MATROIDS

RAYHAAN PATEL

Abstract. This paper discusses matroids, a generalization of the properties of linear independence of vectors, algebraic independence of field extensions and cycles in graphs. Hassler Whitney first developed matroids in his paper *On the abstract properties of linear dependence* [Whi35]. We examine these examples and a few properties of matroids, then we look at how matroids relate to greedy algorithms in combinatorial optimization.

1. Motivation

We start by examining independence in linear algebra.

Definition 1.1. Given a vector space V over a field $\mathbb{F}$, a *linearly independent set* $S \subseteq V$ is a set of vectors such that

$$\sum_{v \in V} a_v v$$

where each $a_v \in \mathbb{F}$ implies $a_v = 0$ for all $v \in S$.

Definition 1.2. The *span* of a set of vectors $S \subseteq V$, is the set containing all linear combinations of elements of S.

That is,

$$\operatorname{span}(S) = \left\{ \sum_{v \in V} a_v v \mid v \in S,\ a_v \in \mathbb{F} \right\}.$$

If $A \subseteq \operatorname{span}(S)$, we say S *spans* A.

Example. Given a linearly independent set of vectors, S, no proper subset, $T \subset S$ spans S, otherwise $u \in S/T$ can be written as $\sum_{v \in T} a_v v = u$, so $u - \sum_{v \in T} a_v v = 0$, and if we set $a_v = 0$ for all other $v \in S$, we get a contradiction; we have shown that S is dependent.

Definition 1.3. A *basis* of a vector space V is a set of vectors $B \subseteq V$ that is linearly independent, and $\operatorname{span}(B) = V$.

Note that this implies B is a linearly independent set of vectors with maximum cardinality.

Definition 1.4. Given a matrix A, the rank of A is the dimension of the span of the column vectors of A.

Now, we look into some field theory.

Definition 1.5. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$, an element $k \in \mathbb{K}$ is *algebraic* over $\mathbb{F}$ if k is a root of some nonzero polynomial in $\mathbb{F}[x]$. If k is not algebraic over $\mathbb{F}$, we say that k is *transcendental* over $\mathbb{F}$. If k is algebraic over $\mathbb{F}$ for all $k \in \mathbb{K}$, then $\mathbb{K}$ is an algebraic extension of $\mathbb{F}$, and if there is some transcendental $k \in \mathbb{K}$ over $\mathbb{F}$, then $\mathbb{K}$ is a trancendental extension of $\mathbb{F}$.

Date: November 2025.

Definition 1.6. Let $\{k_1, k_2, \ldots, k_n\}$ be a subset of $\mathbb{K}$. Then $\mathbb{F}(k_1, k_2, \ldots, k_n)$ consists of all elements of the form $\frac{p(k_1,k_2,\ldots,k_n)}{q(k_1,k_2,\ldots,k_n)}$, where $p, q \in \mathbb{F}[x_1, x_2, \ldots, x_n]$, that is p and q are polynomials over $\mathbb{F}$ of n variables. We call an element $x \in \mathbb{K}$ *algebraically dependent* on $\{k_1, k_2, \ldots, k_n\}$ over $\mathbb{F}$ if s is algebraic over $\mathbb{F}(k_1, k_2, \ldots, k_n)$. A finite subset T of $\mathbb{K}$ is algebraically dependent over $\mathbb{F}$ if there exists some $t \in T$ such that t is algebraically dependent on $T\backslash\{t\}$. If T is not algebraically dependent over $\mathbb{F}$, it is *algebraically independent* over $\mathbb{F}$.

Given a subfield $\mathbb{F}$ of $\mathbb{K}$, we call a maximal algebraically independent subset $B \subseteq \mathbb{K}$ over $\mathbb{F}$ a *transcendence basis* of $\mathbb{K}$. Note that $\mathbb{F}(B) = \mathbb{K}$, and if we remove an element from B to get B', $\mathbb{F}(B') \subset \mathbb{K}$, which resembles the idea of span in linear algebra.

