Matroids

Will Johnson

June 3, 2009

1 Introduction

One of the primary goals of pure mathematics is to identify common patterns that occur in disparate circumstances, and to create unifying abstractions which identify commonalities and provide a useful framework for further theorems. For example the pattern of an associative operation with inverses and an identity occurs frequently, and gives rise to the notion of an abstract group. On top of the basic axioms of a group, a vast theoretical framework can be built up, investigating the classification of groups, their internal structure, and the relationships and operations on groups.

Matroids similarly provide a useful linking abstraction. They were first discovered independently by Hassler Whitney [10] and B. L. van der Waerden in the mid 1930's [11]. Whitney had developed a notion of independence and rank in the context of graph theory, and noted similarities with the concepts of linear independence and dimension from linear algebra. By identifying the properties of abstract 'independence' which made these commonalities occur, he introduced the concept of a matroid, whose definition has proven immensely fruitful. Similarly, van der Waerden was interested in generalizing the notion of 'independence' from the examples of linear independence and algebraic independence. Shortly after the initial work by Whitney and van der Waerden, Birkhoff [2] noted that matroids were connected with a certain type of semimodular lattice that he had been studying. Thus, matroids provide a link between graph theory, linear algebra, transcendence theory, and semimodular lattices.

Several decades later, Jack Edmonds noted the importance of matroids for the field of combinatorial optimization. This connection is due to two fundamental breakthroughs. First of all, Edmonds and a number of other researchers discovered a new type of matroid arising from the combinatorial theory of transversals. Second, Rado and Edmonds noted that matroids were intrinsically connected with the notion of a greedy algorithm (more historical details are in [11] and [3]). These developments have made matroids a mainstay of the field of combinatorial optimization.

2 Two types of independence

At its heart, the concept of a matroid is tied to the notion of "independence." Whitney's initial definition in [10] was driven by formal similarities between the notion of linear independence and a sort of graph-theoretic independence[1]. Before defining a matroid, it is thus helpful to examine these concepts in the two domains which prompted Whitney to invent the matroid.

2.1 Linear Algebra

The concept of linear independence is well-known within linear algebra. Formally, a set of vectors I in a vector space $V \supseteq I$ is said to be *linearly dependent* if there are some $v_1, \ldots, v_m \in I$, and some scalars $a_1, \ldots, a_m \neq 0$, such that

$$a_1 v_1 + \cdots + a_m v_m = 0.$$

[1] Similarly, van der Waerden's independent invention of the matroid stemmed from an effort to unify the formal properties of algebraic and linear independence.

Otherwise, I is linearly independent. For the case of matroids, we will mainly deal with finite I.

Finite independent subsets of a vector space V satisfy the following properties:

(I1) Every subset of an independent set is independent.

(I2) If I_1 and I_2 are independent sets, with $|I_1| < |I_2|$, then $I_1 \cup \{x\}$ is independent for some $x \in I_2 \setminus I_1$.

(I2') If $S \subseteq V$ is finite (or if V is finite-dimensional), then the maximal independent subsets of S are all equal in size.

The common size in (I2') is simply the *rank* of S, which we'll denote as $\rho(S)$.

Connected to the notion of rank and independence is the notion of the span of a set. If $S \subseteq V$, then we say that $x \in V$ is in the *span* of S, if x is a linear combination of elements of S, i.e., there are some $v_1, \ldots, v_m \in S$ and some scalars $a_1, \ldots, a_m$, such that

$$x = a_1 v_1 + \cdots + a_m v_m.$$

This notion is intimately connected with independence and rank, by the following results:

- If $S \subseteq V$, then $x \in V$ is in the span of S iff $\rho(S) = \rho(S \cup \{x\})$.
- The rank of S is the size of the smallest subset of S whose span contains S.
- A set $I \subseteq V$ is independent iff, for each $x \in I$, x is not in the span of $I \setminus \{x\}$.
- If $I \subseteq V$ is independent, then x is in the span of I iff either $x \in I$ or $I \cup \{x\}$ is not independent.

In fact, all of these results generalize to matroids.

2.2 Graph Theory

These same results can be carried over to the world of graph theory, with an appropriate definition of "independence." For this setting, suppose we have a finite undirected graph G, not necessarily simple, with edge-set E and vertex-set V. We will focus on the edges in E, which will be analogous to the vectors in the previous example. The appropriate definition of "independence" is as follows: a set S of edges in E is *independent* if it contains no cycles, and *dependent* otherwise. In other words, a set of edges is independent if the induced graph is acyclic. Somewhat surprisingly, properties (I1), (I2), and (I2') carry over equally well to this setting:

(I1) Every subset of an acyclic set of edges is acyclic.

(I2) If I_1 and I_2 are two sets of edges, both acyclic, and $|I_2| > |I_1|$, then some edge $x \in I_2 \setminus I_1$ can be added to produce an acyclic set, i.e., $I_1 \cup \{x\}$ is acyclic.

(I2') If S is a subset of edges, then the maximal acyclic subsets of S are all equal in size.

The third property suggests that there should be some concept of the "rank" of a set of edges $S \subseteq E$. If we define $\rho(S)$ to be the size of a maximal acyclic subset of S, then it turns out that $\rho(S)$ simply counts the number of vertices minus the number of connected components in the subgraph $G' \subseteq G$ induced by S. This is due to the fact that a maximal acyclic subgraph of G' is just a spanning tree in each connected component of G', and the number of adges in a spanning tree is one less than the number of vertices.

There is also an analogous definition of "span" in the context of graph theory, as hinted at by the terminology "spanning tree." We say that an edge $e \in E$ is *spanned* by a set of edges S if there is some path in S which connects the two endpoints of e. Note that since G may not be a simple graph, e could be a self-loop, in which case the empty path connects the endpoints of e. Therefore, e is spanned by any set of edges. This is analogous to the case of the zero vector, which is a linear combination of any set, even the empty one.

As in the case of linear algebra, the notions of rank, span, and independence are intimately connected. Indeed, the same results carry over:

- If $S \subseteq E$, then $x \in E$ is in the span of S iff $\rho(S) = \rho(S \cup \{x\})$.
- The rank of S is the size of the smallest subset of S whose span contains S.
- A set $I \subseteq E$ is independent iff, for each $x \in I$, x is not in the span of $I \setminus \{x\}$.
- If $I \subseteq E$ is independent, then x is in the span of I iff either $x \in I$ or $I \cup \{x\}$ is independent.

It is an interesting exercise to run through these properties with the given definitions of rank, span, and independence, to verify that each holds.

3 Matroid Definitions

The similarities between the notions of independence, rank, and span in these two domains suggest a common definition. We first present the rather ad-hoc definition of a matroid in terms of independent sets, which draws upon properties (I1-2) above. However, a number of other equivalent definitions are possible, which will be introduced at the end of this section. All of the key definitions and results of this section are summarized in the appendix.

3.1 Independent Sets

Definition 1. *A* matroid *is a finite*[2] *set E with a non-empty collection $\mathcal{I}$ of subsets of E, called* independent sets*, such that*

(I1) Every subset of an independent set is independent.

(I2) If I_1 and I_2 are independent sets, and $|I_2| > |I_1|$, then for some $x \in I_2 \setminus I_1$, the set $I_1 \cup \{x\}$ is independent.

Note that modulo (I1), the requirement that $\mathcal{I}$ is nonempty is equivalent to the requirment that the empty set is independent.

Alternatively, we could have replaced axiom (I2) with (I2') from above. That is, we could have required the independent sets to satisfy the following:

(I1) Every subset of an independent set is independent.

(I2') If $S \subseteq E$, then the maximal independent subsets of S are all equal in size.

The equivalence of these axioms is easy to see. The direction (I2) $\Rightarrow$ (I2') follows by taking two maximal subsets of S, and applying (I2) if they differ in size. The direction (I2) $\Leftarrow$ (I2') follows by applying (I2') with $S = I_1 \cup I_2$. Since $|I_1| < |I_2|$, $|I_1|$ cannot be a maximal independent subset of S, so some element of S $I_1 = I_2 \setminus I_1$ can be added to I_1 to produce another independent set.

With this definition, we can define two sorts of matroids, one from linear algebra and one from graph theory. If V is a vector space over some field k, and E is a finite subset of V, then we can define a matroid M on E whose independent sets are those sets which are linearly-independent within V. This sort of matroid is called a "matric" [3], "vector" [7], or "representable" [11] matroid, and we speak of it as being "representable over k." The term "matric" generally refers to the case in which the vectors in E are the columns of a matrix, but any representable matroid can be converted easily enough to that form.

Similarly, if G is a graph with edges E and vertices V, then we define the "cycle" [7] or "circuit" [11] matroid of G, with base set E and independent sets exactly those $S \subseteq E$ for which S is acyclic. It can be shown that this also produces a matroid. Such matroids are also called "graphic" matroids, because they arise from graphs in the same way that matric matroids arise from matrices.

[2]The theory of matroids can be generalized to the infinite case, but some of the interesting and useful concepts, such as duality, seem to break down. In this paper, only finite matroids will be considered.

We can also define one more example of a very simple type of matroid, a *uniform matroid*. The uniform matroid of rank $k \geq 0$ on a set of size $n \geq k$, denoted $U_{k,n}$, is a matroid on a set E of size n, for which the independent sets are exactly those subsets $S \subseteq E$ which have $|S| \leq k$. The axioms given above are easy to verify in this case, and uniform matroids will provide a useful foil for the complexity of matric and graphic matroids.

At this point, it is not at all obvious that the given definition of a matroid is 'correct' or useful, or that it should provide meaningful definitions of "rank" and "span." However, it does...

3.2 Bases, Circuits, Rank, and other sundries

Assume we have a matroid M on a set E. We begin by defining some important types of sets of elements:

Definition 2. *In a matroid M on a set E,*

- *A set $S \subseteq E$ is* dependent *if and only if it is not independent.*
- *A set $B \subseteq E$ is a* basis *iff it is a maximal independent set.*
- *A set $C \subseteq E$ is a* circuit *iff it is a minimal dependent set.*

For the case of a representable matroid, a basis is a collection of vectors which is linearly independent and spans all the other vectors in the matroid. In other words, if our matroid came from a set of vectors E in a vector space V, then a basis in E is just a basis for the span of E. In the lucky case that E spanned all of V, then a basis is simply a set of vectors which is an actual basis of V, in the usual sense from linear algebra. The notion of a circuit is more obtuse in this setting, but it is can be seen that a set $C = \{v_1, \ldots, v_m\}$ is a circuit iff there are non-zero constants $a_1, \ldots, a_m \neq 0$, such that

$$a_1 v_1 + \cdots + a_m v_m = 0,$$

and the a_i are determined up to a multiplicative factor. This is a stronger condition than requiring that each element of C be spanned by the remainder, since this would still hold in the union of two circuits, and circuits cannot be subsets of other circuits.

