The circuit and cocircuit lattices of a regular matroid

Patrick Mullins

University of Vermont

The Circuit and Cocircuit Lattices of a Regular Matroid

A Thesis Presented

by

Patrick Mullins

to

The Faculty of the Graduate College

of

The University of Vermont

In Partial Fulfillment of the Requirements
for the Degree of Master of Science
Specializing in Mathematical Sciences

May, 2020

Defense Date: March 25th, 2020
Dissertation Examination Committee:

Spencer Backman, Ph.D., Advisor
Davis Darais, Ph.D., Chairperson
Jonathan Sands, Ph.D.
Cynthia J. Forehand, Ph.D., Dean of Graduate College

Abstract

A matroid abstracts the notions of dependence common to linear algebra, graph theory, and geometry. We show the equivalence of some of the various axiom systems which define a matroid and examine the concepts of matroid minors and duality before moving on to those matroids which can be represented by a matrix over any field, known as regular matroids. Placing an orientation on a regular matroid M allows us to define certain lattices (discrete groups) associated to M. These allow us to construct the Jacobian group of a regular matroid analogous to the Jacobian group of a graph. We then survey some recent work characterizing the matroid Jacobian. Finally we extend some results due to Eppstein concerning the Jacobian group of a graph to the case of regular matroids.

Acknowledgements

I would like to thank my advisor Professor Spencer Backman for his support throughout this process. My time studying with him has taught me to be a more careful reader, writer and mathematician. I would also like to thank the other two members of my defense committee, Professor David Darais and Professor Jonathan Sands. Thanks are also due to Professor Richard Foote, without whose support and encouragement I would not have entered the Master's program at UVM.

I would also like to thank other UVM faculty who encouraged my mathematical curiosity during my time in the graduate program: Dr. Francois Dorais, Dr. Dan Hathaway, and Professor Taylor Dupuy. Last but not least, I would like to thank my fellow graduate students Anton Hilado, Oliver Waite, Tyson Pond, Hunter Rehm, Sophie Gonet, and Ryan Grindle.

Table of Contents

List of Figures

Chapter 1

Introduction

The theory of matroids were first developed by Hassler Whitney in his 1935 paper "On the Abstract Properties of Linear Dependence" [19] in order to examine the commonalities between linear algebra and graph theory. Whitney develops the theory of matroids from the simple observations that,

(i) Given a linearly independent set of columns of a matrix, any subset will also be linearly independent.

(ii) Given any two sets of linearly independent columns N_p and N_{p+1}, with p and $p+1$ columns respectively, then N_p along with some column in N_{p+1} is also independent.

Whitney notes several similarities between these relations and those between edges of a graph, where a subset of edges are considered to be dependent if and only if they contain a cycle. The language of matroid theory frequently reflects its origins in these two areas and they provide a useful introduction to the idea of a matroid, but the theory itself extends further to a more abstract notion of dependence which also applies in a discrete geometric setting.

Matroid theory has been an area of great activity, expanding beyond Whitney's original considerations to become a more general theory of independence within a given set system. One of the strengths of matroid theory is its remarkable flexibility; matroids can be characterized by many different axiom systems which arise in different mathematical contexts.

In this thesis, we develop the basic theory of matroids, showing the equivalence of some of the various axiom systems which can be used to define a matroid. We then discuss matroid duality and minors of matroids, two fundamental aspects of the theory that will allow us to define the class of regular matroids. Regular matroids are those which can be represented by a totally unimodular matrix over $\mathbb{R}$; in Chapter 4 we will show that this is equivalent to being representable over any field. Finally we summarize some fundamental results related to the Jacobian group of a matroid, a finite abelian group and generalize certain results due to David Eppstein on the Jacobian of a graph to the Jacobian of a matroid.

In what follows, we will assume that all sets (other than the reals, integers, etc.) are finite. We use X^E to denote the set of functions from X to E; in particular, 2^E is the power set of E. We use $-$ rather than $\setminus$ to denote set subtraction, reserving $\setminus$ for a particular matroid operation. When we have a set X and wish to add an element y, we write simply $X \cup y$ rather than $X \cup \{y\}$. Although we develop the basics of matroid theory at length, we assume basic results from linear algebra, graph theory and elementary group theory, ring theory and field theory.

Chapter 2

Matroid axiom systems

This chapter is primarily concerned with developing some of the basics of matroid theory, in particular the various axiom systems which define matroids. As the equivalence of the matroid axiom systems is in many cases not immediately apparent, the majority of this chapter will be concerned with showing these equivalencies; we will also establish some additional theory which will prove useful in later chapters. Throughout, we provide examples which demonstrate how matroids arise in different mathematical contexts.

That our initial examples will come from linear algebra and graph theory is no surprise, as the commonalities between these two areas was precisely the motivation behind Whitney's original development of the theory [19]. One should bear in mind however that the theory extends beyond these two settings. To that end we include an example of a matroid with no corresponding graph and in another example explicitly demonstrate the connection between matroids and finite geometry. (In a later chapter we shall see an example of a matroid with no matrix representation.)

Roughly speaking, the axiom systems in the first section most directly reflect the theory's origins in linear algebra and graph theory, while the second section contains those axiom systems with a more geometric character. In the current literature, it is common to first define matroids in terms of their independent sets and we shall do the same. Following that, our general approach will be to show the equivalence of each other axiom system to that of independent sets. A standard reference for the material found in this section is Oxley [11].

2.1 Independent sets, circuits, and bases

2.1.1 Independent Sets

Let E be a set and $\mathcal{I}$ a collection of subsets of E satisfying the following three axioms:

(I1) $\mathcal{I} \neq \emptyset$.

(I2) If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$.

(I3) If $I_1, I_2 \in \mathcal{I}$ and $|I_2| < |I_1|$, then there exists an element $x \in I_1 - I_2$ such that $I_2 \cup x \in \mathcal{I}$.

We say that $M = (E, \mathcal{I})$ is a *matroid* on the *ground set* E. When it is clear from the context we simply write M and assume the existence of an appropriate E. The members of $\mathcal{I}$ are the *independent sets* of the matroid. We shall usually simply write $\mathcal{I}$, when it is necessary to distinguish the independent sets of a particular matroid M, we write $\mathcal{I}(M)$. A subset of E which is not independent is called *dependent*. The *rank* of M, denoted $r(M)$ is the cardinality of the largest independent set in M. In general, we denote the cardinality of E by m and denote the rank of M as r.

If one recalls the notion of linear independence, the relationship between matroids and linear algebra is fairly evident from this set of axioms. Indeed, as noted in the Introduction, Whitney's initial investigation of a matroid was partially motivated by the observation that the independent subsets of a vector space satisfy properties (I2) and (I3). The following proposition formalizes this observation.

Proposition 2.1.1. *Let E be the set of column labels of an $n \times m$ matrix A over a field $\mathbb{K}$ and let $\mathcal{I}$ be the set of all subsets of E which are linearly independent in $\mathbb{K}^n$. Then $M = (E, \mathcal{I})$ is a matroid.*

Proof. We show that M satisfies the independent set axioms. We have $\emptyset \in \mathcal{I}$, hence M satisfies (I1). Removing an element from a linearly independent set does not affect linear independence so (I2) is also satisfied. To show (I3), we proceed by contradiction. Let I_1 and I_2 be linearly independent subsets of E such that $|I_1| < |I_2|$ but (I3) fails, i.e., suppose there is no $x \in I_2 - I_1$ such that $I_1 \cup x \in \mathcal{I}$. Let V be the subspace of $\mathbb{K}^n$ spanned by $I_1 \cup I_2$, so the dimension of V is at least $|I_2|$. By assumption, $I_1 \cup x$ is linearly dependent for all $x \in I_2 - I_1$. Then V is entirely contained in the span of $I_1 \cup x$, implying that $|I_2| \leq \dim V \leq |I_1|$, a contradiction. We conclude that $\mathcal{I}$ satisfies (I3) and M is a matroid. □

A matroid obtained from the linearly independent columns of a matrix A in the manner described above is called a *vector matroid* and is denoted $M(A)$.

Example 2.1.2. Let A be the following matrix with coefficients in $\mathbb{R}$:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

with columns indexed left to right by $E = [5]$. Then $M(A)$ has independent sets

$$\mathcal{I} = \{\emptyset, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \{2,3,5\}, \{3,4,5\}, \{1,2\}, \{1,3\}, \{1,4\},$$
$$\{2,3\}, \{2,4\}, \{2,5\}, \{3,4\}, \{3,5\}, \{4,5\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}.$$

Observe that $r(M(A)) = 3$; all 4-element subsets of E contain a dependent subset.

