform(2,4)) #Check whether M is the uniform matroid
```

Sage has many examples of matroids to play with, and you can try out sage using an online server `https://sagecell.sagemath.org/`. Even better than checking the properties one by one is checking the properties for a general construction. This gives you many matroids at once, and we'll do this below for the case of graphs.

2 Matroids from Graphs

A graph is two pieces of data: *vertices* and *edges*. Graphs model relationships (edges) between objects (vertices). A ubiquitous example is social media. In this case, the vertices represent people, and the edges represent relationships. On Facebook, two people are connected by an edge if they are friends.

Imagine that you and 8 other people are all mutual friends. Then the graph representing friendships among you and your friends looks like the one below:



Imagine you are starting at the vertex 1 in the above graph. Maybe you decide to walk to 3, and from there you decide to walk to 4. The *path* $1-3-4$ is highlighted in red. In a general graph, a path is just a sequence of edges that you could walk along. A *cycle* is a path that begins and ends at the same vertex. An example $1-4-5-1$ is colored blue.

To define a matroid from a graph, we'll set the ground set E to be the set of edges. Then the independent sets will be those sets of edges that do not contain a cycle. For example, in the above graph, the red edges form an independent set, but the blue ones do not. The matroids you get this way are called *graphic*.

3 Why should you care?

Matroids seem very mathematical, but they can model many real problems. Many graph theory problems can be restated in matroid language using the construction above, and the restatement of famous graph algorithms – Kruskal's *minimum weight spanning tree* or *finding a matching in a graph* – have very natural interpretations. Similarly, we can (and do!) go the other way. Proving statements for matroids also proves them for all the objects matroids generalize, and this is a very powerful tool in mathematics.