For the case of graphic matroids, a set is dependent iff it contains a cycle, and so we see that a circuit is nothing but a simple cycle. This explains the term "circuit." However, the notion of a basis is more complex. If the underlying graph G is connected, then a maximal independent set is just a spanning tree. Otherwise, we must speak of a spanning forest, which consists of a spanning tree in each component of G. It is well-known in the field of graph theory[3] that the size of a spanning tree is one less than the number of vertices. Therefore, the size of a spanning forest of G will be the number of vertices in G minus the number of connected components. This establishes that all bases have the same size. For $S \subset E$, we can apply the same argument to the subgraph of G obtained by deleting the edges outside of S, and this establishes axiom (I2') above. So therefore graphic matroids actually are matroids.

For a uniform matroid $U_{k,n}$, a set will be dependent exactly when its size is greater than k. Consequently, a set is a basis if its size is exactly k, and a circuit if its size is exactly $k+1$. Note that in the case $k = n$, there are no sets of size $k+1$, and so there are no circuits in the matroid. This example demonstrates that circuits and dependent sets need not exist. On the other hand, independent sets always exist, by the definition of a matroid, and thus bases always exist in any matroid too.

With the given definitions of bases and circuits, we can already state a few interesting results:

(B1) No basis is contained in any other basis.

(B2) If B_1 and B_2 are distinct bases, then for every $x \in B_1 \setminus B_2$, there is some $y \in B_2 \setminus B_1$ such that $(B_1 \setminus \{x\}) \cup \{y\}$ is a basis.

[3]Or at least in the field of Computer Science. The fact that the number of edges in a tree is one less than the number of vertices is easy to prove by induction on the number of edges in the tree.

(B3) All bases have the same size.

(C1) No circuit is contained in any other circuit.

(C2) If C_1 and C_2 are two distinct circuits, and $x \in C_1 \cap C_2$, then $(C_1 \cup C_2) \setminus \{x\}$ contains some other circuit.

Properties (B1) and (C1) are obvious from the definitions. Property (B2), a so-called *basis exchange principle*, follows by applying (I2) to the sets $B_1 \setminus \{x\}$ and X_2, to show that $(B_1 \setminus \{x\}) \cup \{y\}$ is independent for some appropriate y, and using (B3) to show that it is a basis. (B3) itself follows from (I2') applied to the entire matroid. Property (C2)[4] is much less obvious, but will follow from the properties of the next definition.

Definition 3. *If M is a matroid on a set E, then the* rank *of a set of elements $S \subseteq E$, denoted $\rho(S)$, is defined to be the size of a maximal independent subset of S. The* rank *of the matroid M is defined to be the rank of all of E.*

Note that rank is well-defined by virtue of (I2'). Also, the maximal independent subsets of E are just the bases, so the rank of M is just the size of any basis. Finally, note that S is independent iff $\rho(S) = |S|$.

The notion of rank is relatively straightforward to understand in our three examples of matroids. For the case of a representable matroid, the rank of a set of elements is just the dimension of the subspace spanned by the corresponding set of vectors. If the vectors were the columns of a matrix, then the rank of a set of columns is just the rank of the corresponding submatrix, justifying the terminology. For the case of a graphic matroid, the rank of a set of edges S is equal to the number of vertices minus the number of connected components in the graph induced by S, as hinted at above. For the case of a uniform matroid $U_{k,n}$, the rank of a set S is either the size of S, or k, whichever is smaller. Note that the rank of the entire matroid is just k, hence the name, "uniform matroid of rank k..."

As in the case of circuits and bases, there are certain essential properties of rank worth noting:

(R1) For any set S, $0 \leq \rho(S) \leq |S|$.

(R2) If $S \subseteq T$, then $\rho(S) \leq \rho(T)$.

(R3) If $S, T \subseteq E$, then the following *semimodular inequality* holds:

$$\rho(S) + \rho(T) \geq \rho(S \cup T) + \rho(S \cap T).$$

The first property is obvious from the definition, and the second follows by noting that a maximal independent subset of S can be extended to a maximal independent subset of T. To prove (R3), let I be a maximal independent subset of $S \cap T$, and let $I' \supseteq I$ be a maximal independent subset of $S \cup T$, containing I. Then

$$I' \cap (S \cap T) = I,$$

as the left hand side is independent, and I was a maximal subset of $S \cap T$. We also have

$$|I| = \rho(S \cap T),$$

$$|I'| = \rho(S \cup T),$$

$$|I' \cap S| \leq \rho(S),$$

and

$$|I' \cap T| \leq \rho(T).$$

[4]This is called the *(weak) circuit elimination axiom*, and is a weaker form of the original *circuit elimination axiom* used by Whitney, which is listed as (C2') in the appendix (see [7] p. 9). The reason for the designation "axiom" will become clearer when the alternative definitions of a matroid are given. While (C2) can be proven directly in terms of independent sets, as in Oxley's exposition, the derivation belows shows the sort of manipulations which can be made with rank and nullity.

The last inequality follows from the fact that $I' \cap T$ is an independent subset of T, but not necessarily a maximal one, since some element of $I' \setminus T$ might be preventing any more elements of T from being added to I'. So it suffices to show that

$$|I' \cap S| + |I' \cap T| = |I' \cap S \cap T| + |I'|,$$

which is just a form of the inclusion-exclusion principle for two sets.

An important concept related to rank is nullity.

Definition 4. *(Whitney) The* nullity *of a set $S \subseteq E$ is defined to be $n(S) = |S| - \rho(S)$.*

Then we have the following properties analogous to rank:

(N1) For any set S, $0 \leq n(S) \leq |S|$.

(N2) If $S \subseteq T$, then $n(S) \leq n(T)$.

(N3) For any S, T, we have

$$n(S) + n(T) \leq n(S \cup T) + n(S \cap T).$$

The first property is obvious, and the third is obtained by subtracting the semimodular inequality from the identity

$$|S| + |T| = |S \cup T| + |S \cap T|.$$

To prove the second, note that by the semimodular inequality,

$$\rho(T) = \rho((T \setminus S) \cup S) \leq \rho(T \setminus S) + \rho(S) - \rho(\emptyset) \leq |T \setminus S| + \rho(S) + 0 = |T| - |S| + \rho(S).$$

After rearranging, this gives the desired inequality

$$|T| - \rho(T) \geq |S| - \rho(S).$$

Using these theorems on rank and nullity, we can prove property (C2) above.

Lemma 1. *The nullity of any circuit C is 1.*

Proof. Since the empty set is independent in any matroid, every circuit has at least one element. So there is some $x \in C$. Since C is not independent, $\rho(C) < |C|$, but since $C \setminus \{x\}$ *is* independent, $\rho(C \setminus \{x\}) = |C \setminus \{x\}| = |C| - 1$. So by (R2), we have

$$|C| - 1 = \rho(C \setminus \{x\}) \leq \rho(C) < |C|.$$

Therefore, $\rho(C) = |C| - 1$, so $n(C) = 1$. □

Theorem 1. *Property (C2) holds. That is, if C_1 and C_2 are two distinct circuits both containing an element x, then $D = (C_1 \cup C_2) \setminus \{x\}$ contains a circuit.*

Proof. Since C_1 and C_2 are distinct, neither contains the other, so $C_1 \cap C_2$ is a proper subset of both circuits, and is therefore independent. Therefore,

$$n(C_1 \cup C_2) \geq n(C_1) + n(C_2) - n(C_1 \cap C_2) = 1 + 1 - 0 = 2.$$

Then since $C_1 \cup C_2 = D \cup \{x\}$, we have

$$n(D \cup \{x\}) = n(C_1 \cup C_2) \geq 2,$$

and also

$$n(D \cup \{x\}) = |D \cup \{x\}| - \rho(D \cup \{x\}) \leq |D| + 1 - \rho(D) = n(D) + 1.$$

It follows that $n(D) + 1 \geq 2$, and so $n(D) \neq 0$, implying that D is not independent, and therefore contains a cycle. □

To round off the definitions, we can define the notion of "span" in any matroid, though this is more frequently ([11],[7]) referred to as "closure." Formally,

Definition 5. *if S is a set in a matroid, then the* closure *or* span *of S, is the set*

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

If x is in the closure of a set S, we also say that S spans *x, or that x* depends on *S.*

Note that every element of S is in the closure of S, $S \subseteq \mathrm{cl}(S)$.

For the case of a matric matroid, x is in the closure of S if x in in the usual span of S, that is, if x is a linear combination of elements of S. This follows from the fact that if x is a linear combination of S, then the space spanned by $S \cup \{x\}$ is the same as the space spanned by S, and so $\rho(S) = \rho(S \cup \{x\})$. Conversely, if $\rho(S) = \rho(S \cup \{x\})$, then the subspace spanned by S has the same dimension as the larger space spanned by $S \cup \{x\}$, and so the two subspaces are equal, implying that x is itself in the space spanned by S.

For the case of a graphic matroid, an edge e is in the span of another set of edges S unless the graph with edges $S \cup \{x\}$ has fewer connected components than the graph with edges S (assuming we keep all the vertices form the underlying graph around). So clearly, e is spanned by S exactly when the two endpoints of e are already connected by edges in S. Noticed that we could equivalently say that $e \notin S$ is in the closure of S exactly when $e \cup S'$ is a circuit, for some $S' \subseteq S$. This principle holds in any matroid, as we will see shortly.

For the case of a uniform matroid $U_{k,n}$, of rank k on a set of size n, we see that the closure of a set S is just S, when $|S| < k$, and the whole matroid otherwise. This is relatively straightforward from the definitions.

The term "closure" has certain connotations in mathematics, so it behooves us to prove the following three properties, which are generally taken to be the defining attributes of a closure operation:

(S1) If S is a set, then $S \subseteq \mathrm{cl}(S)$.