Let A be an $n \times m$ matrix over a field $\mathbb{K}$, and index the columns of of A by $E = [m]$. Assuming that we keep the column labeling fixed, we may perform elementary row operations, interchange columns, scale columns by non-zero elements of $\mathbb{K}$, and add or remove a zero row without changing the linear dependencies among the elements of E. It follows that the vector matroid $M(A)$ will remain the same. Thus, given a matrix A, we may reduce A to a matrix of the form $[I_r|D]$, where I_r is the $r \times r$ identity matrix and D is an $r \times (n - r)$ matrix without changing the associated vector matroid $M(A)$. Taking the columns of I_r as a basis for the columns space of A shows that $r(M(A)) = r$. A matrix of the form $[I_r|D]$ is called the *standard representation* of $M(A)$.

2.1.2 Circuits

Now that we have defined a matroid M in terms of its independent sets, it is natural to consider the dependent sets of M. The minimal dependent subsets of E are called *circuits*; , i.e., C is a circuit if and only if C is dependent and all proper subsets of C are independent. A singleton dependent set is called a *loop*. We denote the circuits of E as $\mathcal{C}$. As was the case with independent sets, we shall usually simply write $\mathcal{C}$, when it is necessary to distinguish the independent sets of a particular matroid M, we write $\mathcal{C}(M)$.

Proposition 2.1.3. *Let M be a matroid with independent sets $\mathcal{I}$ and circuits $\mathcal{C}$. Then $\mathcal{C}$ has the following properties:*

(C1) $\emptyset \notin \mathcal{C}$.

(C2) *If* $C_1, C_2 \in \mathcal{C}$ *and* $C_1 \subseteq C_2$, *then* $C_1 = C_2$.

(C3) *(circuit elimination) If* C_1, C_2 *are distinct elements of* $\mathcal{C}$ *and* $e \in C_1 \cap C_2$, *then there exists an element* $C_3 \in \mathcal{C}$ *such that* $C_3 \subseteq (C_1 \cup C_2) - e$.

Proof. (C1) follows from the fact that $\emptyset \in \mathcal{I}$. (C2) follows from the definition of $C \in \mathcal{C}$ as a minimal dependent set. To show (C3), we proceed by contradiction. Suppose $I_2 = (C_1 \cup C_2) - e$ does not contain a circuit, i.e., $I_2 \in \mathcal{I}$. Note that by (C2), there exists an element $f \in C_2 - C_1$. Let $I_1 \in \mathcal{I}$ be such that $I_1 \subset C_1 \cup C_2$, I_1 contains $C_1 - f$, and I_1 is of maximum cardinality. By construction, $f \notin I_1$. Also there exists $g \in C_2 - C_1$ such that $g \notin I_1$, otherwise $C_2 \subseteq I_1$. Then

$$|I_1| \leq |(C_1 \cup C_2) - \{f, g\}| = |C_1 \cup C_2| - 2 < |(C_1 \cup C_2) - e| = |I_2|.$$

Therefore, by (I3), there exists $h \in I_2 - I_1$ such that $I_1 \cup h \in \mathcal{I}$, contradicting the maximality of $|I_1|$. We conclude that (C3) holds. □

The previous proposition shows that the circuits of a matroid are determined by its independent sets. The following theorem shows that we can likewise define the independent sets of a matroid in terms of its circuits, i.e., (C1)-(C3) exactly characterize the subsets of E which are the circuits of a matroid on E. It follows from this that we may also view M as being uniquely determined from its collection of circuits. Thus (C1)-(C3) give a second system of axioms which define a matroid.

Theorem 2.1.4. *Let E be a set and let $\mathcal{C}$ be a collection of $C \subseteq E$ which have properties (C1)-(C3) as given above. Define $\mathcal{I}$ to be the collection of all $I \subseteq E$ that do not contain any $C \in \mathcal{C}$. Then $(E, \mathcal{I})$ is a matroid and $\mathcal{C}$ is its collection of circuits.*

Proof. The proof is in two parts. First we show that the members of $\mathcal{I}$ are the independent sets of a matroid M on E, then show that the elements of $\mathcal{C}$ are indeed the set of circuits of M.

By (C1), $\emptyset \notin \mathcal{C}$, hence $\emptyset \in \mathcal{I}$ and (I1) is satisfied. If $I_1 \in \mathcal{I}$, then I_1 contains no $C \in \mathcal{C}$. Then if $I_2 \subseteq I_1$, I_2 contains no such C, thus $I_2 \in \mathcal{I}$ and and (I2) is satisfied.

To prove that (I3) holds, we proceed by contradiction. Let $I_1, I_2 \in \mathcal{I}$ such that $|I_1| < |I_2|$ but (I3) fails. Then for all $x \in I_2 - I_1$, $I_1 \cup x \notin \mathcal{I}$. Let $I_3 \subseteq I_1 \cup I_2$ and $I_3 \in \mathcal{I}$ such that $|I_3| > |I_1|$ and $|I_1 - I_3|$ is minimum but nonzero - this must be the case as (I3) fails. Let $e \in I_1 - I_3$. For $f \in I_3 - I_1$, define $T_f \coloneqq (I_3 \cup e) - f$. Note that $T_f \subseteq I_1 \cup I_2$, and $|I_1 - T_f| < |I_1 - I_3|$. By minimality of $|I_1 - I_3|$, $T_f \notin \mathcal{I}$, hence T_f contains some circuit C_f and $f \notin C_f$. Also $e \in C_f$, otherwise $C_f \subseteq I_3$.

Now let $g \in I_3 - I_1$ and define C_g as above. If $C_g \cap (I_3 - I_1) \neq \emptyset$, then $C_g \subseteq ((I_3 \cap I_1) \cup e) - g \subseteq I_1$, contradicting the independence of I_1. Therefore there exists an element $h \in C_g \cap (I_3 - I_1)$, so we may define C_h. Note that $C_g \neq C_h$ and $e \in C_g \cap C_h$. By (C3), there exists some circuit $C \subseteq (C_g \cap C_h) - e$. But C_g and C_h are both contained in $I_3 \cup e$, hence $C \subseteq I_3$, contradicting the fact that $I_3 \in \mathcal{I}$. Therefore it must be the case that (I3) holds, hence $M = (E, \mathcal{I})$ is a matroid.

We now confirm that $\mathcal{C}$ is the set of circuits of M. Observe that C is a circuit of M if and only if $C \notin \mathcal{I}$ but $C - x \in \mathcal{I}$ for all $x \in C$. The latter holds if and only if C

has no proper subset which is also an element of $\mathcal{C}$ and this is the case exactly when $C \in \mathcal{C}$. $\square$

The following proposition further illustrates the relationship between the circuits and independent sets of a matroid.

Proposition 2.1.5. *Let I be an independent set of a matroid M and $e \in M$ such that $I \cup e$ is dependent. Then M has a unique circuit $C \subseteq I \cup e$ and $e \in C$.*

Proof. If $I \cup e$ is dependent it must contain a circuit and that circuit must contain e. To see that this circuit must be unique, suppose that there exist two distinct circuits $C_1, C_2 \subseteq I \cup e$. Then by (C3), $(C_1 \cup C_2) - e$ contains a circuit $C_3 \subseteq I$, a contradiction. So $C_1 = C_2$. $\square$

The use of the term circuit for a minimal dependent set of a matroid is reminiscent of graph theory and, as previously noted, this is no coincidence. We have already established that the linearly independent columns of a matrix define a matroid; the next proposition shows that, if we take the edge set E of a graph G to be the ground set, the cycles of G define a matroid. Such a matroid is called a *cycle matroid* of G. Note that, while the circuits of the cycle matroid of a graph G are the cycles of G, the correspondence is not exact.

