MATROID THEORY

RICHARD MAI

Introduction

Matroid theory is a branch of combinatorics that studies an abstract notion of independence, generalizing concepts from linear algebra and graph theory. In linear algebra, we say a set of vectors is independent if none of them is a linear combination of the others; in graph theory, a set of edges is independent (an acyclic set) if it contains no cycles (i.e. it forms a forest). Matroids capture the common essence of these notions. In fact, matroids were introduced by Hassler Whitney in 1935 as a way to axiomatize the concept of independence that arises in both graphs and matrices [1]. A matroid can be thought of as the most general kind of structure in which ideas like rank, basis, and linear independence make sense, even outside the usual settings of vector spaces or graph connectivity [6]. This unifying perspective has made matroid theory a fundamental tool in combinatorics, with applications in optimization, network theory, geometry, and coding theory [6].

In this expository paper, we introduce the basic theory of matroids, focusing on their internal structure: the fundamental definitions, core concepts (such as independent sets, bases, circuits, rank, and duality), and a few key theorems. We will illustrate these ideas with examples that should be accessible to students familiar with graphs, sets, and introductory linear algebra. (Applications of matroids will be mentioned only briefly near the end.) Our goal is to convey both the formal definitions and the intuitive meaning of matroids in an engaging way. We encourage the reader to keep in mind two running examples while reading: one from graph theory (forests in a graph) and one from linear algebra (independent sets of vectors). These will help ground the abstract definitions in familiar terms.

Definitions and Axioms

There are several equivalent ways to define a matroid. We will start with the independent set definition, which is often the easiest to grasp intuitively. Later, we will discuss alternative but equivalent descriptions (in terms of bases, circuits, and rank).

Formally, a matroid M is an ordered pair $(E, \mathcal{I})$ where:

- E is a finite set, called the ground set of the matroid. The elements of E can be thought of as the "building blocks" of the structure (for example, E might be a set of vectors, or a set of edges in a graph).
- $\mathcal{I}$ is a collection of subsets of E, called the independent sets, which satisfies the following axioms:

(I1) **Non-emptiness:** The empty set is independent ($\varnothing \in \mathcal{I}$) [6].

Date: December 8, 2025.

(I2) **Hereditary property:** Every subset of an independent set is independent. In other words, if $A \in \mathcal{I}$ and $A' \subseteq A$, then $A' \in \mathcal{I}$ [6]. This reflects the idea that removing elements from an independent set cannot create a dependency.

(I3) **Exchange (augmentation) property:** If A and B are independent sets and $|A| > |B|$, then there exists at least one element $x \in A \setminus B$ such that $B \cup \{x\}$ is also independent [6]. In words, if one independent set A is larger than another independent set B, we can exchange some element of A into B and still have an independent set. This axiom ensures a kind of "stepping up" property, reminiscent of how one can extend a smaller linearly independent set by adding a vector from a larger independent set in linear algebra.

These three axioms are the defining properties of a matroid in terms of independent sets. Axiom (I1) is usually trivial (it just asserts that $\mathcal{I}$ is not empty; note that by (I2) it then follows that $\emptyset$ is independent). Axiom (I2) says that $\mathcal{I}$ is downward-closed, meaning independence is preserved under taking subsets (this is also known as the hereditary property [6]). Axiom (I3), the exchange property, is the most characteristically matroidal condition: it captures the idea that all maximal independent sets in a matroid have a certain uniformity, and one can move from one independent set to another by swaps. Indeed, (I3) implies that any independent set can be expanded to a maximal one by adding elements, and importantly, it implies that all maximal independent sets have the same size (we will prove this shortly) [7].