(S2) If S is a set, then $\mathrm{cl}(\mathrm{cl}(S)) = \mathrm{cl}(S)$.

(S3) If $S \subset T$, then $\mathrm{cl}(S) \subseteq \mathrm{cl}(T)$.

But first,we need the following intermediate result:

Lemma 2. *For any S, $\rho(cl(S)) = \rho(S)$.*

Proof. Consider the following family of sets, for fixed S:

$$\mathcal{F} = \{T \subseteq E \ : \ T \supseteq S, \rho(T) = \rho(S)\}.$$

If $T_1, T_2 \in \mathcal{F}$, then

$$\rho(S) \leq \rho(T_1 \cap T_2) \leq \rho(T_1) = \rho(S),$$

and

$$\rho(S) \leq \rho(T_1 \cup T_2) \leq \rho(T_1) + \rho(T_2) - \rho(T_1 \cap T_2) = \rho(S) + \rho(S) - \rho(S) = \rho(S),$$

so that $T_1 \cup T_2 \in \mathcal{F}$. Also, we know that if $x \in \mathrm{cl}(S)$, then $\rho(S \cup \{x\}) = \rho(S)$, so that

$$S \cup \{x\} \in \mathcal{F}$$

for every $x \in \mathrm{cl}(S)$. Since $\mathcal{F}$ is closed under unions, we see that

$$\mathrm{cl}(S) = S \cup \mathrm{cl}(S) = \bigcup_{x \in \mathrm{cl}(S)} S \cup \{x\} \in \mathcal{F}.$$

So therefore $\rho(\mathrm{cl}(S)) = \rho(S)$. □

Theorem 2. *Properties (S1-3) are true in any matroid.*

Proof. The first condition, (S1), is rather obvious since if $x \in S$, then $\rho(S \cup \{x\}) = \rho(S)$. For (S2), note that if $x \in \text{cl}(\text{cl}(S))$, then

$$\rho(\text{cl}(S) \cup \{x\}) = \rho(\text{cl}(S)) = \rho(S),$$

by the lemma, implying

$$\rho(S) \leq \rho(S \cup \{x\}) \leq \rho(\text{cl}(S) \cup \{x\}) = \rho(S),$$

so that $x \in \text{cl}(S)$.

For (S3), suppose that $x \in \text{cl}(S)$. Then $\rho(S \cup \{x\}) = \rho(S)$, so that

$$\rho(T \cup \{x\}) = \rho(T \cup (S \cup \{x\})) \leq \rho(T) + \rho(S \cup \{x\}) - \rho(T \cap (S \cup \{x\})) \leq \rho(T) + \rho(S \cup \{x\}) - \rho(S) = \rho(T),$$

so that $x \in \text{cl}(T)$. □

Properties (S1-3) establish that closure is in fact a proper closure operator. We can define a set to be *closed* if it equals its closure, or equivalently by (S2), if it is the closure of some set. The intersection of two closed sets is closed, and the closure of any set is just the intersection of the closed sets containing it. If the union of any two closed sets was closed, we would have a topological space. This would actually be equivalent to the identity

$$\text{cl}(S \cup T) = \text{cl}(S) \cup \text{cl}(T),$$

for any S and T. However, this is rarely the case for matroids[5]. Instead, we have an odd property, the *MacLane-Steinitz exchange property*:

(S4) If $x \notin \text{cl}(S)$, but $x \in \text{cl}(S \cup \{y\})$, then $y \in \text{cl}(S \cup \{x\})$.

To prove this, it helps to first prove the following alternative characterization of closure, which is sometimes taken to be the *definition* of closure:

Theorem 3. *For some set S of elements of a matroid, an element x is in cl(S) if and only if at least one of the following is true:*

(a) $x \in S$

(b) $\{x\} \cup T$ *is a circuit, for some* $T \subseteq S$.

Proof. First, suppose that (a) is true. Then obviously $x \in \text{cl}(S)$, by (S1) above. Next, suppose that (b) is true. Then for some $T \subseteq S$, $\{x\} \cup T$ is a circuit, which implies that T is independent. So we have $n(T) = 0$ and $n(T \cup x) = 1$. Then by inequality (N3),

$$n(S \cup \{x\}) = n(S \cup T \cup \{x\}) \geq n(S) + n(T \cup \{x\}) - n(T) = n(S) + 1.$$

so therefore

$$\rho(S) \leq \rho(S \cup \{x\}) = |S \cup \{x\}| - n(S \cup \{x\}) \leq |S| + 1 - (n(S) + 1) = |S| - n(S) = \rho(S).$$

So $x \in \text{cl}(S)$.

Finally, it remains to show that if $x \in \text{cl}(S)$, and $x \notin S$, then (b) holds for some T. Let I be a maximal independent subset of S. Then $|I| = \rho(S) = \rho(S \cup \{x\})$, so I is also a maximal independent subset of $S \cup \{x\}$. Therefore $I \cup \{x\}$ is *not* independent, and contains some circuit C. If $x \notin C$, then $C \subseteq I$, contradicting the choice of I. Therefore $x \in C$, and we are done. □

With this result, (S4) is easy to prove:

Theorem 4. *(S4) above holds.*

[5]In fact, it only occurs for uniform matroids of the form $U_{n,n,}$.

Proof. Intuitively, if x is in the closure of $S \cup \{y\}$, then this is caused by a circuit in $S \cup \{y\}$, which must "use" y, since S by itself does not generate x. Then since some circuit has both x and y, we can reverse this argument to see that y is in the closure of S and x.

Or more rigorously, since $x \in \text{cl}(S \cup \{y\})$, then either $x = y$, or there is some circuit $C \subseteq S \cup \{x\} \cup \{y\}$ containing x. In the first case, we obviously have $y = x \in \text{cl}(S \cup \{x\})$. In the other case, if $y \notin C$, then C shows that $x \in \text{cl}(S)$. Therefore, $y \in C$, so $y \in \text{cl}(S \cup \{x\})$. □

The notion of closure turns out to have many of the properties that we would like it to have. In particular:

- A minimal set whose closure is the entire matroid is the same thing as a basis.
- For any S, a minimal subset of S whose closure contains S is the same as a maximal independent subset of S.
- The closure of S is the biggest set containing S and having the same rank as S.
- A set I is independent iff no element of I is in the closure of the other elements of I.

3.3 A Plethora of Definitions

Amazingly enough, many of the properties of bases, circuits, rank, and closure can be used as alternative definitions of a matroid.

Specifically, we can define a *matroid* to be a set E, and a non-empty collection of subsets $\mathcal{B}$, called *bases*, such that

(B1) No basis is contained in another basis.

(B2) if B_1 and B_2 are bases, then for every $x \in B_1 \setminus B_2$, there is some $y \in B_2 \setminus B_1$, such that $(B_1 \setminus \{x\}) \cup \{y\}$ is a basis.

One would be tempted to add (B3), the claim that all bases have the same size from the previous section, but it can be proven from (B1) and (B2) [6]. Roughly speaking, if we had two bases of different size, $B_1, B_2 \in \mathcal{B}$, with $|B_1| < |B_2|$, then by repeatedly swapping elements of $B_1 \setminus B_2$ for elements of $B_2 \setminus B_1$, one would eventually end up with a basis which was a subset of B_2, but of the original size of B_1, contradicting axiom (B1).

With this definition, we *define* an *independent* set to be any set contained in a basis. Then axiom (I1) is obvious, and axiom (I2) can be established using a similar series of exchanges as is used to prove (B3). So this definition of matroid is equivalent to our original one [7].

Using circuits, we can define a *matroid* to be a set E, and a collection of non-empty subsets $\mathcal{C}$, called *circuits*, such that

(C1) No circuit is contained in another circuit.

(C2) If $C_1, C_2 \in \mathcal{C}$, and $x \in C_1 \cap C_2$, then $C_1 \cup C_2 \setminus \{x\}$ contains a circuit.

Axiom (C2) could also be replaced with the stronger axiom in which "contains a circuit" is replaced with "is a union of circuits" (as was essentially done in [10]). With either definition of matroid, a *dependent set* is defined to be any set containing a circuit, and any other set is an *independent* set. It can be proven that these definitions are equivalent to the one using independent sets.

Using rank, we define a *matroid* to be a set E, and a map ρ from the subsets of E to the integers, satsifying

(R1) For any set S, $0 \leq \rho(S) \leq |S|$.

(R2) If $S \subset T$, then $\rho(S) \leq \rho(T)$.

(R3) If $S, T \subseteq E$, then the following *semimodular* inequality holds:

$$\rho(S) + \rho(T) \geq \rho(S \cup T) + \rho(S \cap T).$$

With this definition, an *independent set* is a set S satisfying $\rho(S) = |S|$. As usual, this definition turns out to be equivalent to the given definition.

Finally, using closure, we define a *matroid* to be a set E, and a map $\mathrm{cl}(\cdot)$ from the subsets of E to the subsets of E, such that

(S1) If S is a set, then $S \subseteq \mathrm{cl}(S)$.

(S2) If S is a set, then $\mathrm{cl}(\mathrm{cl}(S)) = \mathrm{cl}(S)$.

(S3) If $S \subset T$, then $\mathrm{cl}(S) \subseteq \mathrm{cl}(T)$.

(S4) If $x \notin \mathrm{cl}(S)$, but $x \in \mathrm{cl}(S \cup \{y\})$, then $y \in \mathrm{cl}(S \cup \{x\})$.

With this definition, a set I is *independent* iff for every $x \in I$, $x \notin \mathrm{cl}(I \setminus \{x\})$.

Many of these equivalent definitions were noted by Whitney in his original paper [10], though he sometimes used slightly different axioms from what has later become standard. For the most part, the axioms given here agree with Wilson's [11] and Oxley's [7] expositions. There are other definitions of matroids, some of which are more abstract. For example, if we look at the partially ordered set of closed sets, ordered under inclusion, we obtain a lattice (as with any closure operation), but the lattice also has the property that it is semimodular and atomistic[6] Conversely, any lattice that is semimodular and atomistic comes from a matroid, and the semimodular atomistic lattices end up being equivalent to "simple matroids" (which are matroids in which every circuit has cardinality at least 3 - see below) [2]. There is also a definition of matroids involving the greedy algorithm, which seems oddly unrelated to any of the previous definitions.