Proposition 2.1.6. *Let G be a graph and let E be the set of edges of G. Define $\mathcal{C}$ to be the set of edge sets of cycles of G. Then $\mathcal{C}$ is the collection of circuits of a matroid on E.*

Proof. (C1) and (C2) are clear. To see that (C3) holds, let C_1 and C_2 be distinct cycles in G and $e \in C_1 \cap C_2$. Say e has endpoints u, v. Let P_1 be a path from u to v

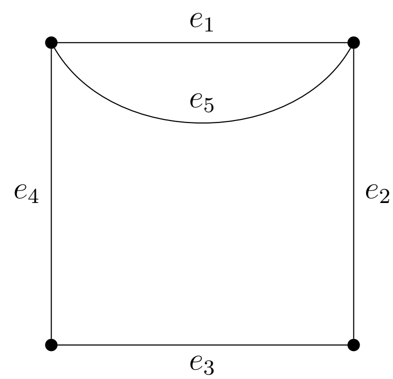

Figure 2.1: The graph G in Example 2.1.7.

with edges in $C_1 - e$ and likewise define P_2. Beginning at u, travel through P_1 to the first vertex w incident to an edge in $P_1 - P_2$. From w continue to travel on P_1 towards v until reaching a vertex x incident to an edge in P_2 - we must reach such a vertex, as both P_1 and P_2 end at v. Concatenating the section of P_1 from w to x and the section of P_2 from x to w gives a cycle $C \subseteq (C_1 \cup C_2) - e$ hence (C3) is satisfied. $\square$

Example 2.1.7. Let G be the graph shown in Figure 2.1 and let $M = M(G)$ be the cycle matroid on the edge set $E(G) = \{e_1, e_2, e_3, e_4, e_5\}$. Then M has circuits $\mathcal{C} = \{\{e_1, e_5\}, \{e_1, e_2, e_3, e_4\}, \{e_2, e_3, e_4, e_5\}\}$. All three element subsets of E not containing $\{e_1, e_5\}$ are independent. It is not hard to see that $M(G)$ satisfies the circuit elimination axiom (C3): $e_1 \in \{e_1, e_5\} \cap \{e_1, e_2, e_3, e_4\}$ and $\{e_2, e_3, e_4, e_5\} \subseteq (\{e_1, e_5\} \cup \{e_1, e_2, e_3, e_4\}) - e_1$.

Recall the matroid $M(A)$ from Example 2.1.2. This was the vector matroid associated to the matrix

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Index the columns of A from left to right by $c_1, \ldots, c_5$. Define a bijection by $\varphi(c_i) = e_i$ for $i \in [5]$. It is not difficult to see that under this bijection, $M(A)$ and $M(G)$ have the same circuits and (equivalently) the same independent sets. We can illustrate the same circuit exchange relationship using the minimal dependent sets of columns of A. We have $C_1 = c_1 + c_2 + c_3 - c_4 = 0$ and $C_2 = c_1 - c_5 = 0$, hence $C_3 = C_1 - C_2 = c_2 + c_3 - c_4 + c_5 = 0$.

In the previous example we saw two matroids which were "the same" under a given bijection. Given two matroids M_1 and M_2, if there exists a bijection φ from $E(M_1)$ to $E(M_2)$ such that, for all $X \subseteq E(M_1)$, $\varphi(X)$ is independent in M_2 if and only if X is independent in M_1, we say that the two matroids are *isomorphic* and write $M_1 \cong M_2$. Informally, this means that a matroid isomorphism amounts to a relabeling of the ground set. A matroid which is isomorphic to the cycle matroid of a graph is said to be *graphic*. A matroid isomorphic to the vector matroid of a matrix over a field $\mathbb{K}$ is *representable* over $\mathbb{K}$. If a matroid M is representable over any field, we say M is *regular*.

2.1.3 Bases

The third axiom system we consider defines a matroid in terms of its maximal independent sets or *bases*. First we show that the bases of a matroid are determined by its independent sets and vice versa.

Proposition 2.1.8. *Let M be a matroid with independent sets $\mathcal{I}$. Define $\mathcal{B}$ to be the collection of maximal elements of $\mathcal{I}$. Then $\mathcal{B}$ has the following properties:*

(B1) $\mathcal{B} \neq \emptyset$.

(B2) If B_1 and B_2 are in $\mathcal{B}$ and $x \in B_1 - B_2$, then there exists $y \in B_2 - B_1$ such that $(B_1 - x) \cup y \in \mathcal{B}$.

Proof. (B1) follows from the definition of $B \in \mathcal{B}$ as a maximal element of $\mathcal{I}$. To see (B2), let $B_1, B_2 \in \mathcal{B}$ and $x \in B_2$. Note that $|B_1| = |B_2|$. Suppose not; say $|B_1| < |B_2|$. By (I3), there exists some $e \in B_2 - B_1$ such that $B_1 \cup e \in \mathcal{I}$, contradicting the maximality of B_1. Let $I_1 = B_1 - x$ and $I_2 = B_2$, then $|I_1| < |I_2|$. Again using (I3) we find $y \in I_2 - I_1$ such that $I_1 \cup y = (B_1 - x) \cup y \in \mathcal{I}$. Note that $|(B_1 - x) \cup y| = |B_1|$, hence $(B_1 - x) \cup y \in \mathcal{B}$. □

Property (B2) is known as the *basis exchange axiom*. Observe that (B1) and the observations made in the above proof imply that all bases of a matroid have the same cardinality. There may be elements of E which are in all bases; such an element is called a *coloop* or sometimes an *isthmus*.

We shall usually simply write $\mathcal{B}$, when it is necessary to distinguish the independent sets of a particular matroid M, we write $\mathcal{B}(M)$.

We now show that members of $\mathcal{B}$ are exactly the maximal independent sets of a matroid.

Theorem 2.1.9. *Let E be a set and define*

$$\mathcal{B} \coloneqq \{B \subseteq E : B \text{ satisfies (B1) and (B2) }\}.$$

Define $\mathcal{I} \coloneqq \{I \subseteq B \in \mathcal{B}\}$. Then (E, I) is a matroid with bases $\mathcal{B}$.

Proof. (B1) implies that $\mathcal{I}$ satisfies (I1). Say $I \in \mathcal{I}$; then by definition, $I \subseteq B$ for some $B \in \mathcal{B}$. If $I' \subseteq I$, then clearly $I' \subseteq B$ hence $I' \in \mathcal{I}$. Hence $\mathcal{I}$ satisfies (I2).

To see that $\mathcal{I}$ satisfies (I3), we proceed by contradiction. Let $I_1, I_2 \in \mathcal{I}$ and without loss of generality, say $|I_1| < |I_2|$. There exists $B_1 \supseteq I_1$ and $B_2 \supseteq I_2$ with $B_1, B_2 \in \mathcal{B}$. Note that $B_1 - I_1 \neq \emptyset$ by assumption on the cardinality of I_1. Let $x \in B_1 - I_1$. By (B2), there exists $y \in B_2 - B_1$ such that $B_1' = (B_1 - x) \cup y \in \mathcal{B}$ and $B_1' \supseteq I_1$. If $y \in I_2$, we are done as $I_1 \cup y \subseteq B_1'$ implies that $I_1 \cup y \in \mathcal{I}$. So say $y \notin I_2$. Assume B_2 is such that $|B_2 - (B_1 \cup I_2)|$ is minimal.

We claim that $B_2 - (B_1 \cup I_2) = \emptyset$. Suppose not and say $y \in B_2 - (B_1 \cup I_2) \neq \emptyset$. By (B2), there exists some $z \in B_1 - B_2$ such that $B_2' = (B_2 - y) \cup z \in \mathcal{B}$. Then $B_2' \supseteq I_2$ and $|B_2' - (B_1 \cup I_2)| = |B_2 - (B_1 \cup I_2)| - 1$, a contradiction. This proves the claim. So it must be the case that $y \in I_2$; if $y \in B_2 - I_2$, then $|B_2 - (B_1 \cup I_2)| \neq 0$. So $y \in I_2 - I_1$ and $B_1' \supseteq I_1 \cup y$. Then $I_1 \cup y \in \mathcal{I}$ hence $\mathcal{I}$ satisfies (I3). □

Note that Proposition 2.1.7 and Theorem 2.1.8 together with Proposition 2.1.3 and Theorem 2.1.4 show the equivalence of the three axiom systems for matroids we have seen so far.

Similarly to the axiom systems for independent sets and circuits, the basis axioms have natural analogies with graph theory and the theory of vector spaces, as the following example shows.

Example 2.1.10. Consider the vector matroid $M(A)$ in Example 2.1.2. The bases of this matroid are the 3-element sets of $\mathcal{I}$. Recall that this matroid is isomorphic to $M(G)$, the cycle matroid of the graph G in Figure 2.1, seen in Example 2.1.7. The bases of $M(G)$ are the maximal subsets of $E(G)$ not containing a cycle which correspond to the 3-element subsets of $E(G)$ which do not contain an $\{e_1, e_5\}$ subset. These are exactly the spanning trees of G. Recall the well-known exchange property for spanning trees, which states that given a graph G for any two spanning trees

T_1, T_2, for every edge $e \in T_1 - T_2$, there exists an $f \in T_2 - T_1$ such that $(T_1 - e) \cup f$ is a spanning tree of G. Comparing this with axiom (B2) makes the character of a matroid basis clear.

