A BRIEF LOOK AT MATROIDS

MARK HUBENTHAL

1. Introduction

While linear independence as it applies to linear algebra is a very useful tool in mathematics, it can only be used in a specific area of study. The idea of a matroid was first explored by Hassler Whitney in a paper he wrote in 1935. Essentially, the concept of a matroid generalizes the idea of linear independence to be within a finite set of elements. These elements could be the edges of a graph, the rows of a matrix, vectors from a vector space V, almost anything. As a result, there are many specific examples of matroids and different ways to visualize them.

In this paper, we will consider some of the varying but equivalent definitions of matroids, some important examples that build on these definitions, and go through various problems. Some of the problems are taken from Wilson's *An Introduction to Graph Theory* while others are problems I invented or have seen elsewhere stated. Some important topics mentioned throughout include the Fano Matroid, the greedy algorithm from the perspective of the matroid, and finally a brief look at the matroid dual.

2. Background

Definition 1. *A* ***matroid*** *M consists of a non-empty finite set E and a non-empty collection $\mathcal{B}$ of subsets of E, called bases, satisfying the following properties:*[1]

$\mathcal{B}$(i) *no base properly contains another base*

$\mathcal{B}$(ii) *if B_1 and B_2 are bases and if e is any element of B_1, then there is an element f of B_2 such that $(B_1 - \{e\}) \cup \{f\}$ is also a base.*

Using $\mathcal{B}(ii)$ repeatedly, we can show that all bases of a matroid on a set E have the same number of elements.

Proof. Suppose we have two bases $\alpha = \{a_1, a_2, a_3, \ldots, a_m\}$ and $\beta = \{b_1, b_2, b_3, \ldots, b_n\}$ where $n > m$. Remove a_1 from α to get the set $\alpha - \{a_1\}$. By property $\mathcal{B}(ii)$, there is an element of β, say b_1, such that $(\alpha - \{a_1\}) \cup \{b_1\} = \{b_1, a_2, a_3, ..., a_m\} = \alpha_1$ is also a base. Repeating this process, we eventually acquire the set α_m which still contains m elements, all of which are contained in β. Suppose WLOG that $\alpha_m = \{b_1, b_2, b_3, \ldots, b_m\}$. However, $|\alpha_m| = m < n = |\beta|$ which implies that α_m is not a base. Thus α was never a base to begin with.

Since all bases of a matroid M have the same number of elements, a special term called the **rank** of M is defined to be the size of its bases. This concept is analogous in linear algebra where the rank of a vector space V is defined as the size of its basis. For example, rank($\mathbb{R}^3$)=3, where $\beta = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$.

[1] Taken from *Introduction to Graph Theory* by Robin J. Wilson

3. Other Definitions of the Matroid

In order to consider another equivalent definition of the matroid, we must define some important terms. A subset $S \subseteq E$ is **independent** if S is contained in some base of the matroid M. The most obvious example of this is the cycle matroid, in which every independent subset contains no cycles.

Definition 2. *A **matroid** M consists of a non-empty finite set E and a non-empty collection I of subsets of E called **independent sets** satisfying the following properties:*

- I(i) *any subset of an independent set is independent;*
- I(ii) *if I and J are independent sets with $|J| > |I|$, then there is an element e, contained in J but not in I, such that $I \cup \{e\}$ is independent.*

We can also define the matroid $M = (E, I)$ in terms of its rank function, where $r(A)$ is the size of the largest independent set contained in A for $A \subset E$. We state the definition here[2]:

Let $E = \{e_1, e_2, e_3, \dots, e_n\}$ be a given set of elements. Let A be an arbitrary subset of E. If the following three postulates are satisfied, we shall call this system a matroid.

- $\mathcal{R}$(i) The rank of the null subset is zero.
- $\mathcal{R}$(ii) For any subset A and any element $e \notin A$,

$$r(A + e) = r(A) + k, \qquad (k = 0 \text{ or } 1).$$

- $\mathcal{R}$(iii) For any subset N and elements e_1, e_2 not in A, if $r(A + e_1) = r(A + e_2) = r(A)$, then $r(A + e_1 + e_2) = r(A)$.