The presence of a multitude of definitions, which are non-obviously equivalent, has been called "cryptomorphism" by some writers. This term was originally coined by Birkhoff in the context of universal algebra, but it certainly is applicable to matroid theory. The variety of definitions is useful in spotting matroids, since for certain examples of matroids, one definition is easy to verify, while another definition is completely opaque. For example, in the matroids arising in linear algebra (the matric matroids), concepts like rank and independence are completely straightforward, but circuits are a bizarre construct. For the case of algebraic closure, the closure axioms seem easiest to check, while for the case of dual matroids, the rank axioms are easiest. Also, the equivalence of the definitions implies that any structure which satisfies one of the definitions immediately has a rich structure involving all the other constructs. For example, as soon as we know that algebraic closure satisfies something like (S4), we immediately can see that a notion like transcendence degree is meaningful, because all the transcendence bases are equal in size, by (B3). Thus for the theory of matroids, one of the most useful tools is simply the ability to seamlessly switch between definitions.

4 Examples of Matroids

We have already seen three types of matroids: graphic, matric, and uniform matroids[7]. In this section, we present several more examples, though there is hardly enough space to prove that all are valid matroids.

[6] A *lattice* is a partial order in which any finite non-empty set has an infimum and supremum. Equivalently, any two elements x and y have a supremum $x \vee y$, and an infimum $x \wedge y$. For the case of finite lattices, all sets will have infima and suprema. A semimodular lattice can be defined in various ways, but one way is to say that whenever x *covers* $x \wedge y$ (meaning that no z satisfies $x \wedge y < z < x$), then $x \vee y$ covers y. For finite semimodular lattices, there is always a rank function ρ into the integers such that $\rho(x) \geq \rho(y)$ if $x \geq y$, $\rho(x) = \rho(y) + 1$ if x covers y, and the semimodular inequality holds: $\rho(x \vee y) + \rho(x \wedge y) \leq \rho(x) + \rho(y)$. The rank of x is the length of any sequence between x and the least element of the lattice, in which each element of the sequence covers its successor. Such a sequence is called a *composition sequence,* and semimodular lattices have the property that any two composition sequences between two elements are equal in length. An *atom* in a lattice is an element which covers the least element, and a lattice is *atomistic* if each element is the supremum of a (possibly empty) set of atoms. It seems like there should be a matroid structure defined on the atoms of *any* finite semimodular lattice.

[7] In fact, both graphic matroids and uniform matroids are representable/matric. Graphic matroids are representable over any field, which is easily seen by choosing the free vector space generated by the vertices, and associating an edge between

4.1 Cographic matroids

We have already seen how to define a "graphic" or "cycle" matroid for any graph G. There is also another matroid, the *cographic matroid* ([11]) of G, which is likewise defined on the edges of E. The circuits in the cographic matroid are the *cut-sets* of G, where a cut-set is a collection of edges C, such that when the edges in C are deleted from G, the number of connected components of G increases by one. So if G is connected, then a cut-set is a group of edges which separet G into two connected halves. Equivalents, we could define x to be in the closure of S if $x \in S$ or the two endpoits of x are disconnected by S. Equivalently, for $x \notin S$, $x \in \mathrm{cl}(S)$ iff every path between the endpoints of x, not using x itself, passes through S.

The significance of this definition becomes evident when considering a planar graph G. Any connected planar graph has a dual graph $G*$, and the edges of G can be naturally identified with the edges of G. With this identification, the cut-sets in $G*$ are exactly the cycles in G, and vice versa. Therefore, the cographic matroid of G is the graphic matroid of $G*$, and vice versa. So in some sense, the graphic and cographic matroid of a planar graph are "dual" to one another. We will see later that this sort of duality can be extrended to any matroid, not just the graphic matroid of a planar graph.

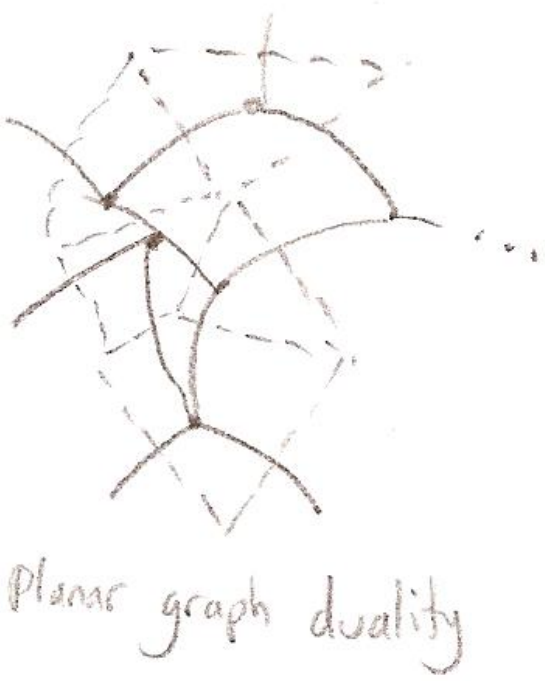

Figure 1: Planar Graph Duality

vertices a and b with the formal difference $a-b$ (or $b-a$). Then a set of edges is cyclic iff the corresponding vectors are linearly dependent. Such matroids, which are representable over all fields, are called regular matroids. A uniform matroid $U_{k,n}$ can be represented over, say $\mathbb{Q}$, by just choosing n random vectors in a k-dimensional space. With high probability, this will produce the correct matroid. This construct doesn't work in finite fields, however. So for example, $U_{2,4}$ is not representable over the field of order 2, as shown on p. 20 of [7].

4.2 Bicircular matroids

We can assign yet another matroid to a graph G, using a slight modification to the definition of the graphic/cycle matroid. In the cycle matroid of G, the independent sets were the sets of acyclic edges, that is, the *forests*. In the *bicircular matroid*, the independent sets are the pseudoforests, where a *pseudoforest* is a graph in which there is at most one cycle in each connected component [9].

It is easy to see that the number of edges in a pseudoforest P is equal to the number of vertices in P minus the number of acyclic connected components of P. A maximal pseudoforest P in a connected graph G will necessarily have a cycle in each component of P, unless G is itself acyclic. Furthermore, if the pseudoforest is truly maximal, its edges must cover all the vertices in G. Therefore the size of a maximal pseudoforest is the number of vertices in G, or one less if G is acyclic. Then if G is not connected, the size of a maximal pseudoforest is the total number of vertices in G minus the number of acyclic connected components of G. Since this doesn't depend on the pseudoforest, we see that the maximal pseudoforests in any graph are all the same size. Therefore, if S is a set of edges in a graph, and we define a set of edges to be independent iff it is a pseudoforest, then the maximal independent subsets of S are all the same size. It follows that axioms (I1) and (I2') hold. The resulting matroid is called a *bicircular matroid*. Unlike graphic matroids, these are not necessarily representable over all fields, though they are always representable over $\mathbb{Q}$.

4.3 Transversal matroids

A completely different type of matroid comes from transversal theory. Suppose that we have two sets, E and F, with a relationship between them: $R \subseteq E \times F$. A good example might be the case where E is a set of classes, F is a set of time slots, and xRy if class x is offered at time slot y. Another example is when E is a set of women, F is a set of men, and xRy if x can be married to y. With this in mind, a *transversal* (defined in [3]) is a one-to-one mapping f from E to F, such that $eRf(e)$ for all $e \in E$. Similarly, a *partial* transversal is a one-to-one mapping f from a subset $E' \subseteq E$ to F, such that $eRf(e)$ for $e \in E'$. For the first example, a partial transversal would be a way to schedule all of the classes in non-overlapping times, and a partial transversal is a way to schedule some of the classes. For the marriage example, a partial transversal would be a way to marry off a set of women. We can define a *transversal matroid* on E by taking the independent sets to be the E' for which a partial transversal exists [3]. Amazingly, this defines a matroid. This type of matroid partially explains the significance of matroid theory in the field of combinatorial optimization.

4.4 Matching matroids

If we have an undirected graph G, then a *matching* is a collection of edges in G such that no two edges share a vertex. If we imagined that the vertices were people, and an edge connected any two people who could be married, then a matching would be a way of marrying off some of the people. As in the previous case, we can define a matroid, in which a set of vertices I is independent if it is covered by a partial matching. We could also restrict ourselves to only consider sets $I \subseteq J$, for some fixed J, while still allowing matches to involve vertices outside of J. This sort of matroid is called a *matching matroid* [3]. In the case that the graph is bipartite, and J is one side of the partition, this is just a transversal matroid.

4.5 Gammoids

Let G be a directed graph, and S and T be two sets of vertices in G, not necessarily disjoint. Let a subset $I \subseteq S$ be independent if there exists a directed path from each element of I to an element of T, and the paths are pairwise vertex-disjoint. This bizarre definition defines a matroid on S, called a *gammoid* [11]. If S and T are disjoint, and every vertex in G is in $S \cup T$, and every edge in G runs from S to T, then the gammoid will just be a transversal matroid again. Gammoids are mainly of interest because they are the closure of transversal matroids under the operations of minors and duality, defined below in §5.

4.6 Matroids from projective configurations

Suppose we have some points in the projective plane. Define the rank of a finite set of points to be 0 if the set is empty, 1 if the set consists of just one point, 2 if the points are contained in a line, and 3 otherwise. In other words, the rank is one more than the dimension of the smallest subspace containing all the points. This also defines a matroid, with the semimodular inequality following from the incidence relationships. Furthermore, this can be generalized easily to higher dimensions, and works just as well over projective and affine spaces from any field. In fact, these matroids are just the representable matroids in disguise. Suppose we have some set of points in a projective space P_n. The space P_n is usually defined as a quotient space of a vector space V of dimension $(n+1)$, so for each of our points, we can choose some vector in V. The rank-k linear subspaces of V correspond to the $(k-1)$-dimensional subspaces of P_n, and so the matroid associated with the configuration of points in projective space is the same as the representable matroid coming from the associated points in V.