Example (Vector independence). To see these axioms in action, consider E to be a set of vectors in $\mathbb{R}^n$. We can take $\mathcal{I}$ to be the collection of all linearly independent subsets of E. Then $(E, \mathcal{I})$ is a matroid (often called a vector matroid or representable matroid) [7]. Axioms (I1)–(I3) correspond to basic facts from linear algebra: (I1) $\emptyset$ is independent (vacuously). (I2) Any subset of a linearly independent set is independent (removing vectors cannot introduce a linear dependence). (I3) If A and B are two sets of vectors with A larger than B, one of the vectors in A can be added to B while preserving independence — essentially a version of the Steinitz exchange lemma from linear algebra. Thus, vector spaces provide a rich source of matroids (we will formalize this example later).

Example (Acyclic subgraphs). Similarly, let E be the edge set of a graph G. Define $\mathcal{I}$ to be the collection of all subsets of E that contain no cycles (i.e. all forests in G). Then $(E, \mathcal{I})$ is a matroid, known as the graphic matroid of G [7]. Verifying the axioms: (I1) $\emptyset$ (no edges) is certainly acyclic. (I2) Any subset of an acyclic set of edges is acyclic (removing edges cannot create a cycle). (I3) If A is a larger acyclic set than B, then A has more edges than B; to extend B, we can add some edge from A that is not in B – since A has no cycles, adding any edge from A that is outside B will not create a cycle in B (one can give a more rigorous graph-theoretic proof of the exchange property, but intuitively it holds because A being larger means it spans more of the graph without cycles, so we can always add some edge from A to B without creating a cycle). In fact, the exchange axiom in graphic matroids is closely related to the fact that all spanning trees of a connected graph have the same number of edges.

Bases and Rank

A subset of the ground set E is called independent if it belongs to $\mathcal{I}$. By definition, an independent set that is not contained in any larger independent set is called maximal independent. In matroid terminology, a maximal independent set is called a *basis* of the matroid. Every matroid has at least one basis (by taking any maximal independent set, which exists by a simple greedy argument using (I3)). One of the fundamental theorems of matroid theory is that all bases in a matroid have the same size. This common size is referred to as the *rank* of the matroid.

We state this result formally:

Theorem (Basis Exchange). In any matroid $M = (E, \mathcal{I})$, all bases have the same cardinality. Moreover, given any two bases B_1 and B_2, one can exchange elements between them: for every $b_1 \in B_1 \setminus B_2$, there exists some $b_2 \in B_2 \setminus B_1$ such that $(B_1 - \{b_1\}) \cup \{b_2\}$ is also a basis [7].

Sketch of Proof. The second part of this statement (often called the basis exchange property) is actually another equivalent axiom system for matroids [7]. Assuming (I1)–(I3), one can prove it as follows: let B_1 and B_2 be two bases. If $B_1 = B_2$ there is nothing to show. If not, pick any element $b_1 \in B_1 \setminus B_2$. Since B_1 is independent and larger than $B_2 \setminus \{b_1\}$, by (I3) there exists some $x \in B_1 \setminus (B_2 \setminus \{b_1\})$ (so either $x = b_1$ or $x \in B_1 \setminus B_2$) that can be added to $B_2 \setminus \{b_1\}$ to form an independent set. Obviously x cannot be b_1 itself (removing b_1 and then adding it back does nothing), so x is in $B_1 \setminus B_2$. Thus $(B_2 \setminus \{b_1\}) \cup \{x\}$ is an independent set containing $B_2 \setminus \{b_1\}$ plus one extra element x. But B_2 was a basis (maximal independent), so B_2 cannot be extended by any element; the only way $(B_2 \setminus \{b_1\}) \cup \{x\}$ can be independent is if x replaced b_1 – that is, x must lie in B_2 already. This x is our b_2. So for each $b_1 \in B_1 \setminus B_2$, we found an element $b_2 = x \in B_2 \setminus B_1$ that we can swap. By symmetry, the same holds swapping the roles of B_1 and B_2. This proves the exchange property (B2).