For comparison, Wilson gives a slightly modified and arguably clearer version of what Whitney's definition of the matroid in terms of a rank function says:

Theorem 1. *A matroid consists of a non-empty finite set E and an integer valued function r defined on the set of subsets of E, satisfying:*

- r(i) $0 \leq r(A) \leq |A|$, *for each subset A of E;*
- r(ii) *if $A \subseteq B \subseteq E$, then $r(A) \leq r(B)$;*
- r(iii) *for any $A, B \subseteq E$, $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.*

The proof of the equivalence of this definition to the one in terms of conditions I(i) and I(ii) is given by Wilson.

Whitney also make the interesting but perhaps trivial point that any subset of a matroid is a matroid. In other words, if we have a matroid M_1 on a set E, we can define a new matroid M_2 on a set A where $A \subset E$.

More specifically, if M is a matroid defined on a set E, and if A is a subset of E, then we define the **restriction** of M to A, written $M \times A$, to be the matroid whose cycles are those cycles of M that are contained in A.

In addition, the **contraction**, written $M\ .\ A$, is the matroid whose cycles are the minimal members of the collection $\{C_i \cap A\}$, where C_i is a cycle of M. When we discuss the dual of a matroid, a simpler definition can be related. Finally, a matroid obtained through successive contraction and restrictions of M is called a **minor** of M. Roughly speaking, these terms correspond to the deletion and contraction of edges in a graph.

[2] *On The Abstract Properties of Linear Dependence* by Hassler Whitney

Theorem 2. *If M is a matroid on a set E and $A \subseteq B \subseteq E$, then $(M \times B) \times A = M \times A$.*

Proof. Consider an arbitrary cycle $C_i \subset A$. Clearly it is also true that $C_i \subset B$. It follows that no cycles of A are omitted when M is restricted to B and therefore the theorem is true.

■

Theorem 3. *If M is a matroid on a set E and $A \subseteq B \subseteq E$, then $(M \ . \ B) \ . \ A = M \ . \ A$.*

Proof. The cycles C_{BAi} of $(M \ . \ B).A$ are the minimal members of the collection $\{C_{Bi} \cap A\}$ where C_{Bi} is a cycle of $M.B$. Furthermore, C_{Bi} is itself an arbitrary minimal member of the collection $\{C_{Mi} \cap B\}$ where C_{Mi} is a cycle of M.

Therefore all cycles C_{BAi} of $(M \ . \ B) \ . \ A$ satisfy the following:

$$\begin{aligned} C_{BAi} &\in \min\{\min\{C_{Mi} \cap B\} \cap A\} \\ &\in \min\{C_{Mi} \cap B \cap A\} \\ &\in \min\{C_{Mi} \cap A\} \qquad \text{Since } A \subset B \end{aligned}$$

Since every cycle C_{BAi} of $(M \ . \ B) \ . \ A$ is from the same collection as each cycle C_{Ai} of $M \ . \ A$, the theorem is true.

■

4. Matroids In Terms of The Cycle

A matroid can also be defined in terms of its cycles. By definition a **cycle** is a minimal dependent set of a matroid $M(E, I)$ defined in terms of its independent sets. Using this idea, we will prove that a matroid can be defined as follows:

Theorem 4. *A **matroid** consists of a non-empty finite set E, and a collection $\mathcal{C}$ of non-empty subsets of E called **cycles** satisfying the following properties:*[3]

$\mathcal{C}$(i) *no cycle properly contains another cycle;*
$\mathcal{C}$(ii) *if C_1 and C_2 are two distinct cycles each containing an element e, then there exists a cycle $C_3 \subseteq C_1 \cup C_2 - \{e\}$.*

Proof. $(\Rightarrow)$ Let $M = (E, I)$ be a matroid defined in terms of its independent sets. To prove $\mathcal{C}$(i), suppose that there exist cycles C_1 and C_2, where $C_1 \neq C_2$, such that $C_1 \subset C_2$. This implies that C_2 is not a minimal dependent set since we can remove at least one element e and still have that $C_2 - \{e\}$ is dependent.

To prove $\mathcal{C}$(ii), suppose that $C_1 \cup C_2 - \{e\}$ does not contain a cycle. This implies that $C_1 \cup C_2 - \{e\}$ is independent, and likewise that $C_1 \cup C_2$ is a minimal dependent set (i.e. it is a cycle). However, this contradicts $\mathcal{C}$(i) since $C_1 \cup C_2$ properly contains two distinct cycles, namely C_1 and C_2.