The following results makes plain the connections between graphs, linear algebra, and matroids.

Proposition 2.1.11. *Let $G = (V, E)$ be a graph with vertices $v_1, ..., v_n$ and edges $e_1, ..., e_m$. Fix an arbitrary orientation of the edges of G. If an edge e is oriented from vertex u to vertex v, we say that u is the tail of e, and v is the head of e. Let A be the $n \times m$ matrix with (i, j) entry either 1 if v_i is the head of e_j, -1 if v_i is the tail of e_j, or 0 if v_i is not incident to e_j. Let $M(A)$ be the vector matroid on A. Then the circuits of $M(A)$ (the minimal linearly dependent sets of columns of A) precisely correspond to the cycles of G. Furthermore, the independent sets of columns of A correspond to the forests of G, and the maximal linearly independent sets of columns (bases) are the spanning forests of G (spanning trees if G is connected).*

Proof. Fix an orientation on G such that all cycles have a counterclockwise orientation. Let $C = \{c_1, \ldots, c_k\}$ be a circuit of $M(A)$. By construction of A, the c_j sum to the zero vector if and only if each vertex v_i with non-zero entries in some c_j has entries of the opposite sign in some other element of C. This occurs exactly when v_i is the head of some edge e and the tail of another edge f in G. So every such v_i has degree 2 and this describes a cycle in G. Note that if $|C| = 1$, C is a loop; if $|C| = 2$, we have parallel edges with opposite orientations.

Now suppose Z is a cycle in G. Then the set of column vectors $C = \{c_1, \ldots, c_k\}$ corresponding to the edges in Z sum to zero as described above. To see that C is minimal as a dependent set in A, simply remove an edge from Z. This corresponds to removing some column vector c_j from C, but then the remaining vectors in C no longer sum to zero. If Z is a loop, then some vertex is both the head and tail of some edge, hence the corresponding column is the zero vector.

From the above, we see that a set of column vectors I in A is independent if and only if it corresponds to an edge set of G which contains no cycles and this is precisely the definition of a forest of G.

Assume G is connected. Let $B = \{b_1, \ldots, b_k\}$ be a maximal set of linearly independent columns of A. Adding any other column in A to B produces a dependent set of column vectors, which corresponds to a cycle in G. Thus B corresponds to a maximum cardinality acyclic set of edges in G, i.e., a spanning tree. If G is not connected, then each component of G will correspond to a submatrix of A. Working with each such component submatrix individually then taking the union of the spanning trees of each component gives a spanning forest of G. □

The following result extends the graph theoretic notion of a fundamental cycle associated to a spanning tree to matroids.

Proposition 2.1.12. *Let B be a basis for a matroid M. Then for every $e \in E - B$, $B \cup e$ contains a unique circuit $C(e, B)$ and $e \in C(e, B)$*

Proof. This follows from Proposition 2.1.5. □

The circuit $C(e, B)$ described in the above proposition is called a *fundamental circuit of e with respect to B.*

At this point the only examples of matroids we have seen are both graphic and representable. Observe that the incidence matrix of a graph described in Proposition 2.1.11 (although originally defined over $\mathbb{R}$) can serve as a representation of $M(G)$ over

$\mathbb{F}_3$; taking the entries mod 2 gives a representation over $\mathbb{F}_2$. When a matroid M is representable over $\mathbb{F}_2$, we say that M is *binary*; when M is representable over $\mathbb{F}_3$, we say that M is *ternary*. However, not all representable matroids are graphic, as the following example shows.

Example 2.1.13. A matroid M on n elements such that all r-element subsets of M are independent is called a *uniform matroid* and denoted $U_{r,n}$. Consider the matroid $U_{2,4}$. This matroid can be represented by the following matrix over $\mathbb{R}$.

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

Suppose that $M = U_{2,4}$ has a graph G. We may assume that G is connected, as the cycles of the graph determine the matroid and G will contain the same cycles if disconnected. The ground set E of M has 4 elements and the independent sets of M have at most 2 elements, hence the bases of M have 2 elements. Then G has 4 edges and a spanning tree of G has 2 edges. Because a spanning tree for a graph with n vertices has $n-1$ edges, G must have 3 vertices. So $|E(G)| = 4$ and $|V(G)| = 3$, hence G must have a loop or a pair of parallel edges. But a loop or pair of parallel edges is a dependent set of cardinality 1 or 2 respectively, contradicting the fact that the independent sets of M are all sets of cardinality less than or equal to 2. Therefore M is not graphic.

2.2 Rank, Flats, and Closure

Any of the three axiom systems already seen can define any matroid, but there are several other axiom systems commonly used in the literature. In this chapter we give two related axiom systems for matroids which emphasize their geometric character, then use these axioms to define certain families of subsets of the ground set of a matroid.

2.2.1 Rank

Recall that the rank of a matroid, $r(M)$, is the size of the largest independent set in E. We can extend this to a rank function $r : 2^E \to \mathbb{Z}^{\geq 0}$ given by

$$r(A) = \max_{I \subseteq A}\{|I| : I \in \mathcal{I}\}.$$

Under this definition, the rank of the matroid is the rank of the ground set which is the cardinality of a basis of a matroid: $r(M) = r(E) = r(B) = |B|$.

Proposition 2.2.1. *Let E be a set and define a function $r : E \to \mathbb{Z}^{\geq 0}$ as described above. Then r is the rank function of a matroid M on E if and only if, for $X, Y \subseteq E$,*

(R1) $0 \leq r(X) \leq |X|$.

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

(R3) $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$.

Before proving the proposition, we define the notion of a *restriction* of a matroid. Let $X \subseteq E$. Then the restriction of M to X, denoted $M|_X$, is simply the matroid we obtain by restricting the independent sets, etc. of M to elements of X. For example, the independent sets of X are $\mathcal{I}(M|_X) = \{I \cap X : I \in \mathcal{I}(M)\}$ with bases and circuits defined similarly.

Proof. The first two properties are clear. Property (R1) follows from the definition of the rank function - the rank of a set cannot be greater than its cardinality. The second property similarly follows from the fact that if $X \subseteq Y$, then $|X| \leq |Y|$.

It remains to show property (R3). Let B_1 be a basis of $M|_{X\cap Y}$. Then B_1 is an independent set contained in a basis B_2 of $M|_{X\cup Y}$. Note that $B_2 \cap X$ is independent in $M|_X$; similarly $B_2 \cap Y$ is independent in $M|_Y$. By definition of the rank function, $r(X) \geq |B_2 \cap X|$ and $r(Y) \geq |B_2 \cap Y|$, hence $r(X) + r(Y) \geq |B_2 \cap X| + |B_2 \cap Y|$. Note that

$$\begin{aligned} |B_2 \cap X| + |B_2 \cap Y| &= |(B_2 \cap X) \cup (B_2 \cap Y)| + |(B_2 \cap X) \cap (B_2 \cap Y)| \\ &= |B_2 \cap (X \cup Y)| + |B_2 \cap X \cap Y| = |B_2| + |B_1|. \end{aligned}$$

Therefore $r(X) + r(Y) \geq |B_2| + |B_1| = r(X \cup Y) + r(X \cap Y)$. □

The next theorem shows that a matroid can be defined in terms of its rank function.

Theorem 2.2.2. *Let E be a set and let $r : 2^E \to \mathbb{Z}^{\geq 0}$ be such that r satisfies properties (R1)-(R3). Define $\mathcal{I} := \{I \subseteq E : r(I) = |I|\}$. Then $(E, \mathcal{I})$ is a matroid on E with rank function r.*

The proof of this theorem requires the following lemma.

Lemma 2.2.3. *Let E be a set and r a rank function on E. If $X, Y \subseteq E$ such that $r(X \cup y) = r(X)$ for all $y \in Y - X$, then $r(X \cup Y) = r(X)$.*

Proof. Say $|Y - X| = k$ for some integer k. The proof is by induction on k. If $k = 1$, the result is immediate. Say the result holds for $k = n$. We will show that the result holds for $n + 1$. By induction, using (R2) and (R3),

$$\begin{aligned} r(X) + r(X) &= r(X \cup \{y_1, \dots, y_k\}) + r(X \cup y_{k+1}) \\ &\geq r((X \cup \{y_1, \dots, y_k\}) \cup (X \cup y_{n+1})) + r((X \cup \{y_1, \dots, y_k\}) \cap (X \cup y_{n+1})) \\ &= r((X \cup \{y_1, \dots, y_{k+1}\}) + r(X) \\ &\geq r(X) + r(X). \end{aligned}$$

Because equality must hold throughout, we have $r(X \cup \{y_1, \dots, y_{k+1}\}) = r(X)$. □

We may now prove Theorem 2.2.2.