Setting aside the formal proof, the intuition is: you can "trade" elements between any two bases and still end up with a basis [7]. Now, to see that all bases must have the same number of elements, consider applying the exchange property repeatedly: if $|B_1| > |B_2|$, then for each extra element in B_1 you can exchange with an element in B_2, suggesting B_2 can be enlarged — a contradiction since B_2 is maximal independent. Thus $|B_1|$ cannot exceed $|B_2|$, and by symmetry $|B_2|$ cannot exceed $|B_1|$. We conclude $|B_1| = |B_2|$.

This number is an important invariant of the matroid:

Definition (Rank). The rank of a matroid M, denoted $r(M)$, is the size of any (hence every) basis of M [7]. More generally, for any subset $X \subseteq E$, the rank $r(X)$ is defined as the size of the largest independent subset of X [7]. In other words,

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

By this definition, the rank of the entire ground set E (denoted simply $r(E)$) equals $r(M)$, the size of a basis.

The rank function $r(\cdot)$ provides a convenient numerical measure of the "independence capacity" of any subset. It satisfies a few useful properties:

(1) **Monotonicity:** If $X \subseteq Y \subseteq E$, then $r(X) \leq r(Y)$ (adding more elements cannot decrease the maximum independent size) [7].

(2) **Upper bound:** For any $X \subseteq E$, obviously $r(X) \leq |X|$, since an independent subset of X cannot be larger than X itself.

(3) **Submodularity:** For any two subsets $X, Y \subseteq E$, one can show

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

an inequality that says the rank function is submodular. Submodularity is a bit advanced, but it generalizes the fact that in linear algebra, $\dim(U) + \dim(W) \geq$

$\dim(U+W)+\dim(U\cap W)$ for subspaces U, W. We will not prove these properties here, but they all follow from the matroid axioms (in fact, one could define a matroid as any set function $r : 2^E \to \mathbb{Z}_{\geq 0}$ satisfying certain axioms analogous to these properties [7]).

Example. In the graphic matroid of a graph G, a basis corresponds to a spanning forest of G (a maximal acyclic set of edges). For a connected graph, a spanning forest is just a spanning tree. Thus the rank of the graphic matroid is $r(M) = |V| - c$, where $|V|$ is the number of vertices in G and c is the number of connected components (since a spanning forest has $|V| - c$ edges) [7]. More generally, the rank $r(X)$ of a subset of edges X is $|V| - \kappa(X)$, where $\kappa(X)$ is the number of connected components in the subgraph that X spans [7]. This is analogous to linear algebra: think of $|V|$ as the "dimension" of the ambient space (for graphs, the number of vertices plays a similar role) and each independent edge reduces the number of components by 1.

Example. In a vector matroid (where E is a set of vectors in some vector space), a basis is just a basis of the vector space spanned by E (or by those vectors) in the linear algebra sense. For instance, if E is a set of column vectors, a basis of the matroid might consist of some of those columns forming a full-rank submatrix. The rank of the matroid $r(M)$ in this case equals the dimension of the subspace spanned by all vectors in E, and the rank $r(X)$ of a subset X is the dimension of the subspace spanned by X [7]. This is exactly the usual definition of the rank of a set of vectors.

Circuits and Dependence

Just as bases are the maximal independent sets, one can define circuits to be the minimal dependent sets in a matroid. A dependent set means a subset of E that is not independent (not in $\mathcal{I}$). A circuit is a dependent set such that every proper subset of it is independent [7]. In other words, a circuit is a minimal configuration of elements that contains a dependence. If any one element is removed from a circuit, the remainder becomes independent, but the full set is dependent.

Definition (Circuit). A circuit of a matroid $M = (E, \mathcal{I})$ is a subset $C \subseteq E$ such that $C \notin \mathcal{I}$ (it is dependent), but every proper subset of C is in $\mathcal{I}$ (it is minimal dependent) [7]. The collection of all circuits of M is often denoted $\mathcal{C}$.