$(\Leftarrow)$Now suppose we have a matroid $M(E, \mathcal{C})$ defined by its cycles. To prove I(i), consider an arbitrary cycle C_1 and remove an element e_1 from it. It follows that $C_1 - \{e_1\}$ is independent. If we then remove any other element $e_i \in C_1 - \{e_1\}$, the set must still be independent otherwise we would have that C_1 properly contains another cycle, contradicting $\mathcal{C}$(i).

[3] *Introduction to Graph Theory* by Robin J. Wilson

To check I(ii), let I_1 and I_2 be independent sets of M with $|I_1| > |I_2|$. If $I_2 \subset I_1$, then clearly there exists an element $e \in I_1 - I_2$ such that $I_2 \cup \{e\}$ is independent. Otherwise, let $I_2 - I_1 = \{x_1, x_2, x_3, \ldots, x_k\}$ where $k \leq |I_2|$. Also let $I_1 - I_2 = \{y_1, y_2, y_3, \ldots, y_j\}$. Note that $j > k$. To see this, suppose that $|I_1| = a$, that $|I_2| = b$ where $a > b$, and that $|I_1 \cap I_2| = c$. Then $|I_2 - I_1| = b - c = k$ and $|I_1 - I_2| = a - c = j$. Since $a > b$, we have that $j > k$.

Now suppose that $I_2 \cup \{y_m\}$ is dependent $\forall m \leq j$. This implies that each set $I_2 \cup \{y_m\}$ contains a cycle, and furthermore, this cycle necessarily contains y_m. If not, we would have that I_2 is not independent. So, we now have j distinct cycles and C_m is the cycle contained in $I_2 \cup \{y_m\}$. We will now show by induction on the number of elements i contained in $I_2 - I_1$, $i \leq k$, that there are at least $j - i$ cycles in $I_1 \cup I_2$ containing none of $x_1, x_2, \ldots, x_i$.

For the base case $i = 1$, if one of the cycles $C_p \subset I_2 \cup \{y_p\} \subset I_1 \cup I_2$ does not contain x_1, we have that $C_p \subset I_1$, which contradicts the fact that I_1 is independent. If all cycles $C_1, C_2, \ldots, C_j \subset I_1 \cup I_2$ contain the point x_1. Then pick two of them, C_1 and C_j for example. By $\mathcal{C}$(ii), there exists a cycle $C_1' \subset C_1 \cup C_j - \{x_1\}$. Now create $j - 2$ additional cycles by pairing C_j with every other cycle in the sequence and applying $\mathcal{C}$(ii). Now delete C_j from the sequence and replace each C_m with C_m'. We now have a sequence of $j - 1$ cycles $C_1', C_2', C_3', \ldots, C_{j-1}'$, none of which contains x_1.

Now suppose that for $i = s$ where $s \leq k - 1$, we have at least $j - s$ cycles contained in $I_1 \cup I_2$, and none of them contain an element from $x_1, x_2, x_3, \ldots, x_s$. Consider the case $i = s+1$. If none of the $j-s$ cycles $C_m \subset I_2 \cup \{y_m\}$ contain x_{s+1}, we are done. Suppose that x_{s+1} is contained in n of these cycles, $C_1, C_2, \ldots, C_n$. By $\mathcal{C}$(ii) for $d = 1, 2, \ldots, n-1$, we can find a cycle C_d' contained in $C_j \cup C_n$ but not containing x_{s+1}. Replacing C_d by C_d' for each $d = 1, 2, 3, \ldots, n-1$ and deleting C_n completes the induction step.

We have now shown that for $i = k$, there are at least $j - k$ cycles contained in $I_1 \cup I_2$ that contain no point of $I_2 - I_1$. In other words, there are $j - k$ cycles properly contained in I_1. Again, this contradicts the independence of I_1.

■

5. Types of Matroids

Two very important and common matroids are the the vector matroid and cycle matroid. If our set E is a finite set of vectors from a vector space V, then E spans some subspace contained in V. Moreover, we define the **vector matroid** on E by taking its bases as all linearly independent subsets $S \subseteq E$ such that $\text{span}(S) = \text{span}(E)$.

