An Expository Introduction to Matroid Theory

Levi Segal

Abstract

This paper gives an expository introduction to matroid theory. Beginning with Whitney's foundational 1935 definition [1], we develop the independent-set axioms, equivalent formulations via bases, circuits, rank functions, and duality [3, 2]. We then explain how graph theory fits naturally into matroid theory through the graphic and cographic matroids. Next, we present the greedy algorithm theorem, following classical proofs from Welsh and Oxley [2, 3]. Finally, we describe modern applications involving representability, the Tutte polynomial [4], and geometric developments [5].

Contents

1 Introduction and Motivation

Matroid theory originates in Hassler Whitney's 1935 paper *On the Abstract Properties of Linear Dependence* [1], where he observed that the fundamental structure of linear independence in vector spaces and acyclic edge sets in graphs could both be captured by the same axioms.

This idea was expanded systematically in the later classical treatments of Welsh [2] and Oxley [3], who established the modern foundational framework. In both linear algebra and graph theory, we observe common concepts:

- independent sets,
- maximal independent sets (bases),
- minimal dependent sets (circuits),
- rank functions,
- and natural duality operations.

Uniting these common combinatorial properties is one of the central motivations of matroid theory [3].

2 Axiomatic Foundations of Matroids

2.1 Independent-set axioms

The following is Whitney's original definition of a matroid in terms of independent sets [1]:

Definition 2.1 (Whitney 1935)**.** A *matroid* is a pair $M = (E, \mathcal{I})$ with E finite and $\mathcal{I} \subseteq 2^E$ satisfying:

(I1) $\emptyset \in \mathcal{I}$,

(I2) if $I \in \mathcal{I}$ and $J \subseteq I$ then $J \in \mathcal{I}$,

(I3) if $I, J \in \mathcal{I}$ with $|I| < |J|$, then there exists $e \in J \setminus I$ such that $I \cup \{e\} \in \mathcal{I}$.

This axiomatizes the pattern observed in linear independence and in forests of graphs.

2.2 Examples

Example 2.2 (Vector Matroid)*.* Let E be a set of vectors in a vector space over a field F. The independent sets are the linearly independent subsets. Whitney already recognized this as one of the motivating examples [1], and it forms the backbone of modern representability theory [3].

Example 2.3 (Graphic Matroid)*.* For a graph $G = (V, E)$, let $\mathcal{I}$ be all subsets of edges that contain no cycle. This definition appears implicitly in Whitney's work and explicitly in later formalizations [2, 3]. Circuits in this matroid are exactly graph cycles.

Example 2.4 (Uniform Matroid)*.* The uniform matroid $U_{r,n}$—where independent sets are all subsets of size $\leq r$— is one of the simplest examples [3].

3 Fundamental Concepts: Bases, Circuits, Rank, and Duality

3.1 Bases

Welsh's and Oxley's treatments emphasize that basis theory provides a complete axiomatization of matroids [2, 3].

Definition 3.1. A *basis* of a matroid M is a maximal independent set.

Theorem 3.2 (Basis Exchange; Welsh–Oxley)**.** *All bases of a matroid have the same cardinality [2, 3].*

3.2 Circuits

Definition 3.3. A *circuit* is a minimal dependent set.

The circuit-elimination axiom giving an equivalent matroid definition is due to early work of Whitney and later formalized in detail by Tutte and Welsh [4, 2].

3.3 Rank function

The rank function was introduced by Whitney [1] and developed fully in modern expositions such as Oxley [3].

Definition 3.4. $r(A) = \max\{|I| : I \subseteq A,\ I \in \mathcal{I}\}$.

Proposition 3.5 (Whitney's Submodularity)**.** *The rank function of a matroid is submodular [1].*

3.4 Duality

The dual matroid M^* was formalized systematically by Tutte [4] and has become a fundamental tool in all modern treatments [3, 2].

Definition 3.6. The dual matroid M^* has bases $E \setminus B$ where B ranges over the bases of M.

Graphic/cographic duality was one of the original motivations for Tutte's work in the 1950s [4].

Example 3.7 (Computing Rank, Circuits, and Bases). Let $E = \{a, b, c, d\}$ and define independence by declaring

$$\mathcal{I} = \big\{ I \subseteq E : |I| \leq 2 \big\}.$$

This is the uniform matroid $U_{2,4}$.

