Matroids

The purpose of this paper is to explore the history, documentation, research, and theory behind the Matroid.

The original concept of the Matroid was introduced by Hassler Whitney an instructor of mathematics at Harvard for the years 1930-31, 1933-35. Graph theory and linear algebra play a major role in the theory and study of matroids. Once the matroid was developed it became an integral part of combinatorics and representation theory. Combinatorics is the study of discrete objects in mathematics and representation theory is a branch of mathematics that studies abstract algebraic structures by representing their elements as linear transformations of vector spaces. (1)

With the creation of a matroid Whitney captured the basic properties of dependence that are part of graphs and matrices. Almost simultaneously, Garrett Birkhoff, an American mathematician, showed that a matroid can be interpreted as a geometric lattice. Saunders Mac Lane showed that matroids have a geometric representation in terms of points, lines, planes, and dimension 3 spaces etc. The discovery leads to Mac Lane’s connection of matroids and classical projective geometry. With a matroid being represented by points and lines Mac Lane discovered the connection between matroids and the Desargues configuration and Pappus configuration.

There are multiple definitions of a Matroid that all define it in slightly different ways. Let’s take three of these definitions and compare them.

**Definition 1** - A matroid is a finite set M of elements together with a family of subsets of M, called independent sets, such that
1. The empty set is independent,
2. Every subset of an independent set is independent,
3. For every subset A of M, all maximal independent sets contained in A have the same number of elements. (2)

Definition 1 is saying that we have a finite Matroid M and in M there is a subset of elements that follows the axioms one, two, and three. Axiom one is saying that the empty set is independent. Another way of putting it is there has to be at least one independent element in M. Axiom two is also called the heredity property, but for every independent set all subsets of the independent set are themselves independent. Axiom 3 is referring to the definition of basis
and states that if \(A\) is a subset of \(M\) all maximally independent subsets of \(A\) have the same number of elements which is the rank of the matroid.

**Definition 2** - A matroid consists of a finite set \(M\) of elements together with a family \(E = \{C_1, C_2, \ldots\}\) of nonempty subsets of \(M\), called circuits, which satisfy the axioms

1. No proper subset of a circuit is a circuit,
2. If \(x \in C_1 \cap C_2\) and \(C_1 \neq C_2\), then \(C_1 \cup C_2 - \{x\}\) contains a circuit.

A circuit is a dependent set whose subsets are all independent. So a circuit is the minimally dependent set of \(E\).

Definition 2 is saying we have a matroid \(M\) and \(M\) is made up of a family of elements called circuits. Axiom one is saying that no proper subset of a dependent set is a dependent set. If the subset was not proper then you could have the whole set as the subset which contradicts the axiom because then the subset would be a circuit. Axiom 2 is saying we have an element \(x\) in the intersection of circuits one and two where circuits one and two are not equal. If this is the case then the union of the two circuits minus the element \(x\) contains a circuit.

**Definition 3** - The closure \(\text{cl}(A)\) of a subset \(A\) of \(E\) in a finitary matroid \(M\) is defined to be \(A\) together with every point \(x\) in \(E \setminus A\), such that there is a circuit \(C\) containing \(x\) and contained in the union of \(A\) and \(\{x\}\). This defines the closure operator, from \(P(E)\) to \(P(E)\), where \(P\) denotes the power set.

We can give axioms for the closure operator, thereby defining a matroid in terms of its closure. First, let \(E\) be a finite set. A function \(\text{cl}: P(E) \to P(E)\) is a matroid closure if it satisfies the following conditions, for all elements \(a, b\) of \(E\) and all subsets \(Y, Z\) of \(E\):

1. \(\text{cl}\) is an abstract closure operator.
2. MacLane–Steinitz exchange property: If \(a\) is in \(\text{cl}(A)\setminus\text{cl}(Y)\), then \(b\) is in \(\text{cl}(A)\).
3. If \(E\) is infinite, we add the property of finite character: If \(a\) is in \(\text{cl}(Y)\), then there is a finite subset \(X\) of \(Y\) such that \(a\) is in \(\text{cl}(X)\).

What definition 3 is saying is if we take the function of closure to be the mapping of the power set of \(E\) to the power set of \(E\) with the three properties defines a matroid by its closure. Any closure function on \(E\) with this property determines a matroid on \(E\). The closure of a subset \(A\) of \(E\) in a finitary matroid \(M\) with any point \(x\) in \(E\) and not in \(A\) creates a circuit containing \(A\) and \(\{x\}\), which is usually written as \(A \cap x\).

The differences between the definitions are almost trivial. One could form each of the definitions from the other given the knowledge base of closure, circuits, and matroids, but these three definitions clearly define the relationship between the properties of closure, circuits, and matroids.
Generally a matroid is a finite set with the concept from linear algebra of linear dependence and independence of subsets of the matroid. Using this general concept of a matroid let’s take a look at a couple of examples of a matroid.