Example 1. *Find a graph corresponding to the cycle matroid on n edges with bases* $\{1, 2, 3, \ldots, n-1\}, \{2, 3, 4, \ldots, n\}, \{3, 4, 5, \ldots, n, 1\}, \ldots, \{n, 1, 2, 3, \ldots, n-2\}$.

Note that all of the matroid's bases have $n-1$ elements. By definition, a matroid is ***k*-uniform** on E, if its bases are those subsets of E with exactly k elements. Thus the matroid in this example is $n-1$ uniform.

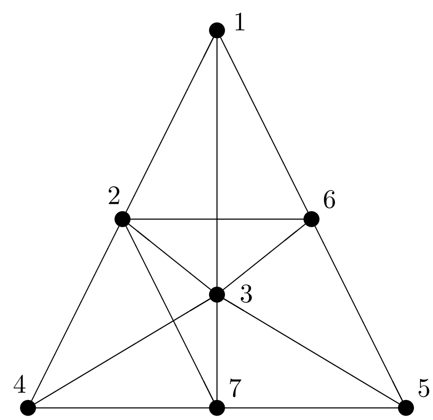
Example 2. *Find a graph that corresponds to a cycle matroid M on n edges in which only 1 basis exists: the basis $\beta = \{1, 2, 4, 5, 7, 8, \ldots, n\}$. β contains no edge labelled with a multiple of 3. Now find the dual M^* and construct a graph of it.*

Example 3. *Find an upper bound for the total number of possible matroids on a set of n elements*

Consider that the total number of subsets of a set of n elements is 2^n. Moreover, if we treat each of these subsets as members of the collection of independent sets of a matroid, then 2^{2^n} is the total of ways of selecting its independent sets. Thus, there are at most 2^{2^n} different matroids on a set of n elements. It turns out that this is indeed an overestimate of the actual numbers.

6. The Fano Matroid and More Terminology

The Fano Matroid is a matroid defined on the set $E = \{1, 2, 3, 4, 5, 6, 7\}$, whose bases are all the triples of E except those determined by the Steiner Triple System[4], that is, $\{1, 2, 4\}$, $\{2, 3, 5\}$, $\{3, 4, 6\}$, $\{4, 5, 7\}$, $\{5, 6, 1\}$, $\{6, 7, 2\}$ and $\{7, 1, 3\}$. The Fano Matroid can be represented geometrically below:



Wilson states that the Fano Matroid can be shown to be binary and Eulerian, but not graphic, cographic, transversal, or regular. Let us provide some of these tedious definitions below:

Note that the **cycle matroid** is denoted by $M(G)$. The rank of the cycle matroid of a graph G is defined by the cutset rank ξ. Remember that the cutset rank is the number of edges in a spanning forest of G, is denoted $\xi(G)$, and equals $n - k$, where n is the number of vertices and k is the number of components. Before we define cographic, note that a matroid M is **graphic** if there exists a graph G such that M is isomorphic to $M(G)$.

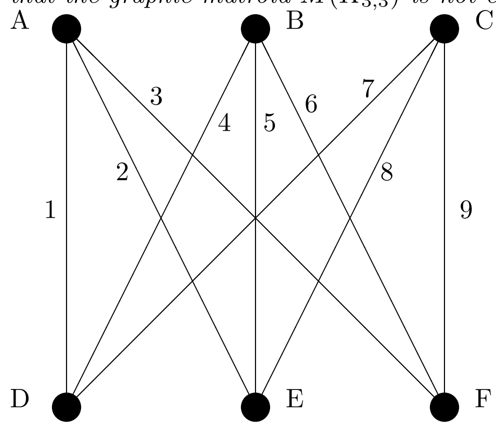
An **isomorphism** for matroids is defined as follows: A matroid M_1 is isomorphic to a matroid M_2 if there is a bijection or 1-1 correspondence between their underlying sets E_1 and E_2 that preserves independence. It is important to note that when looking at cycle matroids, we can have an isomorphism even though the two graphs don't have the same numbers of components, vertices, or degrees. However, matroid isomorphism does preserve cycles, cutsets, and of course the number of edges.