Rank function: For any $X \subseteq E$,

$$r(X) = \min(|X|, 2).$$

Circuits: The minimal dependent sets are the 3-element subsets, e.g.,

$$\{a, b, c\},\ \{a, b, d\},\ \{a, c, d\},\ \{b, c, d\}.$$

Bases: Every maximal independent set has size 2, so

$$\mathcal{B} = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\}.$$

This example concretely demonstrates how rank, circuits, and bases operate within the axioms of a matroid.

Equivalent Axiom Systems

For completeness, we record here the standard equivalent ways to define a matroid in terms of bases, circuits, and rank functions; see, for example, Welsh and Oxley [2, 3]. Each of the following axiom systems determines a unique matroid structure.

Definition 3.8 (Matroid via bases)**.** Let E be a finite set and let $\mathcal{B}$ be a nonempty collection of subsets of E. We say that $(E, \mathcal{B})$ is a *matroid specified by bases* if:

(B1) All sets in $\mathcal{B}$ have the same finite cardinality.

(B2) (Basis exchange) For any $B_1, B_2 \in \mathcal{B}$ and any $x \in B_1 \setminus B_2$, there exists $y \in B_2 \setminus B_1$ such that

$$(B_1 - \{x\}) \cup \{y\} \in \mathcal{B}.$$

The sets in $\mathcal{B}$ are called the *bases*. The independent sets are precisely the subsets of bases, and this recovers an independent-set matroid in the sense of Whitney [1].

Definition 3.9 (Matroid via circuits)**.** Let E be a finite set and let $\mathcal{C}$ be a collection of nonempty subsets of E. We say that $(E, \mathcal{C})$ is a *matroid specified by circuits* if:

(C1) No member of $\mathcal{C}$ properly contains another member of $\mathcal{C}$.

(C2) (Circuit elimination) If $C_1, C_2 \in \mathcal{C}$ with $C_1 \neq C_2$ and $e \in C_1 \cap C_2$, then there exists a circuit $C_3 \in \mathcal{C}$ such that

$$C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}.$$

A subset $I \subseteq E$ is declared *independent* if it does not contain any member of $\mathcal{C}$; then $(E, \mathcal{I})$ is a matroid in the independent-set sense, and $\mathcal{C}$ is exactly the set of circuits of that matroid [2, 3].

Definition 3.10 (Matroid via rank function)**.** Let E be a finite set and let $r : 2^E \to \mathbb{Z}_{\geq 0}$ be a function. We say that (E, r) is a *matroid specified by rank* if r satisfies:

(R1) $0 \leq r(X) \leq |X|$ for all $X \subseteq E$.

(R2) If $X \subseteq Y \subseteq E$, then $r(X) \leq r(Y)$.

(R3) (Submodularity) For all $X, Y \subseteq E$,

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

A set $I \subseteq E$ is declared *independent* if $r(I) = |I|$; with this notion of independence, $(E, \mathcal{I})$ is a matroid and r is its rank function [1, 3].

Example 3.11 (A Uniform Matroid). Let the ground set be $E = \{1, 2, 3, 4\}$. The uniform matroid $U_{2,4}$ is defined by declaring a set $I \subseteq E$ independent iff $|I| \leq 2$.

Thus the independent sets are

$$\mathcal{I} = \{I \subseteq E : |I| \leq 2\},$$

and the circuits are precisely the 3-element subsets:

$$\mathcal{C} = \big\{\{i, j, k\} : i, j, k \in E\big\}.$$

The bases are all 2-element subsets of E:

$$\mathcal{B} = \big\{\{i, j\} : i \neq j,\ i, j \in E\big\}.$$

This example shows a non-graphic matroid whose structure is determined purely by cardinality constraints.

Remark 3.12 (Dual viewpoint). If M is a matroid on E specified by any of the systems above, then its dual M^* is obtained by applying the same construction to the complements of bases, the cocircuits (minimal sets meeting every basis), or the corank function $r^*(X) = |X| + r(E \setminus X) - r(E)$, respectively. Thus one can equally well view a matroid as being specified by its bases, its cobases, its circuits, its cocircuits, its rank function, or its corank function; all of these encode the same underlying structure [4, 3].

Example 3.13 (Dual of a Graphic Matroid). Let G be the triangle graph with edge set $E = \{e_1, e_2, e_3\}$ and cycle matroid $M(G)$. We saw that the bases of $M(G)$ are the 2-element subsets of E.