In particular, a matroid M of rank n is representable over a field k iff it can be represented in terms of some configuration of points in the projective space of dimension $n-1$ over k. This connection was noted by Saunders MacLane [5], who used it to explain why certain matroids were not representable. For example, consider the following abstract configuration of points and lines:

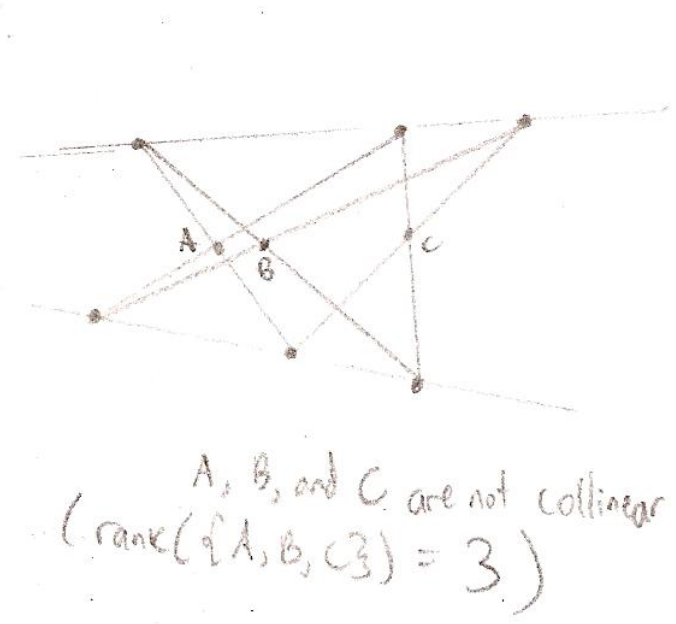

Figure 2: An impossible configuration

This configuration violates Pappus's Theorem, and so it cannot occur in any projective space coming from a field. Yet we can still define a matroid for this structure, by defining the rank of any one point to be 1, the rank of any two points to be 2, and the rank of any 3 points to be 3, unless the 3 points are on one of the "lines" marked in the diagram (in which case they have rank 2). All sets with more than 3 elements have rank 3. The resulting matroid is not representable over any field. This example had been originally found by Whitney, but the geometric understanding is due to MacLane.

MacLane also used this idea to construct matroids which are only recognizable over special fields. For example, in the following affine configuration, the ratio between the distances on the bottom line must be $\sqrt{2}$. By adding the line at infinity, we get a projective configuration which can only exist when the underlying field includes $\sqrt{2}$.

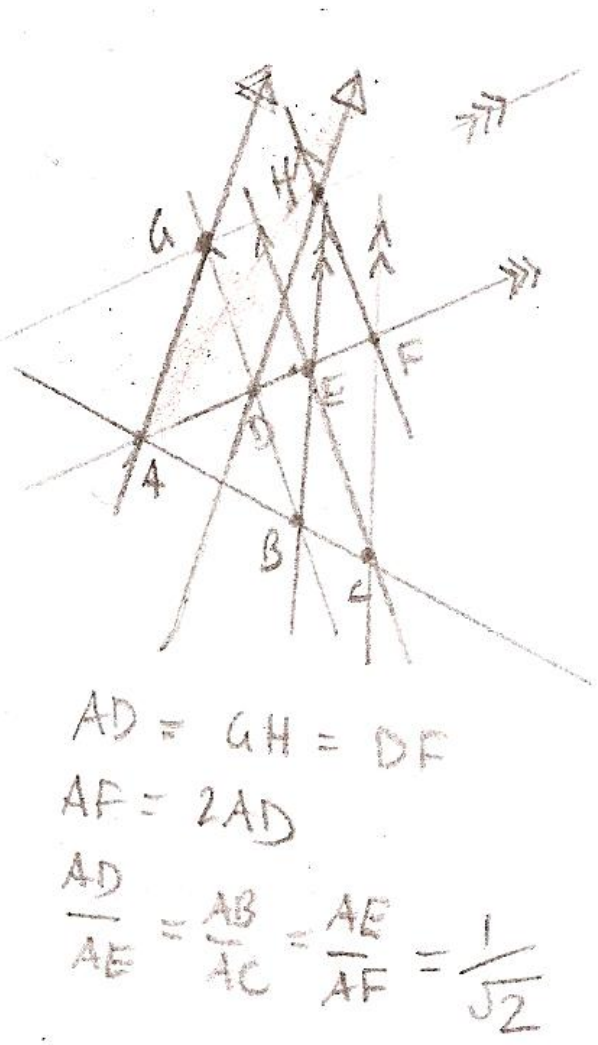

Figure 3: Planar Graph Duality

So the corresponding matroid is not representable over $\mathbb{Q}$. Similar tricks can be used to construct matroids which are only representable over finite fields, or over the fields in which an arbitrary equation can be solved.

5 Operations on Matroids

5.1 Deletion and Submatroids

Like many other structures in mathematics, there is a well-defined notion of a substructure. If M is a matroid on a set E, and E' is any subset of E, then we can define a matroid on E' by taking a subset of E' to be independent if and only if it was independent in the original matroid. In other words, we simply restrict the notion of independence and dependence to the subsets of E'. This is clearly still as matroid, as

it satisfies axioms (I1) and (I2). This new matroid M' is a *submatroid* of M, called the *restriction of M to E'* [7]. We could also have defined the submatroid structure in terms of rank, bases, circuits, or closure. The rank function on the submatroid M' will just be the restriction of the rank function from the original matroid. That is, if $S \subseteq E'$, then $\rho_{M'}(S) = \rho_M(S)$. The circuits in the submatroid are just the original circuits that were contained in E . That is, if $S \subseteq E$, then S is a circuit in M' iff it is a circuit in M. The closure operator in the submatroid is also somewhat similar: for $x \in E'$ and $S \subseteq E'$, x is in the closure of S with respect to M' exactly if it is in the closure of S with respect to M. That is,

$$\mathrm{cl}_{M'}(S) = M' \cap \mathrm{cl}_M(S).$$

These ideas reflect the fact that independence, rank, and closure are in some sense intrinsic properties of a set.

On the other hand, whether a set S is a basis depends on the relationship between S and the ambient matroid M. So a basis in M' will generally not be a basis in M, but will instead be a maximal independent subset of E'.

If M is a matroid, and $x \in M$, then the submatroid on the set $E \setminus \{x\}$ is called the matroid obtained by *deleting* x, and is denoted by $M \setminus x$. We can also delete a subset S of E, which is the same as restricting to the complement of S.

5.2 Duality

An important concept in matroid theory is the notion of *duality*. To each matroid M on a set E, there is a dual matroid M^D defined on the same set E. The simplest definition of M^D is through bases: the bases of M^D are the complements of the bases of M. However, it is not obvious from this definition that M^D is a matroid. Instead, we'll define duality using rank:

Definition 6. *(Whitney) If M is a matroid on a set E, then the* dual matroid M^D *is another matroid on the same set E, with rank function given by:*

$$\rho_{M^D}(S) = \rho_M(E \setminus S) + |S| - \rho_M(E).$$

It's still not obvious that this defines a matroid, but axioms (R1-3) are easy to verify.

Theorem 5. *M^D is a valid matroid satisfying (R1-3).*

Proof. For (R1), note that by the semimodular inequality,

$$\rho_M(E) \leq \rho_M(S) + \rho_M(E \setminus S),$$

so that

$$\rho_{M^D}(S) = \rho_M(E \setminus S) + |S| - \rho_M(E) \geq |S| - \rho_m(S) \geq 0,$$

and since $\rho_M(E \setminus S) \leq \rho_M(E)$, we have

$$\rho_{M^D}(S) = \rho_M(E \setminus S) + |S| - \rho_M(E) \leq |S|.$$

So (R1) holds in M^D.

Next, for (R2), suppose that $S \subseteq T \subseteq E$. Then $E \setminus S = (E \setminus T) \cup (T \setminus S)$, so again applying the semimodular inequality,

$$\rho_M(E \setminus S) \leq \rho_M(E \setminus T) + \rho_M(T \setminus S) \leq \rho_M(E \setminus T) + |T| - |S|,$$

so that

$$\rho_{M^D}(S) = \rho_M(E \setminus S) + |S| - \rho_M(E) \leq \rho_M(E \setminus T) + |T| - \rho_M(E) = \rho_{M^D}(T),$$

establishing (R2).

Finally, (R3) follows by adding together the following three (in)equalities:

$$\rho_M(E \setminus S) + \rho_M(E \setminus T) \geq \rho_M(E \setminus (S \cup T)) + \rho_M(E \setminus (S \cap T)),$$
$$|S| + |T| = |S \cup T| + |S \cap T|,$$
$$-\rho_M(E) - \rho_M(E) = -\rho_M(E) - \rho_M(E).$$

□

Now that the definition of dual is established, we can consider the bases of the dual matroid. Clearly a basis in M was just a set B for which

$$|B| = \rho_M(B) = \rho_M(E).$$

Similarly, a basis in M^D is just a set B such that

$$\rho_{M^D}(B) = |B| = \rho_{M^D}(E),$$

or, using the definition of M^D,

$$\rho_M(E \setminus B) + |B| - \rho_M(E) = |B| = \rho_M(E \setminus E) + |E| - \rho_M(E) \equiv |E| - \rho_M(E),$$

which is equivalent to

$$\rho_M(E \setminus B) = \rho_M(E) = |E| - |B| \equiv |E \setminus B|.$$

We have just proven the following:

Theorem 6. *A set $B \subseteq E$ is a basis in a dual matroid M^D iff its complement $E \setminus B$ is a basis in the original matroid M.*

This justifies the earlier claim that the bases in the dual matroid are exactly the complements of the bases in the original matroid. It also shows that duality is truly an involution. With this result, it is not hard to see that a *codependent* set in a matroid M, i.e., a dependent set in the dual matroid M^D, is just a set which intersects every basis of M.

Duality can also be expressed in terms of the closure operator, by the following theorem:

Theorem 7. *Suppose that M is a matroid on a set E, and E can be written as a disjoint union of $S \cup \{x\} \cup T$. Then exactly one of the following is true:*

(a) $x \in cl_M(S)$.

(b) $x \in cl_{M^D}(T)$.