Graphically speaking, we can also make use of the **cutset matroid** which takes the cutsets of a graph G as the cycles of the corresponding matroid. This defines a matroid that we call the cutset matroid of G, denoted $M^*(G)$. Now, we call a matroid M **cographic** if there exists a graph G such that M is isomorphic to

[4]See http://mathworld.wolfram.com/SteinerTripleSystem.html for more information

$M^*(G)$. Note the analogy between graphic and cographic matroids. Are all graphic matroids also cographic, and vice versa? It turns our that the graphic matroids $M(K_5)$ and $M(K_{3,3})$ are not cographic. An interesting fact since these two graphs are the building blocks of non-planar graphs in the Euclidean plane. Conveniently, we define a matroid to be **planar** if it is both graphic and cographic.

Example 4. *Show that the graphic matroid $M(K_{3,3})$ is not cographic.*



Consider that the only cycle lengths of $K_{3,3}$ are 4 and 6. This is easy to see since a spanning tree of $K_{3,3}$ has exactly 5 edges so the maximum cycle length is 6. Moreover, the graph is bipartite so only even cycle lengths are possible. Thus, if there does exist a graph G such that $M^*(G)$ is isomorphic to $M(K_{3,3})$, then all the cutsets of G have either 4 or 6 edges. G must have a total of 9 edges so suppose that G has 5 vertices. It follows that G has at least $\frac{5\cdot4}{2} = 10$ edges. This obviously doesn't work. Suppose G has 4 vertices. In this case, we have a minimum of $\frac{4\cdot4}{2} = 8$ edges. If we allow one vertex to have degree 6, we get $\frac{3\cdot4+6}{2} = 9$ edges. Thus, G must have 4 vertices with degree sequence $(4, 4, 4, 6)$.

Now, if we remove any 6-cycle of $M^*(G)$ and the corresponding cutset of G, $M^*(G)$ will have no cycles left and will be disconnected. Likewise, the sum of the vertex degrees of G is now 6. Since there are 4 vertices, at least 1 of them has degree 2, which means that a cutset of size 2 remains in G. This means that $M^*(G)$ must have a remaining cycle of length 2. This is the desired contradiction.

Similar to our more common definition of bipartite, a **bipartite matroid** is a matroid in which every cycle has an even number of elements. A matroid is **Eulerian** if its underlying set E can be written as a union of disjoint cycles.

Theorem 5. *The cutsets of a graph G satisfy conditions $\mathcal{C}$(i) and $\mathcal{C}$(ii).*

Proof. Remember that a cutset is defined as a disconnecting set and furthermore, no proper subset of a cutset is a cutset. In this way, a cutset is minimized so $\mathcal{C}$(i) is automatically satisfied. For $\mathcal{C}$(ii), suppose that we have 2 cutsets S_1 and S_2 where there exists some element e such that $e \in S_1 \cap S_2$. Now suppose that $S_1 \cup S_2 - \{e\}$ contains no cutset. However, this implies that $S_1 \cup S_2$ must be a cutset itself, contradicting $\mathcal{C}$(i). ∎

Given a matroid M on an underlying set E, M is said to be **representable over a field** F if there exist a vector space V over F and a map $\phi : E \to V$, such that a subset A of E is independent in M iff ϕ is 1-1 on A and $\phi(A)$ is linearly independent in V. This equates to saying that M is isomorphic to some vector matroid in some vector space, if we ignore loops and parallel elements. A **binary matroid** is a matroid representable over the field of integers modulo 2. The book states that for any graph G, the cycle matroid of G is always a binary matroid. Now, a **regular matroid** is one that is representable over any field[5]. The idea of representable is a tough concept to grasp so let us consider an example.

Example 5. *Show that the Fano Matroid is binary.*

Let us assign each element of $E = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7\}$ a vector in $\mathbb{N}_2^7$. Remember the cycles of F are:

$$\{f_1, f_2, f_4\}\ \{f_2, f_3, f_5\}\ \{f_3, f_4, f_6\}\ \{f_4, f_5, f_7\}\ \{f_5, f_6, f_1\}\ \{f_6, f_7, f_2\}\ \{f_7, f_1, f_3\}$$

We want to eventually assign each element of E to a vector consisting of 7 entries of only 0's and 1's. The trusty guess and check method seemed the to be the easiest way to solve this problem. Fortunately, the answer is attainable this way. Assign each element of E in the following manner. Notice that no two vectors have the same number of zeros.