Because circuits represent the "primitive" dependent sets, they satisfy their own axioms dual to (I1)–(I3). For example, one can show:

- There is no circuit that properly contains another (by minimality) [7].
- If C_1 and C_2 are two distinct circuits and they share an element x, then there is a circuit contained in $(C_1 \cup C_2) \setminus \{x\}$ [7]. This is known as the circuit elimination axiom (essentially, two different minimal dependences can be "combined" to form another dependence after removing the common element).

The circuit elimination property is a bit advanced, but it has a nice interpretation in graphs and linear algebra. In a graph, circuits correspond to simple cycles [8]. The elimination axiom for circuits then says: given two distinct cycles in a graph that share an edge, you can "break" the cycles and find another cycle that lies in the union of those two cycles (indeed, in graph theory, the union of two cycles that share at least one edge will contain another cycle once that common edge is removed). In linear algebra, circuits correspond to minimal linearly dependent sets of vectors (for example, a circuit might be a set of $k+1$ vectors in

$\mathbb{R}^n$ that have the unique linear relation $a_1 v_1 + \cdots + a_{k+1} v_{k+1} = 0$). The elimination axiom in that context reflects the ability to eliminate one of the vectors in a linear dependence and still have a dependence among the others.

A useful relationship between circuits and bases is: a set $B \subseteq E$ is a basis if and only if B has no circuits (i.e. it is maximally independent), and equivalently B has the property that adding any element $e \in E \setminus B$ to B creates exactly one circuit (a dependent cycle) within $B \cup \{e\}$. This again parallels graphs (a spanning tree B has no cycles, but adding any new edge creates exactly one cycle) and linear algebra (a basis has no dependencies, but adding any new vector creates exactly one dependency relation among the extended set).

Duality of Matroids

One of the most beautiful aspects of matroid theory is the notion of a dual matroid. Matroid duality generalizes the duality between spanning trees and cuts in graphs, and the duality between subspaces and quotient spaces (or orthogonal complements) in linear algebra [10]. Intuitively, the dual matroid M^* of a matroid M is formed by declaring the complements of bases of M to be bases of M^*. What was independent in M becomes "co-dependent" in M^* and vice versa.

Definition (Dual Matroid). Let $M = (E, \mathcal{I})$ be a matroid on ground set E with collection of bases $\mathcal{B}$. The dual matroid $M^* = (E, \mathcal{I}^*)$ is defined as follows: a set $B \subseteq E$ is a basis of M^* if and only if $E \setminus B$ is a basis of M [7]. Equivalently,

$$\mathcal{B}^* = \{E \setminus B : B \in \mathcal{B}\}.$$

From this definition, it follows that a set is independent in M^* (i.e. belongs to $\mathcal{I}^*$) if and only if its complement in E contains a basis of M. In particular, the empty set is independent in M^* if and only if E contains a basis of M (which it does, trivially), so $\emptyset \in \mathcal{I}^*$ as needed. One can check that M^* is indeed a matroid; the base exchange axiom is self-dual, so the collection of complements of bases will satisfy the exchange property [6].

What does duality mean for rank? If $r(X)$ is the rank of subset X in M, and $r^*(X)$ is the rank in M^*, one can derive a simple relation:

$$r^*(X) = |X| - r(E) + r(E \setminus X).$$

In particular, taking $X = E$, we get

$$r^*(E) = |E| - r(E) + r(\emptyset) = |E| - r(M),$$

since $r(\emptyset) = 0$ by convention [7]. Thus the rank of the dual matroid M^* is $r(M^*) = |E| - r(M)$. This is analogous to linear algebra: if a subspace has dimension r, its orthogonal complement (in an ambient space of dimension $|E|$) has dimension $|E| - r$. Also, if B is a basis of M (so $|B| = r(M)$), then its complement $E \setminus B$ is a basis of M^* (and $|E \setminus B| = |E| - r(M) = r(M^*)$), consistent with the rank formula [7].