Proof. By (R1), we have $0 = r(\emptyset) = |\emptyset|$, thus $\emptyset \in \mathcal{I}$ and $\mathcal{I}$ satisfies (I1). Let $I_1 \in \mathcal{I}$, so $r(I_1) = |I_1|$ and let $I_2 \subseteq I$. By (R3),

$$r(I_2 \cup (I_1 - I_2)) + r(I_2 \cap (I_1 - I_2)) = r(I_1) + r(\emptyset) \leq r(I_2) + r(I_1 - I_2).$$

By (R2), $r(I_2) \leq |I_2|$ and $r(I_1 - I_2) \leq |I_1 - I_2|$. Hence,

$$|I_1| \leq r(I_2) + r(I_1 - I_2) \leq |I_2| + |I_1 - I_2| = |I_1|.$$

The equality in the above equation must hold throughout, thus $r(I_2) = |I_2|$. So $I_2 \in \mathcal{I}$ and $\mathcal{I}$ satisfies (I2).

To show that $\mathcal{I}$ satisfies (I3), we proceed by contradiction. Let $I_1, I_2 \in \mathcal{I}$ such that $|I_1| < |I_2|$, but for all $x \in I_2 - I_1$, $I_1 \cup x \notin \mathcal{I}$. By definition of $\mathcal{I}$, we know that $|I_1| = r(I_1) = r(I_1 \cup x)$ for all $x \in I_2 - I_1$. It cannot be the case that $|I_2 - I_1| = 1$, otherwise, $I_1 \cup x = I_2$, and $r(I_1 \cup x) = r(I_2) \leq |I_2|$. So $|I_2 - I_1| = k$ for some $k > 1$. By the above lemma, $r(I_1 \cup \{x_1, \ldots, x_k\} = |I_1|$. But then $I_1 \cup \{x_1, \ldots, x_k\} = I_2$, hence $r(I_1 \cup \{x_1, \ldots, x_k\}) = r(I_2) = |I_2| \leq |I_1| < |I_2|$, and we have a contradiction. Therefore $\mathcal{I}$ satisfies (I3). □

The preceding theorem and proposition show the equivalence of the rank axioms (R1)-(R3) with the independent set axioms and thus with the other axiom systems previously shown.

2.2.2 Closure

The rank function can be used to define another function on 2^E. Let M be a matroid on a ground set E and define a function $\text{cl} : 2^E \to 2^E$ given by

$$\text{cl}(X) = \{x \in E : r(X \cup x) = r(X)\}.$$

The function cl is the *closure operator* of M; we call the set $\text{cl}(X)$ the *closure* of X. If $X \subseteq E$ such that $\text{cl}(X) = E$, we say that X is a *spanning set* of M. It is immediate from the definition of a spanning set that a basis is a minimal spanning set.

Following the now familiar pattern, we next establish the equivalence of a set of properties of the closure operator with the independent set axioms.

Proposition 2.2.4. *Let M be a matroid on ground set E. The closure operator on M has the following properties:*

(CL1) If $X \subseteq E$*, then* $X \subseteq \mathrm{cl}(X)$*.*

(CL2) If $X \subseteq Y \subseteq E$*, then* $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$*.*

(CL3) If $X \subseteq E$ *then* $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$*.*

(CL4) If $X \subseteq E$ *and* $x \in E$*, and* $y \in \mathrm{cl}(X \cup x) - \mathrm{cl}(X)$*, then* $x \in \mathrm{cl}(X \cup y)$*.*

The proof of (CL3) uses the following lemma:

Lemma 2.2.5. *Let* E *be the ground set of a matroid* M*. For all* $X \subseteq E$*,* $r(X) = r(\mathrm{cl}(X))$*.*

Proof. Let B be a basis for X. For all $x \in \mathrm{cl}(X) - X$,

$$r(B \cup x) \leq r(X \cup x) = r(X) = |B| = r(B) \leq r(B \cup x).$$

Hence $r(B \cup x) = r(B) = |B| < |B \cup x|$, so $B \cup x$ is a circuit of M. It follows that B is also a basis of $\mathrm{cl}(X)$ and the result follows. $\square$

We now prove Proposition 2.2.4.

Proof. The first property follows from the definition of the closure operator. To see that (CL2) holds, say $X \subseteq Y$ and $x \in \mathrm{cl}(X) - X$, then $r(X) = r(X \cup x)$. If B_1 is a basis of X, B_1 must also be basis of $X \cup x$ and we can extend B_1 to a basis B_2 of $Y \cup x$. Note that $x \notin B_2$, thus B_2 is also a basis of Y. Therefore $r(Y \cup x) = |B_2| = r(Y)$ hence $x \in \mathrm{cl}(Y)$.

To show (CL3), note that it is immediate from (CL1) that $\mathrm{cl}(X) \subseteq \mathrm{cl}(\mathrm{cl}(X))$. Now let $x \in \mathrm{cl}(\mathrm{cl}(X))$. By the above lemma, $r(\mathrm{cl}(X) \cup x) = r(X)$. Then, by (R2),

$$r(\mathrm{cl}(X) \cup x) = r(X) \geq r(X \cup x) \geq r(X).$$

Thus $x \in \mathrm{cl}(X)$, hence $\mathrm{cl}(\mathrm{cl}(X)) \subseteq \mathrm{cl}(X)$.

Finally, we show (CL4). Let $y \in \mathrm{cl}(X \cup x) - \mathrm{cl}(X)$. So $r(X \cup x \cup y) = r(X \cup x)$ and $r(X \cup y) \neq r(X)$. Note that, by (R2) and (R3), $r(X) \leq r(X \cup x) \leq r(X) + 1$. Combining this with the previous inequality shows that $r(X \cup y) = r(X) + 1$. Then

$$r(X) + 1 = r(X \cup y) \leq r(X \cup y \cup x) = r(X \cup x) \leq r(X) + 1$$

which shows that $r(X \cup y \cup x) = r(X \cup y)$, i.e., $x \in \mathrm{cl}(X \cup y)$. □

The following proposition further illustrates the relation between the independent sets of a matroid and its closure operator.

Proposition 2.2.6. *Let M be a matroid with independent sets $\mathcal{I}$. If $I \in \mathcal{I}$ but $I \cup x$ is not, then $x \in \mathrm{cl}(I)$.*

Proof. Because $I \cup x \notin \mathcal{I}$, there is some $y \in I \cup x$ such that $y \notin \mathrm{cl}((I \cup x) - y)$. If $y = x$, we're done. Assume not. Note that $(I \cup x) - y = (I - y) \cup x$ and $y \in \mathrm{cl}((X - y) \cup x) - cl(X - y)$. By (CL4), $x \in \mathrm{cl}((I - y) \cup y) = \mathrm{cl}(I)$. □

We will make extensive use of this proposition in the proof of the following theorem.

Theorem 2.2.7. *Let E be a set and let $\mathrm{cl} : 2^E \to 2^E$ be a function satisfying (CL1) - (CL4). Define*

$$\mathcal{I} = \{X \subseteq E : x \notin \mathrm{cl}(X - x) \text{ for all } x \in X\}.$$

Then $M = (E, \mathcal{I})$ is a matroid with closure operator cl.

Proof. By definition, we have $\emptyset \in \mathcal{I}$, so (I1) is satisfied. For (I2), suppose $I \in \mathcal{I}$ and $J \subseteq I$. Let $x \in J$, then $x \in I$ hence $x \notin \text{cl}(I - x)$. By (CL2), $\text{cl}(J - x) \subseteq \text{cl}(I - x)$, so $x \notin \text{cl}(J - x)$ and $J \in \mathcal{I}$.