$$\begin{aligned}
f_1 &= (0,0,0,1,0,0,0)\\
f_2 &= (0,0,1,1,1,0,0)\\
f_3 &= (1,1,1,0,1,1,1)\\
f_4 &= (0,0,1,0,1,0,0)\\
f_5 &= (1,1,0,1,0,1,1)\\
f_6 &= (1,1,0,0,0,1,1)\\
f_7 &= (1,1,1,1,1,1,1)
\end{aligned}$$

It turns out that there is more than one way to assign binary vectors to each element of F. Tutte[6] gave the following representative matrix:

$$\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 1 & 1\\
0 & 1 & 0 & 1 & 1 & 0 & 1\\
0 & 0 & 1 & 0 & 1 & 1 & 1
\end{pmatrix}$$

Specifically let:

$$\begin{aligned}
f_1 &= (1,0,0)\\
f_2 &= (0,1,0)\\
f_3 &= (0,0,1)\\
f_4 &= (1,1,0)\\
f_5 &= (0,1,1)\\
f_6 &= (1,0,1)\\
f_7 &= (1,1,1)
\end{aligned}$$

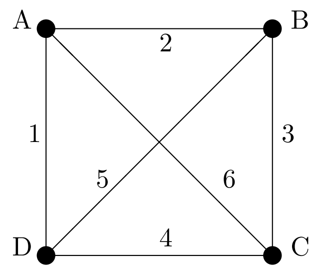
[5] *Introduction to Graph Theory* by Robin J. Wilson
[6] *Graph Theory As I Have Known It* by W.T. Tutte

Example 6. *Show that the Fano Matroid is Eulerian.*

Let $C_1 = \{f_2, f_3, f_4, f_7\}$. Note that C_1 is a minimally dependent set and hence a cycle as it contains a base of F plus one other element. Now, let $C_2 = \{f_1, f_5, f_6\}$. C_2 is a cycle by definition. Since $C_1 \cup C_2 = E$ and $C_1 \cap C_2 = \emptyset$, F is Eulerian.

■

Example 7. *Let us consider the cycle matroid $M(K_4)$ where E can be thought of as the set of edges. Show that this matroid is representable over some field F.*



Note that $E = \{1, 2, 3, 4, 5, 6\}$ and our cycles are $\{1, 2, 3, 4\}$, $\{1, 2, 5\}$, $\{2, 3, 6\}$, $\{3, 4, 5\}$ and $\{1, 4, 6\}$. The maximal independent sets are $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 2, 6\}$, $\{2, 3, 5\}$, $\{1, 4, 5\}$, $\{3, 4, 6\}$, $\{1, 3, 4\}$ and $\{2, 3, 4\}$. Now we just need to figure out vectors to assign to each element of E such that independence and dependence are preserved among subsets. To make things simpler, let us show that $M(K_4)$ is a binary matroid.

The book gives a nice technique for showing that a cycle matroid is also a binary matroid. We'll associate each edge of G (i.e. each element of E) with the corresponding column from its incidence matrix. Here is the incidence matrix for K_4.

$$\mathbf{Q} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Looking at the labelled K_4, notice that the edge set $\{1, 2, 3\}$ is independent. Moreover the vectors from columns 1, 2 and 3 of Q are linearly independent. One could test all possible subset mappings and see that mapping of each edge to a vector in $\mathbb{N}_2^n$ where n is the number of vertices, preserves the independence relation for all subsets $A \subset E$. Specifically, if a set of edges forms a cycle, than the sum of the corresponding vectors is 0 (mod 2).

Theorem 6. *If a matroid M is graphic, then it is binary.*

Proof. Consider that if M is graphic, then there exists a graph G such that M is isomorphic to $M(G)$. Now we assign each edge of G its corresponding column from the incidence matrix of G. Note that this is a vector on the field of integers modulo 2.

Now consider any cycle C of G. Each edge of the cycle is connected to two vertices, one at each end. Also note that the vector associated with each edge has only two 1's in it, for the same reason.

Therefore, the final vector sum of the cycle is 0 (mod 2) at each vertex. Each edge that is connected to a given vertex in the cycle contributes 1 to this sum. Thus, our mapping preserves the dependence of the cycles of G.