From the definition, one can also describe the circuits of the dual matroid. A *cocircuit* of M is defined as a circuit of the dual matroid M^*. It turns out that cocircuits of M are exactly the complements of hyperplanes of M (where a hyperplane is a maximal proper subset of E that is not spanning, or equivalently a subset H with $r(H) = r(M) - 1$). In more concrete terms: in a graph, circuits (cycles) of the graphic matroid $M(G)$ correspond to fundamental cycles, whereas the cocircuits in $M(G)$ correspond to minimal cuts (also called bonds) in the graph [7]. This matches the duality between cycles and cuts in planar graphs: for a planar graph G, the cycle matroid of the dual graph G^* is the dual matroid of the cycle matroid of G [7]. In fact, Whitney's planar graph criterion (1933) states that a graph G is planar if and only if the dual of its cycle matroid $M(G)$ is graphic (i.e. is itself the cycle matroid of some graph) [7]. If G is planar, $M(G)^* = M(G^*)$, where G^* is the planar dual graph [7]. This is a beautiful interplay between graph theory and matroid duality.

To summarize: duality provides a way to derive a new matroid from a given matroid by essentially swapping the roles of independent and dependent sets (more precisely, swapping bases with complements of bases). The dual of a matroid is unique and involutive, meaning $(M^*)^* = M$. Some matroids are self-dual (isomorphic to their duals), though that is a special property (analogous to a planar graph being self-dual in graph theory, or a vector space being isomorphic to its dual space with a pairing).

Examples of Matroids

We have already encountered a few key examples during the definitions. Let us summarize and add a couple more examples to broaden our perspective:

Graphic Matroids For a graph $G = (V, E)$, the matroid $M(G) = (E, \mathcal{I})$ is defined by $\mathcal{I} = \{\text{subsets of } E \text{ that contain no cycle}\}$. We saw that bases of $M(G)$ are spanning forests (spanning trees if G is connected), and the rank is

$$r(M(G)) = |V| - (\text{number of components of } G).$$

Circuits in $M(G)$ correspond to simple cycles in G [8]. The dual matroid $M(G)^*$ has as its circuits the minimal cuts (bonds) of G [7], and if G is planar, $M(G)^*$ is itself graphic (in fact $M(G)^* = M(G^*)$ as mentioned).

Example: If G is a cycle graph C_4 (a 4-cycle), then $M(G)$ is essentially the uniform matroid $U_{3,4}$ (any 3 of the 4 edges can be chosen without creating a cycle, but all 4 together form a circuit).

Figure: The cycle graph C_4 (left) and its graphic matroid represented as a uniform matroid $U_{3,4}$ (right). The independent sets are all subsets of edges of size at most 3 (listed as I_0 through I_{14}), while the only dependent set of full size 4 is the circuit (the 4-cycle itself).

Linear (Vector) Matroids As discussed, any finite set of vectors $E = \{v_1, \ldots, v_n\}$ in a vector space (over a field $\mathbb{F}$) defines a matroid $M = (E, \mathcal{I})$ where $\mathcal{I}$ consists of all linearly independent subsets of E [7]. This matroid is often denoted $M[A]$ if the vectors are taken as columns of a matrix A. Such a matroid is called *representable* (or $\mathbb{F}$-representable to specify the field). Bases in this matroid correspond to bases of the subspace spanned by E. The rank function $r(X)$ for $X \subseteq E$ is $\dim(\text{span}(X))$, the dimension of the subspace spanned by X [7].

Not every abstract matroid is representable as a vector matroid, but many important ones are. For instance, all graphic matroids are representable over $\mathbb{F}_2$ (the field of two elements) [7] — essentially because a cycle (mod 2) is a linear relation mod 2 between edges in a graph's incidence matrix. An example of a non-representable matroid (over any field) is more difficult to give in elementary terms; it requires more advanced combinatorial configurations. But one simpler example of a matroid that is not representable over a particular field is the uniform matroid $U_{2,4}$, which cannot be represented over $\mathbb{F}_2$ (though it can be over $\mathbb{F}_3$) [7].