To show that (I3) is satisfied, we proceed by contradiction. Let $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$ but for all $x \in I_2 - I_1$, $I_1 \cup x \notin \mathcal{I}$. Choose I_1, I_2 such that $|I_1 \cap I_2|$ is maximal among all such pairs. Let $y \in I_2 - I_1$ and consider $I_2 - y$. If $I_1 \subseteq \text{cl}(I_2 - y)$, by (CL2) and (CL3), $\text{cl}(I_1) \subseteq \text{cl}(I_2 - y)$. Then $y \notin \text{cl}(I_1)$. By the above proposition, $I_1 \cup y \in \mathcal{I}$, so (I3) holds for I_1, I_2. So I_1 is not contained in $\text{cl}(I_2 - y)$. Then there exists $z \in I_1$ such that $z \notin \text{cl}(I_2 - y)$, hence $z \notin I_1 - I_2$. Then $(I_2 - y) \cup z \in \mathcal{I}$ by the proposition above. Because $|I_1 \cap (I_2 - y) \cup z| > |I_1 \cap I_2|$, for some $x \in ((I_2 - y) \cup z) - I_1$, $I_1 \cup x \in \mathcal{I}$. But $x \in I_2 - I_1$, hence (I3) holds and $M = (E, \mathcal{I})$ is a matroid.

It remains to be shown that cl is indeed the closure operator of M. Let cl_M be the closure operator of M. Let $x \in \text{cl}(X) - X$. So $r(X \cup x) = r(X)$. Let B be a basis of X, then $B \cup x \notin \mathcal{I}$ and by the above proposition $x \in \text{cl}(B)$. By (CL2), $\text{cl}(B) \subseteq \text{cl}(X)$, hence $x \in \text{cl}(X)$. This shows that $\text{cl}_M(X) \subseteq \text{cl}(X)$. Now suppose $x \in \text{cl}(X) - X$ and let B be a basis of X. Then for all $y \in X - B$, $B \cup y \notin \mathcal{I}$. Again using the above proposition, we have $X \subseteq \text{cl}(B)$. Then $\text{cl}(X) \subseteq \text{cl}(B)$. So $x \in \text{cl}(B)$ and $B \cup x \notin \mathcal{I}$, so B is a basis for $X \cup x$ and $r(X \cup x) = r(X) = |B|$. So $x \in \text{cl}_M(X)$ thus $\text{cl}_M(X) \subseteq \text{cl}(X)$. □

2.2.3 Flats

We may use the rank and closure functions to characterize two important classes of subsets of a matroid M on a ground set E. A subset F of E is called a *flat* or *closed set* of M if $r(F \cup x) > r(F)$ for all $x \notin F$. Equivalently, F is a flat if and only if

$\text{cl}(F) = F$. We denote the collection of flats of a matroid as $\mathcal{F}$. Note that it is always the case that $E \in \mathcal{F}$.

A flat H is a *hyperplane* of M if $r(H) = r(M) - 1$; this is equivalent to the statement that H is a maximal non-spanning set. The next proposition gives a graphic characterization of a hyperplane.

Proposition 2.2.8. *Let $M(G)$ be a matroid on a graph G. Then H is a hyperplane in $M(G)$ if and only if $E(G) - H$ is a minimal cut in G.*

Proof. Suppose $E(G) - H$ is a minimal cut in G. Then all $e \in E(G) - H$ connect two components of G. This implies that $H \cup e$ is a spanning set of $M(G)$ for all, hence H is a maximal non-spanning set, i.e. a hyperplane.

Let H be a hyperplane in $M(G)$. Then H is a maximal non-spanning set, i.e. the edges of H do not span G. Thus $E(G) - H$ has two components, but $H \cup e$ is connected for all $e \in E(G) - H$. Hence $E(G) - H$ is a minimal cut in G. □

An important characteristic of $\mathcal{F}$ is that the collection of flats forms a lattice under inclusion, as the following proposition shows. Recall that a *lattice* is a partially ordered set $(E, \leq)$ such that every pair of elements $x, y \in E$ have a *join* and a *meet*. The join of x and y, denoted $x \vee y$, is defined as $\min\{z : x \leq z \text{ and } y \leq z\}$. The meet of x and y is defined as $x \wedge y : \max\{z : z \leq x \text{ and } z \leq y\}$. If $x \leq y$ and there is no element of the poset between x and y, we say that y *covers* x.

Proposition 2.2.9. *Let M be a matroid. Then the collection of flats $\mathcal{F}$ of M form a lattice under inclusion, in particular given $F_1, F_2 \in \mathcal{F}$, $F_1 \wedge F_2 = F_1 \cap F_2$ and $F_1 \vee F_2 = \text{cl}(F_1 \cup F_2)$.*

Proof. First we need to show that $F_1 \cap F_2 \in \mathcal{F}$. To see that this is the case, suppose there is some $x \in \mathrm{cl}(X \cap Y) - (X \cap Y)$. Then $r((F_1 \cap F_2) \cup x) = r(F_1 \cap F_2)$. Say X is a maximal independent set in $F_1 \cap F_2$. Then $X \cup x$ contains a circuit, hence $(F_1 \cap F_2) \cup x$ contains a circuit and x is a element of that circuit. This implies that $x \in \mathrm{cl}(F_1) \cap \mathrm{cl}(F_2)$, but $\mathrm{cl}(F_1) \cap \mathrm{cl}(F_2) = F_1 \cap F_2$, contradicting the assumption that $x \notin F_1 \cap F_2$. Hence $F_1 \cap F_2 \in \mathcal{F}$. If $F_1 \cap F_2$ is not the meet of F_1 and F_2, then there is some element in F_1 and F_2 not in $F_1 \cap F_2$, a contradiction. Therefore $F_1 \wedge F_2 = F_1 \cap F_2$. If $F_1 \cap F_2 = \emptyset$, then $F_1 \wedge F_2$ is the zero element of the poset, i.e. the empty set, and the result holds.

Now consider $F_1 \vee F_2$; $F_1 \cup F_2$ may not be a closed set but $\mathrm{cl}(F_1 \cup F_2)$ certainly is. We claim that $\mathrm{cl}(F_1 \cup F_2)$ is the smallest flat containing F_1 and F_2, hence $\mathrm{cl}(F_1 \cup F_2) = F_1 \vee F_2$. To see this, suppose there exists some flat $F \supseteq F_1 \cup F_2$ but $F \not\supseteq \mathrm{cl}(F_1 \cup F_2)$. Then $F \cap \mathrm{cl}(F_1 \cup F_2)$ is a flat containing $F_1 \cup F_2$ but contained in $\mathrm{cl}(F_1 \cup F_2)$, a contradiction. □

Note that later in this paper, we consider a lattice in the sense of a free abelian group; it is this group-theoretic lattice rather than the order-theoretic lattice defined above that is our main focus in this paper.

Example 2.2.10. Consider the graph $G = K_4$, the complete graph on four vertices, with edges labeled as in Figure 2.2. Take $E = E(G)$ and define a matroid $M(G)$ on E. Then the bases are all 3-element subsets of $E(G)$ which are not cycles in G; these are exactly the spanning trees of G. It follows that $r(M(G)) = 3$. The circuits are the edge sets of the cycles in G and all subsets of $E(G)$ which contain at least one cycle. The independent sets are the bases plus all singleton and 2-element sets. The hyperplanes are the sets of 2 non-adjacent edges. The other flats of $M(G)$ are the

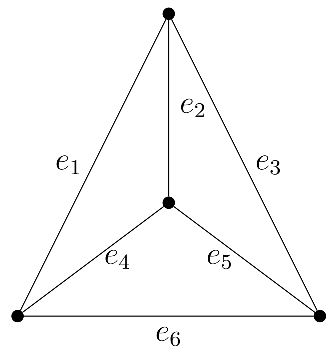

Figure 2.2: K_4, the complete graph on 4 vertices, with edges labeled as in Example 2.2.9.

singleton subsets of E, the 3-cycles of G, and E itself.

Now consider the following matrix A over the real numbers:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Label the columns of A as $E = \{e_1, \ldots, e_6\}$ and define a matroid $M(A)$ on E. It is easy to see that if we associate each column of A to the correspondingly labeled edge in G, it is easy to see that A and G generate the same matroid. For example, a natural basis for the column space of A is $B = \{e_1, e_2, e_3\}$, and this corresponds to a spanning tree T of G. Adding any other column to B gives a linear dependency, hence a circuit in $M(A)$; likewise, adding any edge to T generates a cycle.