If we consider a subset S of E that isn't a cycle, it follows that the subgraph containing each element of S and all incident vertices has at least one end vertex. Let's call this vertex v_i. Furthermore, position i in the vector sum is the number of elements in S that are incident to v_i. Since there is only one such element, the vector sum is non-zero.

■

Example 8. *Construct an Eulerian vector matroid M on a finite set of vectors E that is a subspace of $\mathbb{R}^3$. Remember that a cycle of a vector matroid is a minimal linearly dependent set of vectors.*

The largest cycle we could possibly have would be 4 elements since we are dealing with a 3 dimensional subspace. The simplest case is to construct two cycles where one only occupies the first component of the space and the other cycle occupies the two remaining components. This is analogous to having a cycle restricted to x and another cycle restricted to y and z. Thus, let $C_1 = \{(1,0,0),(3,0,0)\}$ and $C_2 = \{(0,1,0),(0,0,1),(0,1,1)\}$. We want $C_1 \cup C_2 = E$ so let $E = \{(1,0,0),(3,0,0),(0,1,0),(0,0,1),(0,1,1)\}$. From this, it seems relatively easy to construct Eulerian vector matroids on any dimension. However, testing an arbitrary matroid for being Eulerian may prove difficult.

7. The Greedy Algorithm Revisited

Previously, we used the greedy algorithm on weighted graphs. Specifically, we considered the example of a railroad that needs to reach a given network of cities using a minimal amount of track. This essentially breaks down to finding a spanning tree with least possible total weight. We start with the smallest weighted edge and add it to our tree. We then continue adding edges to our tree making sure to pick the one with minimum cost at each step. We stop when we have a spanning tree (i.e. adding any more edges creates a cycle). This process can be described quite nicely in the context of matroids since we don't actually have to look at a specific graph.

Ken Bogart gives another example to consider[7]: suppose we have a school district trying to fill a number of job positions. For each position, there is a set of qualified candidates. We can visualize this situation as a bipartite graph where V_1 is the set of candidates and V_2 is the set of job positions. Furthermore, there is an edge drawn from candidate a to job position b if a is qualified to fill b.

However, there may very well be a financial factor involved here. Consider that each candidate has a minimum salary he or she is willing to accept. We can represent this with a cost function $c : E \to \mathbb{N}$ where E is the set of edges in the graph. From the school district's perspective, we want to fill as many positions as possible with the least total cost. The greedy algorithm tells us to build a maximum-sized independent set by continually adding the cheapest element possible to the current set. This process stops when we can no longer find candidates to add.

How do we know that there isn't some other independent set that is larger than the one we've created? Consider condition I(ii), which states: If I and J are

[7] *Introductory Combinatorics* by Kenneth P. Bogart

independent sets where $|I| < |J|$, then there is an element $e \in J$ such that $I \cup \{e\}$ is independent.

Here is the greedy algorithm, clearly and simply stated:

Step 1. Let $I = \emptyset$.
Step 2. From the set E, pick an element x with minimum cost.
Step 3. If $I \cup \{x\}$ is independent, replace I by $I \cup \{x\}$.
Step 4. Delete x from E.
Step 5. If E is not empty, return to Step 2.

Theorem 7. *Suppose we are given a matroid M on a set E with a cost function $c : E \to \mathbb{N}$. The greedy algorithm selects a basis of minimum cost. In other words, it gives us a basis B such that $c(B) \leq c(B')$ for all bases $B' \neq B$.*

From condition I(ii), the greedy algorithm will be able to continue adding elements to the A (the set in consideration) until A becomes a maximum-sized independent set. Thus we have selected a basis. We call this basis B and suppose that B' is another basis. List the elements of each basis as follows: $B = \{b_1, b_2, b_3, \ldots, b_n\}$ and $B' = \{a_1, a_2, a_3, \ldots, a_n\}$. In addition, the elements are listed in order of increasing cost so that if $i < j$, $c(b_i) \leq c(b_j)$ and similarly, $c(a_i) \leq c(a_j)$.

By Step 2 of the greedy algorithm, $c(b_1) \leq c(a_1)$. If $c(b_i) \leq c(a_i)$ $\forall i$, then $c(B) \leq c(B')$. So let us assume that for some i, but for no previous i, $c(a_i) < c(b_i)$. Clearly, the two sets $\{a_1, a_2, a_3, \ldots, a_i\}$ and $\{b_1, b_2, b_3, \ldots, b_{i-1}\}$ are both independent. Then by I(ii), there exists an a_j with $j \leq i$ such that $\{b_1, b_2, b_3, \ldots, b_{i-1}, a_j\}$ is independent.