Uniform Matroids The uniform matroid $U_{k,n}$ is defined on an n-element set $E = \{1, 2, \ldots, n\}$ by declaring a subset $X \subseteq E$ to be independent if and only if $|X| \leq k$. In other words, any set of up to k elements is independent, but any set of $k+1$ or more elements is dependent (so the circuits are exactly the subsets of size $k+1$, and there are no other dependences) [7]. This clearly satisfies the matroid axioms (it basically abstracts the idea of a bound on dimension or cycle length). The rank of $U_{k,n}$ is k (since any k-subset is independent but the whole set of size n is not if $n > k$). We have seen a special case: $U_{3,4}$ in the example of C_4 above. $U_{n,n}$ is just the free matroid (no dependencies at all, everything is independent), while $U_{0,n}$ is the trivial matroid (only the empty set is independent, everything else is dependent). These are extreme cases. Uniform matroids are very simple in structure, yet they play a role in examples and counterexamples (and as building blocks for more complicated matroids).

Partition Matroids A partition matroid is a generalization of the uniform matroid. Suppose the ground set E is partitioned into disjoint subsets (blocks) $E = E_1 \cup E_2 \cup \cdots \cup E_t$. Fix some nonnegative integers $k_1, k_2, \ldots, k_t$. A set $X \subseteq E$ is defined to be independent if and only if $|X \cap E_i| \leq k_i$ for each $i = 1, 2, \ldots, t$. In other words, you can take at most k_i elements from block E_i. It is easy to verify that this defines a matroid (the exchange property can be checked by considering exchanges within each block). Partition matroids are useful to model certain scheduling or assignment problems, and they too are representable (over a large enough field, one can create a diagonal block matrix to realize the constraints). The uniform matroid $U_{k,n}$ is the special case where the entire ground set is one block (of size n) with $k_1 = k$.

Transversal Matroids A transversal matroid (also known as a Hall matroid) is constructed from a bipartite graph or a set system. We mention it for completeness, though it is a bit more involved than the above examples. Take a bipartite graph with bipartition (X, Y) where X is our ground set of “left vertices” (as elements of the matroid). Suppose we have some family of subsets of Y that X can match into. The independent sets of the transversal matroid are those subsets $A \subseteq X$ that can be matched to distinct neighbors in Y (i.e. A is contained in the neighborhood of some matching). This matroid captures Hall’s marriage theorem in its structure. Transversal matroids are a well-studied class; they are precisely the matroids that are representable as intersections of partition matroids. We will not delve further into this example, but it is an interesting link between matchings in graphs and matroid theory [8].

Properties and Theorems

We have already touched on some fundamental properties in the discussion above (like the basis exchange theorem). There are many important theorems in matroid theory, but we will highlight just a few that underscore the theory’s elegance, especially those relevant to an introduction.

Greedy Algorithm Optimality A matroid is exactly the kind of structure on which the greedy algorithm always produces an optimal solution for selecting a largest (or maximum-weight) independent set. This is known as the Greedy Algorithm Theorem (or Rado–Edmonds theorem). In practical terms, if you assign weights to elements of a matroid, the greedy strategy of iteratively picking the heaviest element that maintains independence will find a maximum-weight independent set [9]. The proof of this theorem relies on the exchange property and is a cornerstone of combinatorial optimization.

As a corollary, many classic problems can be solved greedily because they can be modeled as matroids. For example, Kruskal's algorithm for finding a minimum spanning tree in a graph works because the graphic matroid satisfies the criteria – any greedy choice (like always adding the next smallest edge that does not create a cycle) yields a spanning tree of minimum total weight. If one ever finds a problem where greedy fails, it is a hint that the independence structure of the solution space might not form a matroid.

Duality and Planarity We mentioned Whitney's planarity criterion earlier: a finite graph G is planar if and only if the dual of its graphic matroid $M(G)$ is also graphic [7] (specifically, $M(G)^* = M(G^*)$, where G^* is the planar dual graph). This is a deep theorem linking matroid duality to planar graph duality. In fact, many properties of planar graphs can be elegantly translated into matroid language. For instance, in a planar graph, the cuts (bonds) and cycles stand in a dual relationship; this is exactly the relationship of circuits and cocircuits in the graphic matroid and its dual.