Proof. Note that $x \in \mathrm{cl}_{M^D}(T) \Leftrightarrow \rho_{M^D}(T \cup \{x\}) = \rho_{M^D}(T) \Leftrightarrow$

$$\rho_M(S) + |T \cup \{x\}| = \rho_M(S \cup \{x\}) + |T| \Leftrightarrow \rho_M(S \cup \{x\}) - \rho_M(S) = 1.$$

Now

$$\rho_M(S) \leq \rho_M(S \cup \{x\}) \leq \rho_M(S) + \rho_M(\{x\}) \leq \rho_M(S) + 1,$$

so therefore $\rho_M(S \cup \{x\}) - \rho_M(S)$ is either 0 or 1. It follows that

$$x \in \mathrm{cl}_{M^D}(T) \Leftrightarrow \rho_M(S \cup \{x\}) - \rho_M(S) = 1 \Leftrightarrow \rho_M(S \cup \{x\}) - \rho_M(S) \neq 0 \Leftrightarrow x \notin \mathrm{cl}_M(S).$$

□

We have already seen an example of a pair of dual matroids: if G is a graph, then the graphic and cographic matroids of G are dual to each other[8]. In fact, the notion of duality stems from this example, and is closely connected with graph-theoretic duality. If G is a planar graph, then it has some graph-theoretic dual $G*$, whose vertices are the faces of G, and vice versa. We can naturally identify the edges of $G*$ with the edges of G. Importantly, the cut-sets of $G*$ are the circuits of G, and vice versa. Therefore, the matroids of two dual graphs are dual to each other.

We can also talk about an *abstract dual* of a graph G, which is another graph $G*$, whose edges are identified with the edges of G, such that the circuits of G are the cut-sets of $G*$ (and vice versa). By Whitney's Planarity Criterion, any graph with an abstract dual is in fact planar (see [11] section 8). Stated in terms of matroid theory, this tells us that if a matroid M is graphic, and its dual M^D is also graphic (or equivalently, M is cographic), then M is the cycle matroid of a planar graph. Such matroids are called *planar matroids*.

We can discuss the duals of our other examples of matroids, but sometimes things are more opaque.

- In the uniform matroid of rank k on a set of size n, $U_{k,n}$, the bases are exactly the sets of size k. Therefore, the bases in the dual matroid are exactly the sets of size $n-k$, so the dual matroid is just $U_{n-k,n}$.
- The dual of a transversal matroid or a gammoid is always a gammoid, though this is non-trivial (see [7] sections 2.4 and 3.2).
- Interestingly, if a matroid M is representable over a field, then so is its dual M^D. In proving this, we can assume without loss of generality that the elements of M correspond to the columns of a matrix. If M has rank m and size n, we can assume that the matrix is an $m \times n$ matrix, since the size of the vector space containing the columns might as well be m. After reducing the matrix to reduced echelon form, and rearranging the columns, we can assume that the matrix is of the form $[I|A]$, for an $m \times m$ identity matrix I and an $m \times (n-m)$ matrix A. Then consider the matrix $[A^T|I]$, where I is an $(n-m) \times (n-m)$ identity matrix. This new matrix is an $(n-m) \times n$ matrix, whose columns can be identified with the columns of $[I|A]$ in the obvious manner. When this is done, it is not too hard to show that the resulting matroid is dual to the original one (see [7] p. 80). The duals of representable matroids can also be understood geometrically through hyperplanes, as Whitney noted in his original paper ([10]). Whitney's construction is equivalent to the one given here.

5.3 Contraction and minors

The operation of deletion defined above has a dual notion of *contraction*. Specifically, if M is a matroid, and a is an element of M, then the *contraction* of M by a is the matroid

$$M/a = (M^D \setminus a)^D.$$

This definition may be best understood in terms of closure: if $S \subseteq E \setminus \{a\}$ and $x \in E \setminus \{a\}$, then $x \in \mathrm{cl}_{M/a}(S)$ iff $x \in \mathrm{cl}_M(S \cup \{a\})$. The term "contraction" comes from graph theory, since if G is a graph and M is its graphic matroid, then for an edge e, M/e is the graphic matroid of the graph obtained from G by contracting the edge e.

Just as multiple elements of a matroid can be deleted to produce a submatroid, multiple elements can be contracted. In fact, contraction and deletion can be done simultaneously. Specifically, if M is a matroid, and S and T are two disjoint subsets of E, then we can define the matroid $M \setminus S/T = M/T \setminus S$, called a *minor* of M, to be the matroid M' on $E \setminus (S \cup T)$, in which $\mathrm{cl}_M(X) = \mathrm{cl}_M(X \cup T) \setminus (S \cup T)$, for any $X \subseteq E \setminus (S \cup T)$. By the discussions on contraction and deletion above, and their effects on the closure operator, it is clear that the matroid M can be obtained by successively deleting all the edges in S and contracting all the edges in T, in any order. Of course, either S or T might be empty.

[8]This is because a set is dependent in the dual of the graphic matroid iff it intersects every spanning forest, iff it separates a connected component of G. A set is dependent in the cographic matroid iff its removal increases the number of connected components by some amount.

For the case of graphic matroids, matroid minors correspond to the usual minors of graph theory. That is, if G is a graph, and M is the cycle matroid of G, then a minor $M \setminus S/T$ is just the cycle matroid of the graph obtained by deleting all the edges in S and contracting all the edges in T. This new sort of graph is called a *minor* in the standard terminology of graph theory. Minors can be used to express several interesting results. For example, it turns out that a graph is planar exactly when it has neither of the following two graphs as minors:

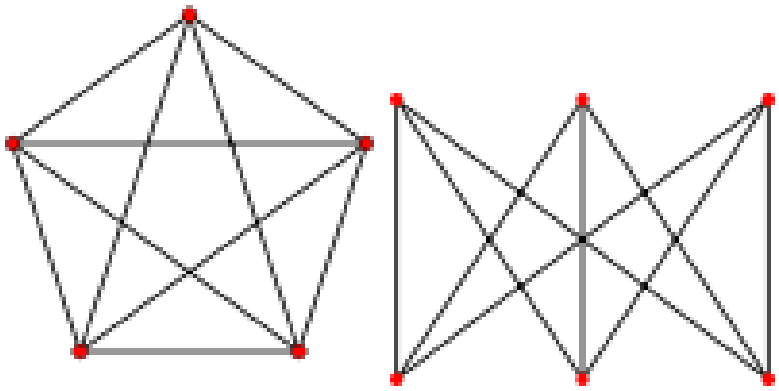

Figure 4: Forbidden minors for planar graphs (images from Wikipedia)

These two graphs are called the *forbidden minors* of the class of planar graphs. Any class definable through forbidden minors must be closed under minors, because the relationship of being a minor is a partial order. Amazingly, any class of graphs which is closed under minors can be defined with a finite set of forbidden minors. This is the celebrated Robertson-Seymour theorem. No similar result is known for matroids, but the notion of forbidden minors is still quite useful. For example, the matroids that are representable over the field of order 2 have been classified in terms of forbidden minors, as have regular, graphic, cographic, and planar matroids ([7], pp. 203,213).

5.4 Sums and components

Given two matroids M_1 and M_2, we can form a *sum* matroid $M_1 + M_2$ on the disjoint unions of the base sets, by saying that a set $S \subseteq E_1 \cup E_2$ is independent if $S \cap E_1$ and $S \cap E_2$ are independent. Equivalently, we have

$$\rho_{M_1+M_2}(S) = \rho_{M_1}(S \cap E_1) + \rho_{M_2}(S \cap E_2),$$
$$\mathrm{cl}_{M_1+M_2}(S) = \mathrm{cl}_{M_1}(S \cap E_1) \cup \mathrm{cl}_{M_2}(S \cap E_2).$$

The sum operator cooperates with duality: $M_1^D + M_2^D = (M_1 + M_2)^D$. A matroid which can be written as a non-trivial sum is called a *separable* matroid. Equivalently, a matroid M is separable if E can be partitioned as $E_1 \cup E_2$, for disjoint E_1 and E_2, such that $\rho(E_1) + \rho(E_2) = \rho(E)$. In his initial paper [10], Whitney proved that any matroid has a unique decomposition as a union of non-separable matroids. Moreover, he proved the following:

Theorem 8. *(Whitney) Two elements e_1, e_2 of a matroid M belong to the same non-separable component of M iff there is some circuit C with $e_1, e_2 \in C$.*

It is rather surprising that this relationship should be transitive, but can be proven using (C1-2).

For the case of graphic matroids, non-separability is just biconnectivity[9]. Thas is, a graph's matroid will be nonseparable if the graph is biconnected[10], and the components of a graphic matroid are just the largest biconnected components of the graph.

[9] A graph is *biconnected* if it remains connected after the removal of any edge.
[10] This ignores the case when there are vertices detached from any edges.

6 Simple Matroids

Within graph theory, we often speak of "simple graphs," which are graphs in which there is at most one edge between any two nodes, and no self-loops running between a vertex and itself. These notions have straightforward analogs in matroid theory. First, we define a *loop* in a matroid M to be an element $x \in M$ which is a circuit by itself. Equivalently, a loop is a singleton set $\{x\}$ of rank 0. Loops are exactly the elements in the closure of the empty set, and are also the elements which are not contained in any independent sets or bases. In the case of a representable matroid, this would correspond to the zero vector. In a graphic matroid, these correspond to self-loops. For the transversal matroid corresponding to classes and timeslots, this would correspond to a class which was not scheduled at any time.

If x and y are not loops, then we say that x and y are *parallel* if $\{x, y\}$ is a 2-element circuit. This is equivalent to any of the following statements:

- The rank $\rho(\{x, y\}) = 1$.
- $x \in \text{cl}(\{y\})$ and $y \in \text{cl}(\{x\})$.
- At most one of x and y occurs in any basis or independent set.

Note that if x is parallel to y and y is parallel to z, then by (C2), there is some circuit contained in $(\{x, y\} \cup \{y, z\}) \setminus \{y\} = \{x, z\}$, and since neither x nor y is a loop, x is parallel to z. It follows that parallelship is an equivalence relationship, and we can speak of parallel classes.

For the case of a graphic matroid, two edges are parallel if they have the same endpoints. For a representable matroid, two vectors are parallel if one is a scalar multiple of another (i.e., they are parallel!). For the transversal matroid corresponding to classes and timeslots, two classes are parallel if each is only offered at one time, and the two times are the same.

With these definitions, a *simple matroid* is one in which there are no loops, and the parallel relationship is trivial (no two elements are parallel). Equivalently, a simple matroid is one in which all sets of one or two elements are independent, or even more simply, one in which all circuits have at least three elements.

A matric matroid will be simple if it does not contain the zero vector, and no two vectors are parallel. In projective geometry, we throw out the zero vector, and identify vectors which are parallel, so the matroids coming from configurations in projective space are always simple. A graphic matroid will be simple if the graph is simple.