The dual matroid $M(G)^*$ has bases equal to the complements of bases of $M(G)$:

$$\mathcal{B}^* = \big\{E \setminus B : B \in \mathcal{B}(M(G))\big\} = \big\{\{e_1\}, \{e_2\}, \{e_3\}\big\}.$$

Since bases of size 1 correspond to rank 1, the circuits of $M(G)^*$ are the 2-element subsets:

$$\mathcal{C}^* = \big\{\{e_i, e_j\} : i \neq j\big\}.$$

Thus in the dual, the "cycles" become "cuts": removing any one edge disconnects the graph minimally. This example demonstrates explicitly how matroid duality interchanges circuits and cocircuits.

4 Matroids and Graph Theory

Graph theory provides some of the most accessible and important examples of matroids. In particular, graphic matroids $M(G)$ and cographic matroids $M^*(G)$ show how the abstract notion of independence in a matroid can appear naturally in a familiar setting. These ideas trace back to Whitney's original paper [1] and were later developed further by Tutte in his work on graph invariants [4]. Because of this history, the connection between graphs and matroids forms one of the foundations of the subject [3, 2].

4.1 Graphic and Cographic Matroids

Given a graph G, the graphic matroid $M(G)$ is defined by taking the edges of G as the ground set, and declaring a set of edges to be independent if it does not contain a cycle. In this framework, the circuits of $M(G)$ are exactly the simple cycles of the graph. This example is often one of the first indications that matroids capture the structure of independence beyond linear algebra.

The corresponding dual construction produces the cographic matroid $M^*(G)$. Here, the circuits are minimal edge cuts, also known as bonds. While the graphic matroid emphasizes how edges combine to form cycles, the cographic matroid focuses on how removing certain edges can disconnect the graph. Whitney and Tutte showed that this dual relationship reflects deeper structural connections in graph theory [1, 4].

This duality helps explain why spanning trees, cuts, and flows in graphs are closely related. For instance, spanning trees correspond to bases in $M(G)$, while minimal cuts correspond to circuits in $M^*(G)$.

Example 4.1 (A Graphic Matroid). Consider the graph G consisting of a triangle with vertex set $V = \{1, 2, 3\}$ and edge set

$$E = \{e_1 = (1, 2), \quad e_2 = (2, 3), \quad e_3 = (3, 1)\}.$$

The graphic matroid $M(G)$ is defined on ground set E.

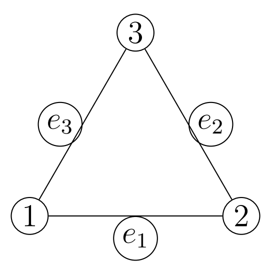

Figure 1: The graph G with vertices $\{1, 2, 3\}$ and edges $e_1 = \{1, 2\}, e_2 = \{2, 3\}, e_3 = \{3, 1\}$ used in the graphic matroid example.

Independent Sets. A set of edges is independent iff it contains no cycle. Thus:

$$\mathcal{I}(M(G)) = \{\emptyset, \{e_1\}, \{e_2\}, \{e_3\}, \{e_1, e_2\}, \{e_2, e_3\}, \{e_1, e_3\}\}.$$

Circuits. The only cycle in G is the 3-cycle, so:

$$\mathcal{C}(M(G)) = \{\{e_1, e_2, e_3\}\}.$$

Bases. A base is any maximal acyclic subset, i.e. any spanning tree. Thus every 2-element subset is a base:

$$\mathcal{B}(M(G)) = \{\{e_1, e_2\}, \{e_2, e_3\}, \{e_1, e_3\}\}.$$

Rank. The rank is the size of any base:

$$r(M(G)) = 2.$$

Dual Matroid. Since G is a 3-cycle, the dual matroid $M(G)^*$ is the uniform matroid

$$M(G)^* = U_{1,3},$$

whose bases are the singletons. This example illustrates the correspondence:

$$B \text{ is a base of } M \quad \Longleftrightarrow \quad E \setminus B \text{ is a base of } M^*.$$

4.2 Graphoids

The term *graphoid* is used in the combinatorial literature to describe matroids that arise from graph-related constructions, even when they do not come directly from a standard graph. One example is the bicircular matroid, where a set of edges is independent if each connected component contains at most one cycle. Oxley includes graphoids when discussing broader classifications of matroid families [3].

Graphoids illustrate how graphical structure can extend beyond ordinary graphs while still producing meaningful matroidal behavior. They clarify the boundary between matroids that are genuinely graphic and those that only share certain graphical properties. This makes them useful in understanding how graph theory influences the development of matroid theory more generally.

5 The Greedy Algorithm Theorem

This theorem is one of the most important foundational results in matroid theory, proved in several classical texts including Welsh [2] and Oxley [3].