Decomposition and Minors Matroids have a notion of minors analogous to graph minors: one can delete or contract elements and still have a matroid. Many matroid properties are hereditary for minors. There are profound structure theorems (such as Tutte's and Seymour's decomposition theorems) describing matroids that can be composed from simpler ones by operations like direct sums and 2-sums. While these are beyond the scope of this introduction, it is worth noting that the theory of matroid minors parallels the famous Robertson–Seymour theorem for graph minors, and there is ongoing research (the Matroid Minors Project) to classify huge families of matroids in a similar way [6].

Representability and Fields A theorem by Tutte (regular matroid theorem) characterizes when a matroid is representable over certain fields (e.g. binary matroids are those representable over $\mathbb{F}_2$, regular matroids are those representable over every field, etc.). One surprising fact is that some matroids are representable over one field but not another. For example, the Fano matroid (coming from the Fano plane geometry) is representable over $\mathbb{F}_2$ but not over $\mathbb{R}$; conversely, some matroids are real-representable but not binary-representable [7]. These results illustrate that matroid theory sits at an intersection of algebra and combinatorics, extending linear algebra in non-obvious ways.

Brief Applications of Matroid Theory

Matroid theory might appear abstract, but it has powerful applications in various domains. We conclude with a few brief examples:

Greedy Optimization As noted, any optimization problem that can be modeled with a matroid constraint can be solved by a greedy algorithm. This includes classical problems like finding a maximum spanning tree in a network, scheduling problems with precedence constraints that form a matroid, and certain scheduling or resource allocation problems modeled by partition matroids [8]. Beyond spanning trees, matroid intersection algorithms (for finding a largest common independent set of two matroids) generalize bipartite graph matchings and have applications in scheduling and assignment problems [8].

Network Design and Electrical Engineering The circuits and cocircuits of graphic matroids correspond to cycles and cuts in electrical networks. Concepts in network flow and connectivity can be elegantly phrased in matroid terms. For instance, the cut-set space and cycle space of a graph (over $\mathbb{F}_2$) are orthogonal complements, reflecting matroid duality in network analysis [10]. Designing reliable networks or analyzing redundancy often implicitly uses matroid theory.

Coding Theory Linear codes in coding theory are essentially subspaces of $\mathbb{F}_q^n$ and have generator and parity-check matrices. The set of coordinates of a code that correspond to linearly independent columns of a generator matrix form a matroid (called a vector matroid of the matrix). Thus, properties of codes (like redundancy, code length vs. dimension trade-offs) can be studied with matroid theory. Certain bounds in coding theory (like the Hamming bound and Johnson bound) have interpretations via matroid invariants. Additionally, concepts like greedily optimal or perfect codes can be related to matroid greediness.

Bibliography

References

[1] H. Whitney. On the abstract properties of linear dependence. *American Journal of Mathematics*, 57(3):509–533, 1935.

[2] J. G. Oxley. *Matroid Theory*. Oxford University Press, 1992.

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

[4] D. L. Neel and N. A. Neudauer. Matroids you have known. *Mathematics Magazine*, 82(1):26–41, 2009.

[5] W. T. Tutte. *Introduction to the Theory of Matroids*. American Elsevier Publishing, 1971.

[6] Matroid. *Wikipedia, The Free Encyclopedia*. Accessed 2025.

[7] Lecture notes on matroid theory. Department of Mathematics, The Ohio State University.

[8] Various expository notes on matroids and graph theory. Fiveable Learning Resources.

[9] Notes on the Rado–Edmonds theorem and the greedy algorithm for matroids. Scribd document.

[10] Notes on matroids, graphs, and electrical networks. College of Engineering, Drexel University.