There is a certain sense in which any matroid is associated with a canonical simple matroid ([7]). If M is a matroid on E, let E' be the set obtained by removing the loops from E, and factoring out the parallel equivalence relationship. That is, the elements of E' are the parallel classes of non-loops in M . Then we can give E' a matroid structure M', by any of the equivalent ways:

- A set $S \subseteq E$ is independent if, when some arbitrary representative in E is chosen for each element of S, the set of representatives is independent. (This turns out to not depend on the choice of representatives).
- If S is a set in E', and T is any set which projects onto S when taken modulo parallelicity, then $\rho'_M(S) = \rho_M(T)$.
- If B is a basis in E, then when B is projected onto E' (seeing how no loops are in B), the resulting set is a basis in M, and all bases are generated in this way.
- If S is a set in E', and T is any set which projects onto S modulo parallelicity, then the closure of S is the closure of T with the loops removed, modulo parallelicity.

These rules show that the structure of M and M' are closely related. In fact, the structure of M can be reconstructed from the structure of M', using only the set of loops $L \subseteq M$, and the quotient map of $M \setminus L \to M'$. So really, simple matroids contain all the complexity of general matroids. Interestingly, simple matroids are determined by the structure of their lattice of closed sets. The lattice of closed sets will be a

"geometric" lattice[11] for any matroid, and it turns out that every "geometric" lattice is the lattice of closed sets of an essentially unique simple matroid. If we take a matroid, obtain the lattice, and then obtain the simple matroid, we have just obtained the simple matroid associated with the original matroid.

The notion of a simple matroid does not play well with duality. Neither the notion of a "loop" or a pair of "parallel" elements is self-dual. A loop is an element not contained in any base, so a *coloop* is one contained in *every* basis, or equivalently, an element which is not in the span of everything else. For graphic matroids, this would be an edge which is not part of any cycle, because it connects two otherwise unconnected subgraphs.

Interestingly, the dual notion to two elements x and y being parallel is x and y being serial. Since x and y are parallel iff only one is contained in any basis, x and y are *serial* iff at least one is contained in any basis. Equivalently, any set which spans x contains y, and vice versa. For the case of graphic matroids, this corresponds to two edges which are in series[12], hence the name. Since a simple graph can have coloops and serial edges, we see that the dual to a simple matroid is not necessarily simple.

7 The Greedy Algorithm

One of the main reasons for the importance of matroids in the field of combinatorial optimization is the association between matroids and greedy algorithms. The archetypical example of a greedy algorithm of the sort we're interested in is Kruskal's algorithm for finding a minimal (or maximal) spanning tree. Suppose we have a network of nodes and links between the nodes, and each link has a weight or a cost. We wish to find a collection of links that connect all nodes, using the cheapest total cost. A minimal spanning set will clearly be a tree, so this amounts to finding a spanning tree with minimal cost. Since all spanning trees have the same number of edges, we could also have subtracted all the weights from some upper bound, and asked for a spanning tree with maximal value. Either way, Kruskal's algorithm works as follows:

1. Initialize a set of edges $I = \emptyset$.
2. Sort the edges in order of weight.
3. Run through the edges, starting with the cheapest or most valuable. For each edge e, add e to I unless this produces a cycle in I.

This algorithm is guaranteed to always find a minimal (or maximal) spanning tree, whose elements will end up in I. With the proper data structures, the bulk of the time is spent sorting the edges in the second step, and fast sorting algorithms exist. Consequently, Kruskal's algorithm is of much practical value. The terminology "greedy" refers to the fact that at each step, the algorithm chooses to add the best edge possible at the moment, without any planning ahead. It is rather astonishing that such a greedy algorithm, which only makes locally optimal decisions, manages to always find the globally optimal solution. This often doesn't occur for naive greedy algorithms.

This algorithm can be generalized to any matroid. Suppose we have a matroid M and a function $w : M \to \mathbb{R}$ which assigns weights to each element. The weights could be negative or positive. Our goal is to find the basis B of M such that

$$\sum_{x \in B} w(x)$$

is minimized. If all the weights are positive, we could let B range over not only the bases but all sets which span M. If all the weights are negative, we could let B range over all independent sets. In both cases, the optimal solution will necessarily be a basis.

As in Kruskal's algorithm, we proceed as follows:

1. Initialize a set of elements I to be the empty set $\emptyset$.

[11] an atomistic semimodular lattice, [7] p. 55

[12] with the caveat that neither edge can be a coloop. Also, if we have a long string of edges in series, then any two in the string will be "in series," as this relationship must be an equivalence relationship.

2. Sort the elements of M according to weight.

3. Run through the elements, starting with the smallest/most-negatively weighted elements. For each element x, add x to I unless $I \cup \{x\}$ is dependent.

This algorithm is guaranteed to find a basis. Note that I will certainly end up being an independent set. Moreover, for any element x of the matroid, x must be spanned by I, since if $x \notin I$, then when x was considered on the list, the intermediate set I' must have had $I' \cup \{x\}$ being dependent, which implies that $x \in \text{cl}(I') \subseteq \text{cl}(I)$. So the final set is always an independent set which spans the entire matroid. This is the same as being a basis.

Moreover, this algorithm is guaranted to find an optimal basis.

Lemma 3. *At each step, the set I is contained in an optimal basis.*

Proof. We prove this by induction, by showing that this property is initially true, and is never lost. Clearly the empty set $\emptyset$ is contained in an optimal basis, as it is contained in *all* bases.

Now suppose that the set I is contained in an optimal basis, and we add x, to produced the new set $I \cup \{x\}$. Let B be an optimal basis which contained I. If $x \notin B$, then $I \cup \{x\}$ is a subset of B, so we still have a subset of an optimal basis. So suppose that $x \notin B$.

Since $I \cup \{x\}$ is still independent, it is contained in *some* basis B', which is not optimal. We have $x \in B' \setminus B$, so by the *dual* of the basis exchange principle, there is some $y \in B \setminus B'$, such that $B'' = (B \setminus \{y\}) \cup \{x\}$ is a basis. Now since $y \in B$, we know that $I \cup \{y\}$ is independent, and clearly this would remain true with fewer elements in I. It follows that y could not have been rejected at a prior step, and so we know that y has not yet been considered. Since we are considering things in order by weight, we know that $w(y) \geq w(x)$, which implies that

$$\sum_{z \in (B \setminus \{y\}) \cup \{x\}} w(z) \leq \sum_{z \in B} w(z).$$

Therefore, the basis $(B \setminus \{y\}) \cup \{x\}$ is also optimal, and it contains $I \cup \{x\}$, so we are done. □

Theorem 9. *At the end of the algorithm I will contain an optimal basis. That is, the greedy algorithm always works.*

Proof. We have already seen that at the final step, I will be a basis. Furthermore, by the lemma, I will be contained in an optimal basis B. Since no basis in a subset of another basis, $I = B$, so I is an optimal basis. □

As another example of a greedy algorithm, consider the transversal matroids defined above. Suppose a student has a set of classes she would like to take, and each one can occur in a different time slot. It may not be possible to take all the classes, but the sets of classes which can be all taken are the independent sets of a transversal matroid. So if she has preferences between different classes, then she can find an optimal schedule by running through her classes from most to least favorite, and adding each one to the set that she is going to take, unless it cannot be added. This requires the ability to tell whether or not a given set of classes is feasible, but there are algorithms to do this. It is interesting that she only needs to rank the classes, and not to assign numerical weights to each one.

In fact, by considering the *matching* matroid on the bipartite graph associated with the classes and time slots, she could also factor in preferences between different time slots. Confusingly, however, this algorithm might ask her to compare a timeslot with a class.

Matroid duality has an interesting implication for these sorts of algorithms. We are trying to find an optimal basis, and the total weight of a basis is inversely related to the total weight of its complement. So we could also negate the weights and run the greedy algorithm to find the optimal *cobase*, and then take the complement. In the case of finding a minimal spanning tree, this would produce the following "reverse-delete" algorithm:

1. Initialize a set I to contain all of the edges.

2. Sort the edges in order of weight.

3. Run through the edges, starting with the most expensive. For each edge e, remove e from I unless this disconnects the graph (that is, makes I no longer span the whole graph).

The really astonishing property of these greedy algorithms is the fact that they *characterize* matroids, and can be used as an alternative definition. That is, suppose we have a set E, and a non-empty collection $\mathcal{F}$ of "feasible" subsets of E. We might as well assume that a subset of a feasible subset is a subset. Suppose we have a weighting function which assigns positive values to each element of E. We want to find a feasible set with maximum total weight. The greedy algorithm works by initializing a set I to be empty, sorting the elements of E, and at each step adding to I the element of greatest value among those that don't make I infeasible. Then the key result is the following (from [3], p. 276):

Theorem 10. *(Rado and Edmonds) If the greedy algorithm works for any possible set of weights, the feasible sets are the independent sets of a matroid.*

Proof. We already know that axiom (I1) holds, by assumption, so it remains to prove (I2). Suppose we have some set S, and F_1 and F_2 are maximal feasible subsets of S, but $|F_2| > |F_1|$. By assigning weights of the form $1+\epsilon_x$ to each $x \in S$, and 0 to all other elements, we can arrange that the first elements which are added to I are the elements of F_1. After this point, no more elements of S can be added, because F_1 is a maximal independent subset of S. Therefore the final feasible set will consist of elements of F_1 and elements of $E \setminus S$. Then since the weights in S are all approximately 1, and the weights outside of S are approximately 0, the weight of this final feasible set will be approximately $|F_1|$, which is less than the weight of the feasible set F_2. So the greedy algorithm failed to produce the optimal feasible set. □

Or dually, suppose we have a set E, and a non-empty collection F of "feasible" subsets of E. In this case, we might as well assume that a superset of a feasible set is also feasible. Suppose we have a weighting function that assings a positive cost to each element of E. Then the greedy algorithm will work by defining the set I to be the entire set E, and at each step, removing from I the costliest element which can be removed without losing feasibility. *If this algorithm finds an optimal solution for any set of weights, then the minimal feasible sets are the bases of a matroid on E.*

To prove that this dual algorithm works only for matroids, note that the complements of the feasible sets in the second algorithm can be taken as the feasible sets in the first algorithm, and then the two algorithms will basically do the same thing. Then the minimal feasible sets in the second algorithm are the complements of bases of a matroid M, and so are the bases of a dual matroid M^D.

