MATROIDS

ARPIT MITTAL

Abstract. After briefly touching independence in vector spaces and graph theory, we begin with the definition of a matroid, and then give analogous results in graph theory. We then briefly study bases and circuits, and quickly move on to a more interesting topic, nullity. After this, we examine multiple types of matroids, and gloss over a few results that come from those definitions. We can then examine one of the most important applications of matroids, the greedy algorithm. Finally, as mentioned in the introduction, matroid theory has some interesting conjectures, so we look at one of the most important conjectures in matroid theory.

1. Introduction

In the most basic of terms, matroids generalize linear independence in vector spaces. Although this may sound like a very small topic, matroids appear in many fields of math such as linear algebra, graph theory, and partially-ordered sets. There are even applications of Matroids in topology, combinatorial optimization, and coding theory. Because of their vast reach, matroids are very important and have thus had many papers and books written about them, some of which go deep into applications of matroids that nobody would have guessed, including applications in hyperplanes. As matroid theory was introducted by Hassler Whitney[1] in 1935, it is a relatively new subject and has some fascinating open problems including the Aharoni-Berger Conjecture and Rota's Unimodal Conjecture.[2]

[1]https://en.wikipedia.org/wiki/Hassler_Whitney

[2]http://www.openproblemgarden.org/category/matroid

2. Definitions

2.1. **Linear Independence.** As matroids generalize linear independence, we cannot learn matroids without first understanding the meaning of independence.

Definition 2.1. A set of vectors V in a vector space $S \supseteq V$ are said to be *linearly dependent* when there are vectors $v_1, \dots, v_n \in V$ and scalars $s_1, \dots, s_n \neq 0$ such that $v_1 s_1 + \cdots + v_n s_n = 0$. If this is not true, V is *linearly independent*.

The following properties hold about finite independent subsets of vector spaces:

(1) Every subset of an independent set is independent.
(2) If A and B are independent sets, with $|B| > |A|$, then there is some $x \in B \setminus A$ such that $A \cup \{x\}$ is independent.
(3) All maximal subsets of a finite subset of V have the same cardinality.

2.2. **Graph Theory.** We also have similar results of independence in Graph Theory, although our definition of independence here might be slightly different:

Definition 2.2. Let there be a finite undirected graph G with E denoting its set of edges and V denoting its set of vertices. A set of edges $S \subseteq E$ is *independent* if it contains no cycles, and is *dependent* otherwise.

We can also say that S is independent if the induced graph is acyclic.[3] Similar properties hold in this new context:

(1) Every subset of an acyclic set of edges is acyclic.
(2) If A and B are sets of edges, both acyclic with $|B| > |A|$, then there is some $x \in B \setminus A$ such that $A \cup \{x\}$ is acyclic.
(3) All maximal acyclic subsets of a subset of edges have the same size.

It should be clear that these properties are almost identical to the ones for independent subsets of vector spaces. We can also say that an edge $e \in E$, where E is the edge-set, is *spanned* by a set of edges $S \subseteq E$ if there is some path in S that connects the two endpoints of e. Because it is not certain that G is a simple graph, it is possible for e to be a self-loop, and when this is the case, the empty path connects the endpoints of e. So, e is spanned by any set of edges.

2.3. **Matroids.**

Definition 2.3. We define a matroid as an ordered pair $(E, \mathcal{I})$ where E is a finite set, and $\mathcal{I}$ is a collection of subsets of E, such that:

(I1) $\mathcal{I}$ is non-empty.
(I2) If $A \in \mathcal{I}$, and $x \subseteq A$, then $x \in \mathcal{I}$.
(I3) If $A, B \in \mathcal{I}$, and $|B| > |A|$, then there exists some $x \in B \setminus A$, that $A \cup \{x\} \in \mathcal{I}$.

Note that when we use $|S|$ we mean the cardinality of the set S. The set E and the collection of subsets $\mathcal{I}$ are known as the ground set and independent sets respectively. Let us look at an example of a matroid.

Example. Let $E = \{1\}$ and $\mathcal{I} = \{\{\emptyset\}, \{1\}\}$. We see that $\mathcal{I}$ is non-empty, so axiom (I1) holds. The only subset of $\{\emptyset\}$ is $\{\emptyset\}$, and the only subsets of $\{1\}$ are $\{\emptyset\}$ and $\{1\}$, so since both subsets are in $\mathcal{I}$, (I2) holds. $\mathcal{I}$ has only two elements so we have $|\{1\}| > |\{\emptyset\}|$. If we append $\{1\}$ to $\{\emptyset\}$, then $\{\emptyset\} \cup \{1\} \in \mathcal{I}$. Thus, axiom (I3) holds so $(E, \mathcal{I})$ is a matroid.