By adding rows of A and then scaling columns, we obtain the following matrix

$$A' = \begin{bmatrix} 1 & 0 & 0 & 1/3 & 0 & 1/2 \\ 0 & 1/2 & 0 & 1/3 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

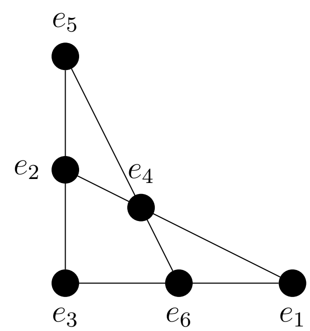

Figure 2.3: $M(K_4)$, the cycle matroid associated to K_4, with elements labeled to correspond to the edge labeling of K_4 in Figure 2.2.

which is equivalent to the matrix A, and keep the same labeling of the columns. We shall show in a later chapter that performing elementary row and column operations on a matrix does not affect the associated vector matroid, so in this case $M(A') = M(A) = M(K_4)$. By taking each column of A' as a vector in $\mathbb{R}^3$ and projecting onto the plane $z = 1$, we obtain the geometric representation of $M(K_4)$ shown in Figure 2.3. Observe that three colinear points represent a circuit, as do any four non-colinear points; any three non-colinear points give a basis. Note that the coordinates in the projections of the column vectors of A' give the position of the corresponding point in the plane; this is reflected in the position of the elements in Figure 2.3.

Chapter 3

Duality and minors

As is the case with many areas of matroid theory, the notions of matroid duality and minors can be intuitively but not precisely understood by analogy with the graph theoretic notions of the same name. Duality, like many of the basics of matroid theory, was originally investigated by Whitney [19]; the theory of matroid minors was developed at length by Tutte, see e.g. [15]. These topics are covered extensively in standard references such as [11] and [17].

3.1 Duality

Let M be a matroid with ground set E and bases $\mathcal{B}(M)$. The *dual matroid* M^* is the matroid with bases $\mathcal{B}(M^*) := \{E - B : B \in \mathcal{B}(M)\}$. We sometimes write $\mathcal{B}^*$ when the context is clear. Of course, it is necessary to verify that M^* is indeed a matroid.

Proposition 3.1.1. *Let M be a matroid with ground set E and bases $\mathcal{B}(M)$. Then $\mathcal{B}(M^*) := \{E - B : B \in \mathcal{B}(M)\}$ are the bases of a matroid.*

Proof. Because there exists some $B \in \mathcal{B}$, there is a complement $E - B \in \mathcal{B}^*$, hence

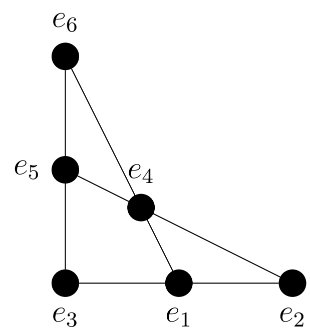

Figure 3.1: $M^*(K_4)$, the dual of the cycle matroid $M(K_4)$ shown in Figure 2.3. See Example 3.1.2.

(B1) is satisfied. Using the definitions of $\mathcal{B}$ and $\mathcal{B}^*$, we have that, for all $B'_1, B'_2 \in \mathcal{B}^*$ and $x' \in B'_1 - B'_2$, there exists $y' \in B'_2 - B'_1$ such that $(B'_1 - x') \cup y' \in \mathcal{B}^*$ if and only if for all $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 - B_2$, there exists $y \in B_2 - B_1$ such that $(B_1 - x) \cup y \in \mathcal{B}$. Therefore, (B2) holds and $\mathcal{B}^*$ is the collection of bases of a matroid. □

From the above theorem, it is evident that, for a matroid M with basis B we have $r(M) = |B|$; it follows that $r(M) + r(M^*) = |E|$. Moreover, it is evident that $(M^*)^* = M$.

A matroid which is isomorphic to its dual is said to be *self-dual*. The dual $M^*(G)$ of a graphic matroid $M(G)$ is sometimes called the *bond matroid* or *cocycle matroid* of G. A matroid which is isomorphic to the cocycle matroid of a graph is said to be *cographic*. The following example exhibits a matroid which is both self-dual and cographic.

Example 3.1.2. Figure 3.1 shows a geometric representation of $M^*(K_4)$, the dual matroid of $M(K_4)$, the cycle matroid of the complete graph on four vertices. A geometric representation of $M(K_4)$ is shown in Figure 2.3. Comparing the two figures it is evident that the two representations are the same save that the labels of the elements have been changed, indicating that $M(K_4) \cong M^*(K_4)$. Note that, e.g., $B = \{e_3, e_5, e_6\}$ is a basis for $M(K_4)$ and $E - B = \{e_1, e_2, e_4\}$ is a basis in $M^*(K_4)$.

Carrying on with the use of co- to indicate matroid duality, the bases of M^* are called the *cobases* of M. We similarly define the *coindependent* sets, *cocircuits*, *cohyperplanes*, and *cospanning* sets. The next two propositions, adapted from [7] and [11], establish the relations between the distinguished sets of a matroid and those of its dual.

Proposition 3.1.3. *Let M be a matroid on a set E and let $X \subseteq E$. Then*

(i) X is independent if and only if $E - X$ is cospanning;

(ii) X is spanning if and only if $E - X$ is coindependent;

(iii) X is a hyperplane if and only if $E - X$ is a cocircuit;

(iv) X is a circuit if and only if $E - X$ is a cohyperplane.

Proof. For *1* and *2*, notice that a coindependent set X is contained in a cobasis, hence $E - X$ must contain a basis for M hence $E - X$ spans M. To show *3* and *4*, observe that X is a hyperplane in M if and only if $r(X \cup y) = r(M)$ for all $y \notin X$. Hence $E - X$ is dependent in M^* but $(E - X) - y$ is independent in M^* and this is precisely the definition of a cocircuit. □

Proposition 3.1.4. *Let M be a matroid and let C and C^* be a circuit and cocircuit of M. Then $|C \cap C^*| \neq 1$.*

Proof. Suppose not. Then $C \cap C^* = x$ for some $x \in E$. Consider the hyperplane $H = E - C^*$ and recall that $\mathrm{cl}(H) = H$. Note that $x \in C^*$, hence $x \notin H$ but

$C - x \subseteq H$. Moreover, $x \in \text{cl}(C - x)$ hence $x \in \text{cl}(H) = H$. Then $x \notin C^*$, a contradiction. □

The following proposition exactly dualizes the argument of Proposition 2.1.12.

Proposition 3.1.5. *Let M be a matroid and let B be a basis of M. Then for all $y \in B$, there is a unique cocircuit $C^* \subseteq (E - B) \cup y$.*

The cocircuit described in the above proposition is called the *fundamental cocircuit of y with respect to B* and is denoted as $C^*(y, B)$.

3.1.1 Duals of graphic matroids

While Proposition 3.1.5 holds for all matroids it is not difficult to see the connection with the well-known result in graph theory that associates an edge in a spanning tree of graph G with a fundamental cut of the graph. The first proposition of this section makes precise this intuitive connection between the cocircuits of a graphic matroid and the cuts of the associated graph. Recall that a *bond* is a minimal cut in a graph G.

Proposition 3.1.6. *Let G be a graph with cycle matroid $M(G)$. Then the cocircuits of $M(G)$ are precisely the bonds of G.*

Proof. Recall from Proposition 2.2.8 that given a hyperplane H in a graphic matroid $M(G)$, $E - H$ is a minimal cut in G. Combining this with (iii) of Proposition 3.1.3 gives the result. □

An easy corollary to the above theorem follows from the graph-theoretic result that any cycle and cut in a graph have even intersection.

Corollary 3.1.7. *Let G be a graph with cycle matroid $M(G)$. Let C, C^* be, respectively, a circuit and cocircuit in $M(G)$. Then $|C \cap C^*|$ is even.*

When considering the duals of graphic matroids, it is natural to ask which graphic matroids have duals which are also graphic. In other words, how do we characterize those graphs which have graphic cocycle matroids? The next theorem, our main result regarding cographic matroids, shows that these are exactly the *planar graphs*.

Theorem 3.1.8. *A graph G is planar if and only if $M^*(G)$ is graphic. Furthermore, $M(G^*) = M^*(G)$.*

Our proof of this theorem will roughly follow that given in [7]. First we review the necessary background.

Recall that a planar graph G is a graph which admits a plane drawing, i.e., an embedding in the plane such that no two edge cross each other. Such an embedding is called a *plane graph*. The *dual graph* of a plane graph, denoted G^*, has a vertex for each face and an edge across every edge of G which separates two faces; an edge of G contained in a face corresponds to a loop in G^*. It is known that the dual of the complement of a spanning tree in G is a spanning tree in G^*; we shall make use of this fact in the proof of Theorem 3.1.8.