Also, graph theory has a similar notion of independence:

Definition 1.7. A *cycle* of a graph G is a finite sequence of edges, $(v_0, v_1), (v_1, v_2), \ldots, (v_n, v_0)$, where $v_0, v_1, \ldots, v_n$ are distinct elements of G.

A set of edges of G is independent if it does not contain any cycles.

Definition 1.8. A *spanning tree* of a connected graph G with n vertices is a connected subgraph of G with $n-1$ edges and n vertices.

A spanning tree cannot contain any cycles, since $n-1$ edges is the minimum number of edges that can connect n vertices, and in a cycle, $(v_0, v_1), (v_1, v_2), \ldots, (v_n, v_0)$, we can delete (v_n, v_0) and we still connect all the vertices in the cycle.

2. Matroid definition and Examples

We generalize these ideas with the notion of a matroid:

Definition 2.1. A *matroid* $\mathcal{M}$ consists of a set $E(\mathcal{M})$, called the *ground set*, paired with a set of some subsets of E, $\mathcal{I}$, called the set of *independent* sets, which satisfies the following properties:

- I-1 The empty set is independent.
- I-2 (*hereditary property*) If $A \in \mathcal{I}$, then $B \subseteq A$ implies $B \in \mathcal{I}$.
- I-3 (*independence augmentation property*) If $A, B \in \mathcal{I}$, and $|B| > |A|$, then there exists $b \in B\backslash A$ such that $A \cup \{b\} \in \mathcal{I}$.

We often consider a matroid to be the ordered pair $\mathcal{M} = (E, \mathcal{I})$, where E and $\mathcal{I}$ are the ground set and set of independent sets, respectively.

A subset of E that is not independent is called a *dependent set*.

We start by constructing matroids from our examples of independence in linear alglebra, field theory and graph theory.

Theorem 2.2. *Given a matrix A over a field $\mathbb{F}$, we let E be the set of columns vectors of A, and $\mathcal{I}$ be the the set of subsets of E that are linearly independent, $(E, \mathcal{I})$ is a matroid. We call matroids of this form* vector matroids*, and denote them by $\mathcal{M}[A]$.*

Proof. We simply check the matroid properties: the empty set of column vectors is linearly independent, and given a set of linearly independent vectors, we know that any subset is also linearly independent, so $\mathcal{M}[A]$ satisfies I-1 and I-2.

Now, we check I-3: let X and Y be linearly independent subset of E where $|X| = |Y| + 1$, and let V be the vector space spanned by $X \cup Y$. Then $\dim V \geq |X|$. If $Y \cup \{a\}$ is linearly dependent for all $a \in X\backslash Y$, then V is a subset of the span of Y, so $\dim V \leq |Y|$. This

implies $|X| \leq \dim V \leq |Y|$, so $|X| \leq |Y|$ but $|X| = |Y| + 1$, which is a contradiction. Thus, there must be some $a \in X \backslash Y$ where $y \cup \{x\}$ is linearly independent. Thus $\mathcal{M}[A]$ satisfies I-3 and is a matroid.

We also will construct matroids from graphs, with the notion of independence we described above: a set of edges of a graph G is independent if it does not contain any cycles.

Theorem 2.3. *Let $G = (V, E)$ be a graph, and let $\mathcal{I}$ be the the set of sets of edges that do not contain any cycles. Then $\mathcal{M}(G) = (E, \mathcal{I})$ is a matroid, called a* cycle matroid.

Proof. We start by constructing the *vertex-edge incidence matrix* over $\mathbb{F}_2$, A_G of G: to do this, we label each vertex and edge in G, then create a matrix with a row for each vertex and a column for each edge, label the rows and columns with their corresponding vertex and edge labels. If an edge e connects a vertex to itself (we say e is a *loop*), then column corresponding to e is the zero vector, and otherwise $a_{ij} = 1$ if the vertex i is contained in the edge j and 0 if i is not contained in j.