We could have we could have replaced axiom (I3) with

(I4) If $S \subseteq E$, the maximal independent subsets of S have the same cardinality.

Let us see why these two axioms are essentially the same. The proof of (I3) $\implies$ (I4) follows from applying (I3) on two maximal subsets of S if one has a larger cardinality than the other. The proof of (I4) $\implies$ (I3) follows from applying (I4) with $S = A \cup B$. Because $|A| < |B|$, A is not a maximal independent subset of S, so there is some $x \in B \setminus A$ that can be appended to A to produce an independent set.

[3] `https://en.wikipedia.org/wiki/Directed_acyclic_graph`

From this general definition of a matroid, we can define two types of matroids, from both linear algebra and graph theory. If V is a vector space over a field k, and E is a *finite* subset of V, then we can define a matroid M on E whose independent sets are the sets that are linearly independent in V. This is the linear algebra type of matroid, and it is sometimes known as a *matric*[4] , *vector*, or *representable* matroid. When speaking, we say that "M is representable over k. " To go into the graph theory "type" of matroid, we will need some new terminology that will be introduced in subsection 2.4.

2.4. **Bases, Circuits, and Graphic Matroids.** As promised in the prior subsection, we will define the graph theory type of matroids in this subsection. However, we must first define bases and circuits.

Definition 2.4. Let there be a matroid M on ground set E. Then,

(1) A set $S \subseteq E$ is dependent iff it is not independent.
(2) A set $B \subseteq E$ is a basis iff it is a maximal independent set.
(3) A set $C \subseteq E$ is a circuit iff it is a minimal dependent set.

For representable matroids, specific definitions for bases and circuits can be found in [1].

Proposition 2.5. *The following statements hold:*

(1) *No basis is contained in a different basis.*
(2) *If A and B are distinct bases, then for every $x \in A \setminus B$ there is a $y \in B \setminus A$ such that $(A \setminus \{x\}) \cup \{y\}$ is a basis*
(3) *If A and B are distinct bases, then $|A| = |B|$.*
(4) *No circuit is contained in a different circuit.*

Proof. Properties (1) and (4) follow from the definitions of bases and circuits respectively. Property (3) follows from axiom (I4) applied to the entire matroid. To prove property (2), we can first apply (I3) to the sets $A \setminus \{x\}$ and B, to see that $(A \setminus \{x\}) \cup \{y\}$ is independent for an appropriate y. We can let $X = (A \setminus \{x\}) \cup \{y\}$, and since it has the same cardinality as A, X is a basis from property (3). ∎

We now have the tools required to define a matroid in a graph theory way.

Definition 2.6. If G is a graph with edge-set E and vertex-set V, the cycle matroid of G has ground set E and has independent sets $S \subseteq E$ such that S is acyclic. These matroids are called *graphic matroids.*

In graphic matroids, a set $D \subseteq E$ is dependent iff it contains a cycle, so a circuit in a graphic matroid is merely a simple cycle. If the underlying graph G of the graphic matroid is connected, a maximal independent set is a spanning tree. If G is not connected, then there will be a spanning forest that has a spanning tree in each component of G. The size of a spanning tree is one less than the number of vertices,[5] so the size of a spanning forest in G will be the number of vertices in G minus the number of connected components. Thus, all bases in G have the same size. For any $S \subseteq E$, we can use the same argument as above on the subgraph of G that is obtained from deleting the edges outside of S. This shows that (I4) holds for a graphic matroid, which proves that graphic matroids are matroids.

2.5. **The Rank Function.**

Definition 2.7. In a matroid $(E, \mathcal{I})$, the rank of a set $S \subseteq E$ is the size of a maximal independent subset of S. The rank of the matroid is the rank of all E.

Since we previously defined a basis as the maximal independent subsets of a matroid, the rank of a matroid is simply the size of one of its bases. If we define the function $r(S)$ as the rank of S, the following inequality is true:

Proposition 2.8. *If $A, B \subseteq E$, then $r(A) + r(B) \geq r(A \cup B) + r(A \cap B)$.*

Proof. Let S be a maximal independent subset of $A \cap B$ and $T \supseteq S$ be a maximal independent set of $A \cup B$. Then, $T \cap (A \cap B) = S$. We also have $|S| = r(A \cap B)$ and $|T| = r(A \cup B)$ by our definitions of S and T. In addition to this, we have $|T \cap A| \leq r(A)$ and $|T \cap B| \leq r(B)$. The first inequality in the prior sentence is obvious from our definitions, and the second ineuquality is true because $T \cap B$ is an independent subset of

[4]The word "matric" generally means when the vectors in E are the columns of a matrix.
[5]You can prove this via induction on the number of edges in the tree.