8 Conclusion

Matroids seem to be fairly interesting mathematical objects, if only for the sake of novelty. They unite concepts from linear algebra, projective geometry, transversal theory, graph theory, combinatorial optimization, lattice theory, and even transcendence theory. The most distinctive feature of matroids seems to be the diversity of definitions of one concept. For example, we could roughly paraphrase some of the different definitions of a matroid as follows

- A structure for which the greedy algorithm always works.
- An intrinsic notion of coherence or acceptability, for which the maximal coherent sets are all the same size[13]
- A closure operation, where one element is in the closure of a set of others exactly when it satisfies some symmetric relationship with some of the others[14].

[13] For example, the notions of being a forest or a pseudoforest.

[14] For example, the notion of linear dependence. Any closure operation that comes from a symmetric relationship in this way will satisfy (S4).

On the surface, these notions seem totally unrelated, and it is indeed surprising that in some sense they produce exactly the same definition. It is also fascinating that as soon as a structure satisfies one set of axioms, a dozen more concepts are immediately defined on the structure, including some which may have been not at all obvious from the original structure. Since algebraic closure satisfies the closure axioms, we immediately get a notion of transcendence degree. Since maximal pseudoforests all have the same size, there's some sort of interesting closure operation associated with them.

Moreover, matroids provide a nice framework for generalizing results from graph theory and linear algebra. For example, if a theorem about a graph can be defined in terms of cycles, bases, and spanning trees, then the statement can be translated into the framework of matroids, and we can ask whether the new statement holds for all matroids, or for some interesting class of matroids. One example of a problem which was solved by generalizing from graphs to matroids was the Shannon Edge-Switching game[15][3]. In this game, two players, called SHORT and CUT, alternatively choose an edge in a graph, either contracting it or deleting it, respectively. There is also a special edge linking the source and sink, which neither player can choose. In the end, SHORT wins by connecting the source and sink (or equivalently, by spanning the designated edge), and CUT wins by preventing this. This has an obvious generalization to matroids, and we see by the characterization of duals in terms of closure, that CUT wins exactly by co-spanning the designated edge. So matroid theory reveals the symmetry between the two players: the roles of the two players are exactly dual. Moreover, matroid theory was used by Alfred Lehman to solve the game in full generality, in [4]. Only later was the solution translated back into a graph- theoretic construct, for the case of the edge-switching game. Interestingly enough, the edge-switching game includes the game GALE, which was marketed commercially as Bridg-It during the 1960s.

8.1 Limitations and Generalizations of Matroids

There are several unsatisfactory properties of matroids. One of these is the poor theory of infinite matroids. Many of the fundamental theorems about matroids rely on the assumption that the underlying set is finite. It is not clear how to generalize (I2) or (I2') to the case when the underlying set is infinite. While some of the definitions, such as the closure axioms, have obvious generalizations, the resulting structure will not necessarily have any meaningful notion of a basis or an independent set. We can handle the case of infinite matroids of finite rank, but such matroids have no theory of duality (because the complement of a finite base will always be infinite; Oxley sees duality as one of the main obstacles towards a reasonable theory of infinite matroids, [7] p. 68).

Another thing that is sometimes useful is a notion of orientation. In a graph, we might like to distinguish between two orientations of an edge, corresponding to the two directions in which we transverse it. Then we can ask meaningful questions about whether we have a directed cycle, or whether a series of edges in a path span another one in a directed way. This notion doesn't really fit into a matroid, so we must extend the matroid with additional structure, to create an "oriented matroid." This turns out to be related to the notion of the orientation of a basis in a vector space (over an ordered field). More details are in [8].

Also, the characterization of matroids in terms of greedy algorithms is a little less universal than we made it out to be. There are many sorts of algorithms which are generally seen as "greedy," but have little to do with any kind of matroid structure. One example would be Dijkstra's algorithm for finding shortest paths in a graph. By relaxing the constraints on feasible sets, and putting more requirements on the weight function, we can consider more general structures called "greedoids," of which matroids are a special class. Another type of greedoid is an "antimatroid." Like matroids, antimatroids are also associated with special semimodular lattices, as well as a special type of closure operator, one that generalizes the notion of the convex hull of a set [1].

[15]Not to be confused with the related Shannon Vertex-Switching game, which is known to be (NP-)hard to solve in full generality. This contains as an instance the well-known strategy game HEX.

References

[1] K. V. Adaricheva, V. A. Gorbunov, and V. I. Tumanov, Join-semidistributive lattices and convex geometries, *Advances in Mathematics* **173** (2003), 1-49.

[2] Garrett Birkhoff, Abstract Linear Dependence and Lattices, *American Journal of Mathematics* **57** (1935), 800-804.

[3] Eugene Lawler, *Combinatorial Optimization: Networks and Matroids*, Holt, Rhinehart and Winston, New York, 1976.

[4] Alfred Lehman, A Solution of the Shannon Switching Game, *Journal of the Society for Industrial and Applied Mathematics* **12** (1964), 687-725.

[5] Saunders MacLane, Some Interpretations of Abstract Linear Dependence in Terms of Projective Geometry, *American Journal of Mathematics* **58** (1936), 236-240.

[6] David L. Neel and Nancy Ann Neudauer, Matroids You Have Known, *Mathematics Magazine* **82** (2009), 26-41.

[7] James G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, 1992.

[8] Jürgen Richter-Gebert and Günter M. Ziegler, Oriented Matroids, (1997), Online at `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.34.990`.

[9] J. M. S. Simões-Pereira, On Matroids on Edge Sets of Graphs with Connected Subgraphs as Circuits, *Proceedings of the American Mathematical Society*, **38** (1973), 503-506.

[10] Hassler Whitney, On the Abstract Properties of Linear Dependence, *American Journal of Mathematics* **57** (1935), 509-533.

[11] Robin J. Wilson, An Introduction to Matroid Theory, *American Mathematical Monthly* **80** (1973), 500-525.

A The Matroid Definition Cheat Sheet

For a matroid on a finite set E...

(I0) $\mathcal{I}$, the collection of independent sets, is a non-empty collection of subsets of E.

(I1) A subset of an independent set is independent.

(I2) If I_1 and I_2 are independent sets, and $|I_2| > |I_1|$, then for some $x \in I_2 \setminus I_1$, $I_1 \cup \{x\}$ is independent.

(I2') If $S \subseteq E$, then all maximal independent subsets of S have the same size.

(R0) Each subset S of E is assigned a rank $\rho(S)$, which is an integer.

(R1) For any S, $0 \leq \rho(S) \leq |S|$.

(R2) For any S, T, $\rho(S) + \rho(T) \geq \rho(S \cup T) + \rho(S \cap T)$.

(B0) $\mathcal{B}$, the collection of bases, is a non-empty collection of subsets of E.

(B1) No basis is contained in another basis.

(B2) If B_1 and B_2 are bases, for every $x \in B_1 \setminus B_2$, there is some $y \in B_2 \setminus B_1$, such that $(B_1 \setminus \{x\}) \cup \{y\}$ is a basis.

(B2') If B_1 and B_2 are bases, for every $x \in B_1 \setminus B_2$, there is some $y \in B_2 \setminus B_1$, such that $(B_2 \setminus \{y\}) \cup \{x\}$ is a basis.

(C0) $\mathcal{C}$, the set of circuits, is a collection of non-empty subsets of E.

(C1) No subset of a circuit is a circuit.

(C2) If C_1, C_2 are two distinct circuits both containing some x, then $(C_1 \cup C_2) \setminus \{x\}$ contains a circuit.

(C2') If C_1, C_2 are two distinct circuits both containing some x, then $(C_1 \cup C_2) \setminus \{x\}$ is a union of circuits.

(S0) Closure is an operation $\mathrm{cl}(\cdot)$ from the subsets of E to the subsets of E.

(S1) For any S, $S \subseteq \mathrm{cl}(S)$.

(S2) For any S, $\mathrm{cl}(\mathrm{cl}(S)) = \mathrm{cl}(S)$.

(S3) If $S \subseteq T$, then $\mathrm{cl}(S) \subseteq \mathrm{cl}(T)$.

(S4) If $x \in \mathrm{cl}(S \cup \{y\}) \setminus \mathrm{cl}(S)$, then $y \in \mathrm{cl}(S \cup \{x\})$.

(I $\to$ R) The rank of a set S is the size of a maximal independent subset of S.

(I $\to$ B) A basis is a maximal independent set.

(I $\to$ C) A circuit is a minimal dependent set (i.e., a minimal not-independent set).

(R $\to$ I) An independent set is a set whose size is its cardinality, that is, $\rho(S) = |S|$.

(R $\to$ B) A basis is a set S for which $|S| = \rho(S) = \rho(E)$.

(R $\to$ B) A basis is a minimal set S for which $\rho(S) = \rho(E)$.

(R $\to$ S) The closure of a set S is the maximum set S' for which $\rho(S') = \rho(S)$, and $S' \supseteq S$.

(R $\to$ S) The closure of a set S is the set

$$\{x \in E \ : \ \rho(S \cup \{x\}) = \rho(S)\}.$$

(B $\to$ I) An independent set is a set contained in a basis.

(C $\to$ I) An independent set is a set not containing a circuit.

(C $\to$ S) The closure of a set S is the set

$$S \cup \{x \in E \ : \ S' \cup \{x\} \text{ is a circuit for some } S' \subseteq S\}.$$

(S $\to$ I) An independent set is a set I for which $x \notin \mathrm{cl}(I \setminus \{x\})$ for every $x \in I$.

(S $\to$ R) The rank of a set S is the size of the smallest subset $S' \subseteq S$ whose closure contains S.

(S $\to$ B) A basis is a minimal set B whose closure contains all of E.

A.1 Key to the Cheat Sheet

Each set of statements starting with the same letter can be taken as a definition of a matroid. Primed statements are equivalent given the other axioms in the set. Given one set of axioms, the arrowed statements serve as definitions of the other concepts in terms of the chosen one. For instance, we can take (C0), (C1), and (C2) as the matroid axioms, or alternatively, (C0), (C1), and (C2'). Either way, we would then define rank, independence, bases, and closure using the statements (C $\to$ I), (C $\to$ S), and then, say, (I $\to$ B) and (S $\to$ R). As a coherent whole, all of these statements listed here are true in every matroid.