Theorem 5.1 (Greedy Algorithm Theorem)**.** *Let $M = (E, \mathcal{I})$ be a matroid and let $w : E \to \mathbb{R}$ be a weight function. Order the elements of E so that $w(e_1) \geq w(e_2) \geq \cdots \geq w(e_m)$, and let the greedy algorithm construct*

$$I_0 = \varnothing, \qquad I_i = \begin{cases} I_{i-1} \cup \{e_i\}, & \text{if } I_{i-1} \cup \{e_i\} \in \mathcal{I}, \\ I_{i-1}, & \text{otherwise.} \end{cases}$$

Let $I_g = I_m$. Then I_g is a maximum–weight independent set of M.

Proof. The set I_g is independent by construction. Let $J \in \mathcal{I}$ be any independent set. We show that $w(I_g) \geq w(J)$.

List the elements chosen by the greedy algorithm in the order added:

$$I_g = \{f_1, \dots, f_k\}.$$

We will construct sets

$$J_0, J_1, \dots, J_k$$

such that: (i) $J_0 = J$; (ii) each J_i is independent; (iii) $|J_i| = |J|$; (iv) $\{f_1, \dots, f_i\} \subseteq J_i$; (v) $w(J_i) \geq w(J_{i-1})$.

Assume J_{i-1} has been constructed. If $f_i \in J_{i-1}$, set $J_i = J_{i-1}$.

If $f_i \notin J_{i-1}$, then since the greedy algorithm added f_i, the set $I_{i-1} \cup \{f_i\}$ is independent. Because all maximal independent sets in a matroid have the same size and $|I_{i-1}| \leq |J_{i-1}|$, the augmentation property applied to I_{i-1} and J_{i-1} implies that there exists $x \in J_{i-1} \setminus I_{i-1}$ such that

$$(J_{i-1} \setminus \{x\}) \cup \{f_i\} \in \mathcal{I}.$$

Define

$$J_i = (J_{i-1} \setminus \{x\}) \cup \{f_i\}.$$

Then J_i is independent and $|J_i| = |J_{i-1}|$.

Since the elements are processed in nonincreasing weight order, every element that could have been added at step i has weight at most $w(f_i)$. In particular, $w(f_i) \geq w(x)$, so

$$w(J_i) = w(J_{i-1}) - w(x) + w(f_i) \geq w(J_{i-1}).$$

Thus J_i satisfies all required properties.

After k steps we obtain J_k, which contains all of I_g and has the same size as J. Since all maximal independent sets of a matroid have the same cardinality, it follows that $J_k = I_g$. Therefore

$$w(I_g) = w(J_k) \geq w(J_0) = w(J).$$

Since J was arbitrary, I_g has maximum weight among all independent sets. □

[2].

6 Modern Applications

6.1 Representability

One really important question in matroid theory is whether a matroid actually comes from linear algebra. A matroid is called *representable over a field* $\mathbb{F}$ if you can label its elements with vectors in $\mathbb{F}^n$ so that a set is independent in the matroid exactly when the corresponding vectors are linearly independent. Whitney first noticed this connection [1], but the modern theory mostly comes from Oxley [3].

What makes representability interesting is that it depends a lot on which field you use. For example, the Fano matroid F_7 works over $\mathbb{F}_2$, but not over $\mathbb{R}$. The non-Fano matroid is the opposite. So it is not just a yes/no property—different fields give different answers. This was surprising to me because I originally thought linear independence would behave the same everywhere, but it definitely does not.

A major idea in this area is using *excluded minors* to understand representability. One famous result is:

Theorem 6.1 (Tutte)**.** *A matroid is representable over $\mathbb{F}_2$ if and only if it has no $U_{2,4}$ minor.*

This basically means that there is one small matroid, $U_{2,4}$, that blocks binary representability. If your matroid contains it, then it cannot come from vectors over $\mathbb{F}_2$. I think this kind of "forbid one configuration and everything works" result is really cool.

There is also a huge conjecture by Rota that said every finite field should have a *finite* list of excluded minors that characterize representability over that field. This was proven recently, which is a big deal, even though we still do not actually know what the lists are. It shows that representability has a deeper structure than people expected.

Representability connects matroids to other areas too. In coding theory, linear codes are basically representable matroids, and things like minimum distance relate to dependent sets. In network coding, whether you can send information efficiently sometimes depends on whether a certain matroid is representable over a field. So these ideas actually show up in real communication systems.