B, but is not guaranteed to be a *maximal* independent subset. With these new inequalities, all we have to do now is prove that

$$|T \cap A| + |T \cap B| = |T \cap A \cap B| + |T|$$

is true, and it is true because of the Principle of Inclusion-Exclusion. ■

In abstract algebra, all groups have the closure property which means that all applications of the group's binary operation results with an element that is in the group. Although not entirely the same, we also have the closure function of matroids. This is also referred to as the span of the matroid.

Definition 2.9. If S is a set in the matroid M, then the closure of S is the set

$$cl(S) = \{x : r(S \cup \{x\}) = r(S)\}.$$

If x is in the closure set S, we may say that x spans S, or x depends on S.

2.6. **Nullity.**

Definition 2.10. The *nullity* of a set $S \subseteq E$ is $n(S) = |S| - r(S)$.

Proposition 2.11. *For any sets A, B, we have*

$$n(A) + n(B) \leq n(A \cup B) + n(A \cap B).$$

Proof. We first have $|A| + |B| = |A \cup B| + |A \cap B|$ from the Principle of Inclusion-Exclusion. We can subtract the inequality from Proposition 2.8 from this to see that:

$$|A| - r(A) + |B| - r(B) \leq |A \cup B| - r(A \cup B) + |A \cap B| - r(A \cap B)$$

which completes the proof. ■

3. Types of Matroids

Although we will not get very in-depth with them, we will briefly look at some common examples of matroids.

Base-Orderable Matroids: Matroids that satisfy the property that for any two bases A, B, there exists a bijection $f : A \to B$ such that for each $a \in A \setminus B$, both $(A \setminus \{a\}) \cup \{f(a)\}$ and $(B \setminus \{f(a)\}) \cup \{a\}$ are bases.

We can create a stronger condition to define a Strongly Base-Orderable Matroid.

Strongly Base-Orderable Matroids: Matroids that satisfy the property that for any two bases A, B, there exists a bijection $f : A \to B$ such that for every $X \subseteq A$, both $(A \setminus X) \cup f(X)$ and $(B \setminus f(X)) \cup X$ are bases.

3.1. **Transversal Matroids.** A set system $(S, \mathcal{A})$ is a set S and a multiset $\mathcal{A} = (A_j : j \in J)$ of subsets of S. Because of this definition, it is possible that the same subset of S will appear multiple times in $\mathcal{A}$. We can also write $\mathcal{A}$ as a sequence of subsets of S. The order of the sequence is non distinguishable, so we cannot swap two elements and call it a new sequence. A transversal of the set system $(S, \mathcal{A})$ is a subset X of S for which there is a bijection $\phi : J \to X$ where $\phi(j) \in A_j$ for $j \in J$.

Definition 3.1. A *partial transversal* of $(S, \mathcal{A})$ is a transversal of some subsystem $(S, \mathcal{A}')$ where $A' = (A_k : k \in K)$ with $K \subseteq J$.

Theorem 3.2. *A* finite *set system* $(S, \mathcal{A})$ *has a transversal iff, for all* $K \subseteq J$,

$$|\bigcup_{i \in K} A_i| \geq |K|.$$

As the proof of this theorem has ben omitted, a proof of this can be found in [2].

Theorem 3.3. *The partial transversals of a set system* $\mathcal{A}$ *are the independent sets of a matroid.*

The proof of this theorem can also be found in [2].

3.2. **Laminar Matroids.** A family of subsets $\mathcal{A}$ of E is laminar if when $A, B \in \mathcal{A}$ and $A \cap B \neq \emptyset$, either $A \subseteq B$ or $B \subseteq A$. If we let $\mathcal{A}$ be a laminar family of subsets of E, we can define $\tau : \{\mathcal{A}\} \to \mathbb{R}$. Let us define Y to be the set of subsets M of E such that $|M \cap A| \leq \tau(A)$ for $A \in \mathcal{A}$. Y is the set of independent sets of a matroid with ground set E. Going back to τ, τ is a capacity function for the matroid (E, Y) and the matroid can be expressed as $M(E, Y, \tau)$.

Lemma 3.4. *If* A *is independent in* $M(E, \mathcal{A}, \tau)$ *and* $B \in \mathcal{A}$*, then* A *is independent in* $M(E, \mathcal{A} \backslash \{B\}, \tau|_{\mathcal{A}-\{A\}})$.

This lemma is clearly true as it follows the definition of a laminar matroid.