However, since $c(a_j) \leq c(a_i) < c(b_i)$, a_j would have been chosen by the greedy algorithm. Therefore, $c(b_i) \leq c(a_i)$ and so B is a minimum-cost basis.

■

8. Dual Matroids

It turns out that the duality of matroids is a much nicer and more generalized way of defining the dual concept. In fact, the definition encountered before for the abstract dual of a planar graph is a direct consequence of the definition of a matroid dual.

Earlier, we found the cutset matroid $M^*(G)$ on the set of edges of G by taking as cycles of $M^*(G)$ the cutsets of G. It is conveniently the case that $M^*(G)$ is the dual of $M(G)$.

Definition 3. *If M is a matroid on a set E, defined in terms of its rank function r, we specify the **dual matroid** M^* of M as the matroid on E whose rank function $r*$ is given by:*

$$r^*(A) = |A| + r(E - A) - r(E), \textit{ for } A \subseteq E$$

Theorem 8. *$M^* = (E, r^*)$ is a matroid on E.*

The proof is given by Wilson.

As this is a rather convoluted definition, it is nice that the bases of M^* are defined in terms of the bases of M.

Theorem 9. *The bases of M^* are precisely the complements of the bases of M.*

Now we will define some important terms that apply to the matroid dual. The elements of a matroid M form a **cocycle** of M if they form a cycle of M^*. It turns out that the cocycles of the cycle matroid of a graph G are the cutsets of G. In addition, a **cobase** is a base of $M*$. There are also the similarly defined terms **corank** and **co-independent set**. Before, we said that a matroid M is cographic if there exists a graph G such that $M*(G)$ (the cutset matroid of G) is isomorphic to M. An equivalent definition is as follows: a matroid M is **cographic** if and only if its dual $M*$ is graphic.

Example 9. *Find the dual of the Fano Matroid. Is there a graphical representation of this perhaps similar to that of the F? Is F^* binary?*

Theorem 10. *Every cocycle of a matroid intersects every base. Likewise, every cycle of a matroid intersects every cobase.*

The proof of this is contained in the class text.

Theorem 11. *Let M be a binary matroid on a set E. If M is an Eulerian matroid, then M^* is bipartite.*

Theorem 12. *If M is a graphic Eulerian matroid on a set E, then M^* is bipartite.*

Proof. Since M is graphic, there exists a graph G such that $M(G)$ is isomorphic to M. The edge set $E(G)$ can thus be written as a union of disjoint cycles. By Corollary 6.3, G is an Eulerian graph. We can assume G to be connected because if not, we could just piece it together by its cycles connecting them at single vertices. Connecting two cycles at a single vertex does not increase the number of cycles nor does it affect any previously existing cycles.

Since G is Eulerian, every vertex has even degree. Therefore, every cutset of G has an even number of edges. If we suppose otherwise that there is a cutset with an odd number of edges, then we can easily construct a contradiction that G is not Eulerian. With this established, each cycle of G^* has even length. Therefore, G^* is bipartite. By Theorem 32.6, $M(G^*)$ is isomorphic to $(M(G))^*$. Since $M(G)$ is isomorphic to M, we have that $M(G^*)$ must also be isomorphic to M^*. Hence M^* is bipartite.

■

We end with an important theorem in matroid theory proven by Tutte. The proof is too difficult to be explained simply, but it has important connections to the planarity of graphs.

Theorem 13. *(Tutte). A matroid M is graphic if and only if it is binary and contains no minor isomorphic to $M(K_5)$, $M(K_{3,3})$, F or $F*$.*

9. Conclusion

The examples and problems presented have been intended to help one to better understand the idea of a matroid. In a manner of speaking, the matroid relates numerous fields of mathematics, including graph theory and linear algebra, and links them with a supreme generalization of independence. So perhaps understanding the matroid will help one to better understand mathematics as a whole. Nonetheless, matroid theory is *huge*. There are so many different ways of using them in the context of a research project. Ultimately, this paper was designed to pose some interesting problems and exercises in matroid theory that may help another student wishing to learn something about it.