6.2 The Tutte Polynomial

The Tutte polynomial was introduced by W. Tutte [4] while studying graph colorings, but later people realized it works for matroids too. It is defined for a matroid M by

$$T_M(x, y) = \sum_{A \subseteq E} (x-1)^{r(E)-r(A)}(y-1)^{|A|-r(A)}.$$

At first this formula looks pretty overwhelming, but the surprising thing is how much information it contains. A bunch of different combinatorial ideas that used to seem unrelated all turn out to be special cases of the Tutte polynomial [2, 3].

One of the main tools for working with $T_M(x, y)$ is the *deletion–contraction* rule. If e is not a loop or a coloop, then

$$T_M(x, y) = T_{M \setminus e}(x, y) + T_{M/e}(x, y).$$

If e is a loop or a coloop, the formulas become

$$T_M(x, y) = y\, T_{M \setminus e}(x, y) \quad \text{(loop)}, \qquad T_M(x, y) = x\, T_{M/e}(x, y) \quad \text{(coloop)}.$$

These rules let you break down a matroid step by step, which feels a lot like simplifying a problem by removing one element at a time. This is a big reason why the Tutte polynomial shows up everywhere in combinatorics.

For graphs, the Tutte polynomial gives several famous results in one framework. If $M(G)$ is the cycle matroid of a graph G, then:

- the number of spanning trees of G is $T_{M(G)}(1, 1)$,

- the chromatic polynomial comes from

$$\chi_G(\lambda) = (-1)^{|V|-k(G)}\lambda^{k(G)}T_{M(G)}(1-\lambda, 0),$$

- flow and tension polynomials, and network reliability, are also evaluations of $T_{M(G)}(x, y)$.

So instead of having separate formulas for all these things, the Tutte polynomial explains them all at once.

What I really like is that the Tutte polynomial still works even when there is no graph picture at all. In coding theory, certain weight enumerators of linear codes can be written using Tutte-like polynomials. In statistical physics, the partition function of the Potts model turns out to be an evaluation of the Tutte polynomial along a curve in the (x, y)–plane. So ideas from physics can actually answer combinatorial questions and vice versa.

Overall, the Tutte polynomial shows how one idea can connect a ton of different areas. Something that started as a tool for graph colorings now links combinatorics, coding theory, and even physics [4, 2, **?**]. To me, this really shows the unifying power of matroid theory.

6.3 Geometry and Matroids

At first, matroids feel very combinatorial, since they are all about independence sets and circuits. But in the last couple of decades, people have realized that matroids actually have really interesting geometric structures attached to them (see surveys by Ardila [5]). Two of the main ones are *matroid polytopes* and *Bergman fans*.

A matroid polytope is a shape in high-dimensional space where each vertex represents a basis of the matroid. Even though that sounds abstract, it gives a way to study matroids using geometry. For example, properties like exchanges between bases show up as edges in the polytope. This means that questions about independence and structure can sometimes be answered by looking at the geometry of the polytope instead of working purely combinatorially. I think this is really cool because it turns a discrete object into something you can visualize (at least in lower dimensions).

The other major geometric object is the *Bergman fan* of a matroid. This comes from tropical geometry, which basically replaces usual addition and multiplication with min and +, creating a kind of "piecewise linear" version of geometry. The Bergman fan captures all possible ways a linear space can degenerate, and it turns out that matroids describe exactly the combinatorial patterns behind those degenerations. So a Bergman fan lets us see how a matroid behaves like a tropical variety, which is a big idea in modern algebraic geometry.

One of the most shocking results in this area is that matroids satisfy analogues of the *hard Lefschetz theorem* and the *Hodge–Riemann relations*. These are extremely deep results in algebraic geometry that originally applied to smooth projective varieties. The fact something as combinatorial as matroids had similar properties to geometric objects was very suprising.

7 Conclusion

Matroid theory provides a unifying lens through which independence phenomena in algebra, graph theory, and optimization can be understood. From Whitney's original axioms [1] to

Tutte's duality and invariants [4], through the classical textbooks of Welsh and Oxley [2, 3], and finally to modern developments in geometry [5], matroids continue to offer a powerful framework.

References

[1] H. Whitney, "On the Abstract Properties of Linear Dependence," *American Journal of Mathematics*, 57(3):509–533, 1935.

[2] D. J. A. Welsh, *Matroid Theory*. Academic Press, 1976.

[3] James Oxley, *Matroid Theory*. Oxford University Press, 2011.

[4] W. T. Tutte, "A Contribution to the Theory of Matroids," *Canadian Journal of Mathematics*, 4:13–28, 1952.

[5] Federico Ardila, "Matroid Theory: Connections to Geometry and Beyond," various lecture notes and survey articles.