Definition 3.5. A set $X \in \mathcal{A}$ is essential if $M(E, \mathcal{A}, \tau) \neq M(E, \mathcal{A} \setminus \{X\}, \tau|_{\mathcal{A} \setminus X}$.

4. Greedy Algorithm

Matroids are highly useful in the field of combinatorical optimization. A greedy algorithm in general is a process that follows the optimal step at each step. We will be paying attention to one specific greedy algorithm, Kruskal's Algorithm. If we have nodes, and links connecting the nodes, we can say that each link has a weight, or for better visualization, a *cost*. We want to spend as little money as possible, so we must find the least amount of links that we must use to connect all nodes. Each minimal spanning set is a tree, so Kruskal's algorithm is finding a tree with the least cost.

Algorithm 1 Kruskal's Algorithm

$S \leftarrow E$
$F \leftarrow \emptyset$
while $S \neq \emptyset$ and F is not spanning **do**
  Remove the min-weight edge e from S.
  if $F \cup \{e\}$ does not create a cycle **then**
    $F \leftarrow F \cup \{e\}$
  else
    Discard e
  end if
end while

We can also write this algorithm in a more understandable way as follows:

1. Create a set of edges $\mathcal{I} = \emptyset$.
2. Set the edges in order of weight.
3. Start with either the cheapest or most valuable edge, and then for each edge e, add e to $\mathcal{I}$ unless it will produce a cycle in $\mathcal{I}$.

This algorithm will always find a minimal spanning tree which satisfies our conditions. As greedy algorithms take the optimal choice at each step, this algorithm takes the cheapest or most expensive edge at each step which makes it a greedy algorithm. More algorithms can be found in [3].

We can generalize this from graphs to matroids. Let us have a matroid M and a weight function $w : M \to \mathbb{R}$ that assigns a weight to each element.[6] The weight of the entire matroid M is simply $\sum_{i \in M} w(i)$. We wish to find the basis B such that $\sum_{x \in B} w(x)$ is minimized. Let us now create a variation on Kruskal's Algorithm to use on a matroid:

1 Initialize a set of elements to be the empty set.
2 Sort the elements of M based on weight.
3 Start by going through the elements, and start with the smallest weighted elements first. For each element x, add x to $\mathcal{I}$ unless $\mathcal{I} \cup \{x\}$ is dependent.

Let us compare this algorithm to the original Kruskal's algorithm. We first made a set of objects the empty set. Then, we sorted them based on their weight or cost. And then finally, we started with the least weighted elements and added them to the independent sets unless it's union with the independent sets resulted with a dependent set. This algorithm will definitely end up with a basis.

Lemma 4.1. *At each step, the set $\mathcal{I}$ is contained in an optimal basis.*

A proof of this lemma through induction can be found in [1].

Theorem 4.2. *This algorithm always works.*

[6] Note that weights can be both positive and negative.

Proof. We already know that after completing the process, $\mathcal{I}$ will be a basis. By the lemma, $\mathcal{I}$ will be contained in an optimal basis that we can denote as B. As no basis is a subset of another basis, $\mathcal{I} = B$, so $\mathcal{I}$ is an optimal basis. ■

5. White's Conjecture

As mentioned in the introduction, matroid theory has been introduced fairly recently so there are some quite interesting open conjectures in this field. As the title of this section suggests, we will look at one of the most fascinating conjectures in this section.

Conjecture 5.1. *(White's Conjecture) For every matroid M, its toric ideal I_M is generated by quadratic binomials corresponding to symmetric exchanges.*

In 1980, Neil White conjectured that for every matroid M, its toric ideal[7] I_M is generating by quadratic bionomials corresponding to symmetric exchanges. The conjecture remains open to this day. Although the conjecture is still open, the conjecture has been proved for some specific types of matroids including graphic matroids, sparse paving matroids, lattice path matroids, and matroids with rank less than or equal to 3.[8] As most results in this conjecture go beyond the scope of this paper, we will not list any but some, including a proof of White's Conjecture holding up for strongly base-orderable matroids, and an extension of the paper's results to discrete polymatroids[9], can be found in [4].

[7]https://arxiv.org/pdf/1302.5236.pdf
[8]We did not cover majority of these matroids in this paper, but you can look them up if you like!
[9]https://en.wikipedia.org/wiki/Polymatroid

References

[1] W. Johnson, "Matroids," 2009.
[2] J. E. Bonin, "An introduction to transversal matroids," 2010.
[3] S. Oakley, "Polyhedral techniques in combinatorial optimization," 2010.
[4] M. Lasoń, "Coloring games and algebraic problems on matroids," 2013.

Email address: `arpit.mittal.2.71@gmail.com`