Now, we can show that a set X of columns of A_G is linearly dependant if and only if X contains the set of edges of a cycle of G, as this would imply that $\mathcal{M}[A_G]$ has all subsets of E that do not contain the edges of a cycle as its independent sets, meaning $\mathcal{M}[A_G] = \mathcal{M}(G)$, so $\mathcal{M}(G)$ must be a matroid. Assume that X contains a cycle C of G, if C is a loop, (making it a single edge) then its corresponding column is the zero vector, so X is linearly dependent. If C is not a loop, then each vertex in C is contained by exactly 2 edges in C, so the sum of the columns of C taken modulo 2 is the zero vector, making X lienarly dependent.

Now, assume X is a linearly dependent set of columns. Let $D \subseteq X$ be a minimal linearly dependent set (D is linearly dependent, but removing any element from D makes it linearly independent) that does not contain the zero column vector. The sum of the columns of D must be the zero vector modulo 2, so all verticies that is contained in an edge of D must be contained in at least two edges of D. Let d_1 be an edge of D, and let v_0 and v_1 be verticies contained in d_1. v_1 must be contiained by another edge, d_2 of D, and we call the other vertex contained by d_2 v_2. We can use this process create a sequence $d_1, d_2, \ldots$ of edges in D and a sequence $v_0, v_1, \ldots$ of vertices, and since G is finite, eventaully one of the vertices v in the sequence will repeat. Once this happens, we have found a cycle in D starting at v, so D contains the edges of a cycle in G, completing the proof.

Similarly, the notion of algebraic independence has a corresponding matroid:

Theorem 2.4. *Let $\mathbb{K}$ be a field and $\mathbb{F}$ be a subfield. Let E be a finite subet of $\mathbb{K}$, and $\mathcal{I}$ be the collection of subsets of E that are algebraically independent over $\mathbb{F}$, then $(E, \mathcal{I})$ is a matroid.*

We leave the proof to [Oxl11] section 6.7.

If a matroid $\mathcal{M}$ is isomorphic to some $(E, \mathcal{I})$ as described in the above theorem, then we call $\mathcal{M}$ an *algebraic matroid*.

3. Basis and Rank

Now, we generalize the idea of a basis to matroids, and define them to match the definitions of vector space bases, spanning trees and transcendence bases.

Definition 3.1. A *basis* B of a matroid $\mathcal{M}$ is an independent set with maximal cardinality, that is, $B \cup \{x\}$ is dependent for all $x \in E(\mathcal{M}) \backslash B$.

Since all bases of a vector space and all spanning trees of a graph have the same cardinality, we want to see if this applies to matroids more generally as well.

Proposition 3.2. *All bases of a matroid $\mathcal{M}$ have the same cardinality, which we call the* rank *of $\mathcal{M}$ and write as $r(\mathcal{M})$.*

Proof. Seeking a contradiction, we let B_1 and B_2 be bases such that $|B_2| > |B_1|$. By I-3, there exists $x \in B_2 \backslash B_1$ such that $B_1 \cup x$ is independent, but B_1 is a basis, so this is a contradiction. 

Corollary 3.3. *Given a field $\mathbb{F}$ and an extension $\mathbb{K}$ all finite transcendence bases have the same cardinality, called the* transcendence degree *of the extension (this is true in the infinite case as well, but involves infinite matroids)*

Proof. Given any two transcendence bases, B_1, B_2, we let $E = B_1 \cup B_2$, and consider the algebraic matroid $\mathcal{M}$ over $\mathbb{F}$ with E as its ground set. Since B_1 and B_2 are maximal algebraically independent sets, they must be bases of $\mathcal{M}$, so they have the same cardinality. We can compare any two finite transcendence bases in this way, so they all must have the same cardinality. 

Definition 3.4. The *rank function* $r : \mathscr{P}(E) \to \mathbb{N}$ of a matroid $\mathcal{M} = (E, \mathcal{I})$ is defined so that $r(X)$ is the cardinality of the largest independent set contained in A, where $A \subseteq E$

We have a generalized rank-nullity theorem for matroids:

Theorem 3.5. *Let $X, Y \subseteq E$, then*

$$r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y).$$

Proof. Let $B_\cap$ be a basis of $X \cap Y$ and let $B_\cup$ be a basis of $X \cup Y$, so $B_\cap \subseteq B_\cup$. Since $B_\cup \cap X \subseteq B_\cup$, $B_\cup \cap X$ is independent, and $r(B_\cup \cap X) = |B_\cup \cap X|$. Since $B_\cup \cap X \subseteq X$, $r(B_\cup \cap X) \leq r(X)$, and similarly $|B_\cup \cap Y| \leq r(Y)$. Thus,

$$\begin{aligned} r(X) + r(Y) &\geq |B_\cup \cap X| + |B_\cup \cap Y| \\ &= |(B_\cup \cap X) \cup (B_\cup \cap Y)| + |(B_\cup \cap X) \cap (B_\cup \cap Y)| \\ &= |B_\cup \cap (X \cup Y)| + |B_\cup \cap (X \cap Y)| \\ &= |B_\cup| + |B_\cap| \\ &= r(X \cup Y) + r(X \cap Y) \end{aligned}$$

which completes our proof. 

4. Greedy algorithms

Suppose we give the elements of the ground set of a matroid $\mathcal{M}$ an arbitrary (non-negative) weight, $w(x) : E \to \mathbb{N}$. The *matroid optimization problem* is to find a basis with maximum total weight.

Definition 4.1. The *Greedy algorithm* for the matroid optimization problem is defined as follows:

Set $B_G = \varnothing$ While B_G is not a basis, choose an element $x \in E$ such that $B_G \cup \{x\} \in \mathcal{I}$ with maximum weight.

Proof. We prove this by contradiction: let $B_G = \{g_1, g_2, \ldots, g_n\}$ be the basis returned by the greedy algorithm (it must be a basis, otherwise the algorithm would continue adding elements), where B_G is indexed by decreasing weight.

We assume there exists some basis $A = \{a_1, a_2, \ldots a_n\}$ (also indexed by decreasing weight) such that

$$\sum_{g \in B} g < \sum_{a \in A} a.$$

Let i be the smallest index such that $w(g_i) < w(a_i)$, and consider the independent sets

$$B_{i-1} = \{g_1, g_2, \ldots, g_{i-1}\} \quad \text{and} \quad A_i = \{a_1, a_2, \ldots, a_i\}$$

By I-3, there exists some $a_j \in A_i$ such that $B_{i-1} \cup \{a_j\}$ is an independent set. Since $w(a_j) \geq w(a_i) > w(g_i)$, the greedy algorithm must choose the lighter element g_i over the heavier a_j, which is a contradiction, and completes the proof.

We remark that Kruskal's algorithm is a special case of this greedy algorithm. It turns out that matroids are the *only* subset systems (a finite collection of sets that satisfies I-) where the greedy algorithm is optimal; we can define matroids as subset systems where the greedy algorithm is optimal, which appears almost entirly unrelated to our first definition based on linear independence.

Theorem 4.2. *For all subset systems S that ar not matroids, there exists a weight function w where the greedy algorithm does not return a maximum-weight set in S.*

Proof. Let $A, B \in S$ violate $I-3$: $|A| > |B|$ but for all $a \in A \backslash B$, $A \cup \{a\} \notin S$. We define the weight function $w(x)$ such that if $x \in B$, $w(x) = |B| + 2$, if $x \in A \backslash B$, $w(x) = |Y| + 1$ and $w(x) = 0$ otherwise.

The greedy algorithm will start by adding every element of Y to B_G, but since $B \cup \{a\}$ is not in S for all $a \in A \backslash B$, the greedy algorithm cannot select any elements from A, so all remaining elements have weight zero.

This gives a total weight of $|B|(|B|+2) = |B|^2 + 2|B|$, while the total weight of X must be at least $(|B|+1)^2 = |B|^2 + 2|B| + 1$, so the greedy algorithm does not return the maximum weight set in S, which completes the proof.

Acknowledgments

I would like to thank Dr. Simon Rubinstein-Salzedo and Freya Edholm for guidance in writing this paper.

References

[Oxl11] James G. Oxley. *Matroid theory*, volume 21 of *Oxf. Grad. Texts Math.* Oxford: Oxford University Press, 2nd ed. edition, 2011.

[Whi35] Hassler Whitney. On the abstract properties of linear dependence. *Am. J. Math.*, 57:509–533, 1935.