Example 1:
Let E be a finite set of vectors from a vector space, and let A be the set of linearly independent subsets of vectors of E. Then M = (E, A) is a matroid. The three axioms given in definition 1 of a matroid apply as follows:
1. By taking independent to mean linearly independent in the vector space, the empty set is independent.
2. If we have a subset of independent vectors then obviously any subset of those is going to be independent.
3. If we take a subset A of the vector space M then the maximally independent sets contained in A have the same number of elements.

Example 2:
Let M = (E, A) and let I be the matrix:

\[
\begin{bmatrix}
1 & 2 & 3 & 4 & 5 \\
1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1
\end{bmatrix}
\]

over the field R of real numbers. Let M Then E = \{1, 2, 3, 4, 5\} and A = {\Ø, \{1\}, \{2\}, \{4\}, \{5\}, \{1, 2\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{4, 5\}}. Thus the set of dependent sets of this matroid is:

\{\{3\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{3, 4\}, \{3, 5\}\} \cup \{ X \subseteq E : |X| \geq 3\}. (4)

In this example the circuits would be the minimally dependent sets:

\[ \mathcal{E}(M) = \{\{3\}, \{1, 4\}, \{2, 4, 5\}, \{1, 2, 5\}\} \]

The rank of a matroid is defined as the number of elements of all maximally independent sets of the matroid. In this example the maximally independent sets of A are: \{1, 2\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{4, 5\}. Thus the rank of the matroid is 2.

Lemma:
The set \( \mathcal{E} \) of circuits of a matroid has the following property: If \( C_1 \) and \( C_2 \) are distinct members of \( \mathcal{E} \) and \( e \in C_1 \cap C_2 \), then there is a member \( C_3 \) of \( \mathcal{E} \) such that \( C_3 \subseteq (C_1 \cup C_2) - e \).

Proof:
Assume that \( (C_1 \cup C_2) - e \) does not contain a circuit. Then \( (C_1 \cup C_2) - e \in A \), where A is the set of independent vectors. By the second axiom of the first definition, \( (C_2 - C_1) \) is non-empty, so we can choose an element f from this set. As \( C_2 \) is a minimal dependent set, \( C_2 - f \in A \). Now choose a subset B of \( (C_1 \cup C_2) \) which is maximal with the properties that it contains \( C_2 - f \) and is
independent. Evidently \( f \notin A \). Moreover, as \( C_1 \) is a circuit, some element \( g \) of \( C_1 \) is not in \( A \). As \( f \in C_2 - C_1 \), the elements \( f \) and \( g \) are distinct. Hence

\[
|A| \leq |(C_1 \cup C_2) - \{f, g\}| = |C_1 \cup C_2| - 2 < |(C_1 \cup C_2) - e|.
\]

Using the property of a matroid, if \( I_1 \) and \( I_2 \) are in \( A \) and \( |I_1| < |I_2| \), then there is an element \( e \) of \( I_2 - I_1 \) such that \( I_1 \cup e \in A \). Taking \( I_1 \) and \( I_2 \) to be \( A \) and \( (C_1 \cup C_2) - e \), respectively. The resulting independent set contradicts the maximality of \( A \). Therefore \( (C_1 \cup C_2) - e \) contains a circuit. (4)

Now let’s take a look at the structure of a matroid. An oriented matroid is called simple if it has no loops and no (distinct) parallel elements. A loop is not a circuit but a dependent element of the set and a parallel element are circuits of 2 elements. In figure 1 edge 5 (e5) is a loop and edge 6 (e6) and edge 7 e(7) are parallel elements.

Furthermore, a circuit is a minimal dependent set, while a basis is defined as a maximal independent set. (5) That is if \( E \) is an independent set of \( M \) and we add any element of \( M \) to \( E \) and \( E \) becomes dependent then it was a basis before we added the element. This leads to the fact that any two bases of a matroid have the same number of elements, which means that the number of elements of the base is the rank of the matroid.

Below is a figure of the Fano matroid and it is a projective plane of order two. This might be familiar to you because The Fano Plane is a projective plane of order two hence the name Fano Matroid. The Fano Matroid is not representable by any set of vectors in a real or complex vector space or in any vector space over a field whose characteristic differs from two, which is similar to the Fano Plane.
The Fano Matroid is of rank 3 and has a curve drawn through every 3-element circuit. Figure 2 originally appeared in Whitney’s Paper in 1935 describing his newly invented matroid. The duality of a matroid then follows since the matroid is similar in structure to the Fano Plane the duality of a matroid follows the same logic.

With the structure and properties of the matroid defined mathematicians have been applying the theory to combinatorics, representation theory, and other fields of study.

Works Cited