Matroids

Eric Cohan

7/7/2021

Matroids are one of the most basic algebraic structures in mathematics. They outline independence in systems, and have many equivalent definitions across fields of mathematics. I have found those building off of linear algebra to be the most intuitive, one of which being linear independence between a set of vectors. A series of vectors $v_1, ..., v_n$ is linearly independent if there are no constants $a_1, ..., a_n$ that satisfy the equation $a_1v_1 + a_2v_2 + ... + a_nv_n = 0$ other than $a_i = 0$ for all a_i. This addition of scaled vectors is called a linear sum, hence *linear* independence.

This might not be the most intuitive definition if you haven't worked with vectors in this context, but it's pretty much asking if all of your vectors point in different-enough directions. We can get an equivalent definition by subtracting one of the vectors and dividing by it's scalar, for one of the vectors that isn't scaled by zero. For some other list of a's, we get: $a_1v_1 + ... + a_{n-1}v_{n-1} = v_n$, which might convey the sense of independence a little better. Vectors that *aren't* independent can expressed in terms of the others in the set. (in $\mathbb{R}^2$ any two vectors that are not scaled versions of each other are linearly independent, but any third vector could be expressed as a linear sum of the first two. Think about it for a bit and it should make sense that the number of vectors is related to the dimension of the space.)

The Matroid $M = (E, I)$ is composed of a "ground set" E and a set of subsets of E, which are defined to be "independent," called I, such that:

- $I \neq \{\}$, There exists some subset that is independent.
- $A \subseteq B \in I \implies a \in I$ Every subset of an independent set is independent
- For all $|A| > |B| \in I, \exists a \in A$ such that $B \cup a \in I$, For all independent subsets of different sizes, there is an element of the larger that could be added to the smaller such that it remains independent.

Which, for those familiar with linear independence, it quite intuitively applies between vectors. Matroids show from the most basic of building blocks properties that you have likely already worked with. Even within the scope of linear algebra there are alternative definitions, especially for the last axiom, which gets a special name, the "exchange axiom," which is more intuitive with other choices for it. (Like the ability to swap vectors between two distinct bases and have them remain bases.) A matroid based on linear independence is called a linear matroid.

Matroids have many other equivalent definitions, some relying on rank functions, columns or rows of a matrix, and closure/span of vectors, which, from a linear algebra perspective, are all intimately related. More interesting is the definition based on graph theory. A graph is defined as a set of vertices and a set of edges, unordered pairs of vertices. First we need some definitions:

- A Basis of a matroid is a maximal independent set.
- A Path is a set of edges such that they can be ordered so edge starts from the vertex the previous edge ended on.
- A Circuit is a path that ends on the vertex it started on.
- A Connected Graph is a graph where each vertex has a path to each other vertex.
- A Tree is an acyclic connected graph, or a graph which contains no circuits. All paths are unary trees .
- A Spanning Tree is a maximal tree, and is the basis of a connected graphic matroid. On a connected graph maximal trees include every vertex.
- A Forest is a disjoint set of Trees, or simply an acyclic graph (without the "connected" requirement). Spanning Forests analogously

Remember that for a spanning trees and forest are maximal in terms of the number of edges they have, not vertices they touch. For a tree this is the same, but for a forest it is not, hence there can be a forest that "spans" all vertices, but additional edges may be includable (connected subtrees), so it may not be maximal. Rather pedantically, paths, trees, only contain edges and not vertices, when we say "a vertex in a given forest" we mean a vertex in one of the edges of the forest.

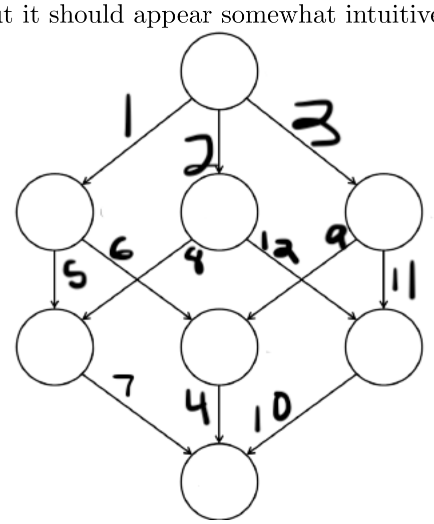
One way to define a Matroid with a graph is with a ground set of edges of the graph and the independent set as the set of all forests in the graph. This is called a graphic matroid. We can see it satisfies similar conditions as the linearly independent vectors:

- $I \neq \{\}$, There exists some forest. (the empty forest is a forest)
- $A \subseteq B \in I \implies A \in I$, All subsets of forests are forests
- For all $A, B \in I, |A| > |B|$, there exists an edge $e \in A/B$ such that $B \cup e \in I$

These are all evident from the definition of a forest, though with a little more thought into the axiom of exchange, we can define a matroid on a connected graph and the set of *trees*.

An important feature we want to show is that all bases of a matroid have the same size. This follows from the third axiom, as if we have two independent sets of different sizes, we know the smaller of them can always be extended, and is hence not maximal and not a basis. This helps us extended another linear algebra concept: rank. We can say the rank of a set is the size of its maximal independent subset.

An interesting and useful property of graphic matroids is, when dealing with weighted edges, you can use the greedy algorithm! For example, say a company wants to build a phone line that connects many different points. They first estimate the cost of connecting pairs of locations (possibly not every pair, though *that* might not give the optimal solution) and construct a connected graph of said points, weighing each edge with the expected cost. They can find the minimally costed spanning tree using a greedy algorithm: by repeatedly choosing the minimally costed edge that connects previously unconnected points, they'll be guaranteed the best network! (on the way they may have a forest, but never something it would always be acyclic) Rather shockingly they are the only simplicial complex where this holds (a simplicial complex requiring only the first two axioms), and furthermore the greedy algorithm working can even be interchanged with the last axiom! The proof for this is a little more complicated, but it should appear somewhat intuitive with an example:



To get the minimally weighted spanning tree, we'd start with the minimally weighted edges and check if the we can add them without losing independence. We'd start with the edge evaluated as 1, then 2, through edge 6 would all be acyclic. If we tried to add edge 7 though, this would form a circuit with 4, 5, and 6. 8 and 9 would also for cycles, so we skip them too, but 10 would connect us to the final vertex and give us our minimal spanning tree.

This was pretty brief, but if you want to look deeper some terminology to look into are:

- The Dual of a matroid is a unique, "inverse" matroid denoted by M^*, defined on the same ground set, but with bases which are complementary to those in M.

- The Deletion of a set from a matroid gives a new matroid whose ground set is the remaining elements of E and whose independent sets simply have the deleted elements removed.
- The Contraction of a set and a matroid is the subtraction of a set from the dual of a matroid. So the contraction of M and S is $(M^* - S)^*$

These concepts were mostly built out of graph theory, but can be quite useful when applied to matrices of other forms. (and there's *a lot* out there about them!)

- A Trivial Matroid has an independent set consisting of exactly the empty set
- A $k-$uniform matroid on E means every subset of E of size k is a basis
- A matroid on E is free or discrete if all subsets of E are independent, this is a special case of uniform matroids, for $k = |E|$

Note that no vector space will be a uniform matroid, because they must include the zero vector which will never be part of an independent set. Unlike vector spaces, matroids don't require closure of any kind, so you could have a uniform matroid that is a finite subset of a vector space. A matroid of a finite subset of $\mathbb{R}/0$ and linear independence would be a 1-uniform matroid.