Kuratowski's theorem, a celebrated result in graph theory, characterizes planar graphs. Recall that K_5 is the complete graph on 5 vertices; $K_{3,3}$ is the complete bipartite graph with 3 vertices in each partition. A graph G' is a topological minor of a graph G if G contains a subgraph isomorphic to G' via subdivisions of edges or removal of degree 2 vertices.

Theorem 3.1.9 (Kuratowski)**.** *A graph is planar if and only if it has neither K_5 nor $K_{3,3}$ as a topological minor.*

Kuratowski's theorem motivates the next lemma, which will allow us to prove Theorem 3.1.8.

Lemma 3.1.10. *Neither $M^*(K_5)$ nor $M^*(K_{3,3})$ is graphic.*

Proof. We first show that $M^*(K_5)$ is not graphic. The proof is by contradiction. Say that $M^*(K_5)$ is isomorphic to the cycle matroid of some graph G. Observe that K_5 has ten edges and that a spanning tree of K_5 has four edges. Therefore $M(K_5)$ has ten elements and $r(M(K_5)) = 4$. So $M^*(K_5) \cong M(G)$ has ten elements and rank 6, thus G has ten edges and a spanning tree of G has six edges. Hence G is a graph with seven vertices and ten edges, hence an average vertex degree $2|E(G)|/|V(G)| = 20/7 < 3$. This implies that G has a vertex with degree at most 2, hence a minimal cut of cardinality 1 or 2. This implies that $M^*(G)$ has a circuit of cardinality 1 or 2 but $M^*(G) \cong (M^*(K_5))^* = M(K_5)$, but if this were true then K_5 would have a loop or a set of parallel edges and we have a contradiction.

To show that $M^*(K_{3,3})$ is not graphic, we again proceed by contradiction. Assume $M^*(K_{3,3}) \cong M(G)$ for some graph G. Similarly to the case of K_5, we note that $M(K_{3,3})$ has nine elements and rank 5. So $M(G)$ will have nine elements and rank 4, implying that G is a graph with nine edges and five vertices. Then G has average vertex degree $18/5 < 4$, hence a vertex v with $d(v) \leq 3$. So $M^*(G) \cong M(K_{3,3})$ has a circuit of cardinality at most 3, a contradiction. □

We are now ready to prove that planar graphs are exactly those with graphic cocycle matroids.

Proof of Theorem 3.1.8. Say G is planar, so G^* exists and is planar. Recall that the dual of the complement of a spanning tree T of G is a spanning tree T^* of G^*. Thus the edges of T^* are in bijective correspondence with the edges of $G \setminus T$. Thus the bases of $M(G^*)$ are the complements of the bases of $M(G)$, that is $M(G^*) = M^*(G)$; furthermore, $M^*(G)$ is graphic.

Now suppose $M^*(G)$ is graphic. Therefore, by Lemma 3.1.9, G cannot contain K_5 or $K_{3,3}$ as a minor. Then by Kuratowski's theorem, G is planar. □

3.1.2 Duals of representable matroids

Recall that given an $n \times m$ matrix A with entries in some field $\mathbb{K}$, we can apply elementary row operations to put the matrix in the standard form $[I_r|D]$ while preserving the vector matroid $M(A)$.

Theorem 3.1.11. *Let M be a vector matroid with standard representation $A = [I_r|D]$. Then the vector matroid associated to $A^* = [-D^T|I_{n-r}]$ is the dual matroid M^*.*

Proof. Let E be the ground set of M. As A and A^* have the same number of columns, we may also index the columns of A^* by E. Note that $r(M) = r$. Let B be a basis of M. We will find a set of columns in A^* corresponding to a basis $B^* = E \setminus B$ of $M(A^*)$.

Consider the following block decomposition of A:

$$A = \left[\begin{array}{c|c|c|c} I & 0 & D_{11} & D_{12} \\ \hline 0 & I & D_{21} & D_{22} \end{array}\right].$$

We can arrange the columns of A (and therefore of A^*) so that the elements of B correspond to the middle two blocks of columns in A. Because B is a basis, the columns of D_{11} are linearly independent. Therefore the first and fourth column blocks of

$$A^* = \left[\begin{array}{c|c|c|c} -D_{11}^T & -D_{21}^T & I & 0 \\ \hline -D_{12}^T & -D_{22}^T & 0 & I \end{array}\right]$$

are a maximal linearly independent set of columns. Call this set of columns B^*. Then B^* is a basis for $M(A^*)$. Further, $B^* = E \setminus B$; this shows that B^* corresponds to a basis for M^*. □

The following corollary is immediate.

Corollary 3.1.12. *If a matroid M is representable over a field $\mathbb{K}$, then the dual matroid M^* is also representable over $\mathbb{K}$.*

The following proposition illustrates the connection between matroid duality and vector space orthogonality.

Proposition 3.1.13. *Let $A = [I_r|D]$ and $A^* = [-D^T|I_{n-r}]$. Then the row spaces of A and A^* are orthogonal complements.*

Proof. This follows from the construction of A and A^*. Notice that the rows of both matrices have length n. In particular, the rows of the submatrix $-D^T$ have length r and the rows of D have length $n-r$. Recall that taking the transpose of a matrix preserves the position of the diagonal entries, thus the diagonal entries of $-D^T$ are exactly the negatives of the diagonal entries of D. Further, the diagonal entries of D and $-D^T$ are the only entries which will be multiplied by the non-zero entries in I_{n-r} and I_r (respectively) in the bilinear form over $\mathbb{K}$. Then for any a_i in A and a'_i in A^*, we have

$$\langle a_i, a_j \rangle = \sum_{k=1}^{n} a_{ik}a'_{ik} = a_{ii} + a'_{ii} = a_{ii} - a_{ii} = 0.$$

Now observe that both A and A^* are full rank, thus the row space of A has dimension r and the row space of A^* has dimension $n-r$. $\square$

Example 3.1.14. In Example 2.2.10, we saw that the matrix

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

represents $M(K_4)$ over $\mathbb{R}$. Then the matrix

$$A^* = \begin{bmatrix} -1 & -1 & 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 1 & 0 \\ -1 & 0 & -1 & 0 & 0 & 1 \end{bmatrix}$$

represents $M^*(K_4)$ over $\mathbb{R}$. It is not difficult to see that the geometric representation of $M^*(K_4)$ in Figure 3.1 corresponds to the vector matroid $M(A^*) = M^*(K_4)$. It is also straightforward to observe that every row of A^* is orthogonal to every row of A.

3.2 Minors

Recall that a graph G' which can be obtained from a graph G by deleting and contracting edges is called a minor of G. We may similarly define a minor M' of a matroid M.

3.2.1 Deletion and contraction

Let M be a matroid on ground set E, and let $X \subseteq E$. Recall that the *restriction* of a matroid, denoted $M|_X$, is simply the matroid we obtain by restricting the independent sets, etc. of M to elements of X. If $Y = E - X$ may equivalently refer to the *deletion* of Y from M, $M \backslash Y$. We define the *contraction* of X from M to be $M/X = (M^* \backslash X)^*$. A matroid M' obtained from M by a sequence of deletions and contractions is said to be a *minor* of M.

It is straightforward to determine the bases of $M \setminus e$ and M/e; from these bases one may find the other distinguished sets of $M \setminus e$ and M/e. Our development of this material is standard, see e.g. [7] or [17].

Proposition 3.2.1. *Let M be a matroid on ground set E. Let $e \in E$ be such that e is not a coloop. Then the bases of $M \setminus e$ are the bases of M which do not contain e.*

Proof. Let B_1 be a basis for M such that $e \notin B_1$ and let B_2 be a basis for M such that $e \in B_2$. Then B_1 is still a maximal independent set in $M \setminus e$. On the other hand, the image of B_2 in $M \setminus e$ is $B_2 - e$ and $|B_2 - e| < |B_1|$, hence $B_2 - e$ is not a basis of $M \setminus e$. □

Proposition 3.2.2. *Let M be a matroid on ground set E and let $e \in E$ be such that e is not a loop. Then B is a basis of M/e if and only if $B \cup e$ is a basis of M.*

Proof. Say $B \in \mathcal{B}(M/e)$. Recall that $M/e = (M^* \setminus e)^*$. So $B' = (E - e) - B$ is a basis for $M^* \setminus e$, hence for M^* as well. Therefore $E - B' = B \cup e$ is a basis for M.

Now suppose $B \cup e \in \mathcal{B}(M)$. So $B' = E - (B \cup e)$ is a basis for M^*, hence for $M^* \setminus e$. Then $(E - e) - B' = B$ is a basis for $(M^* \setminus e)^* = M/e$. □

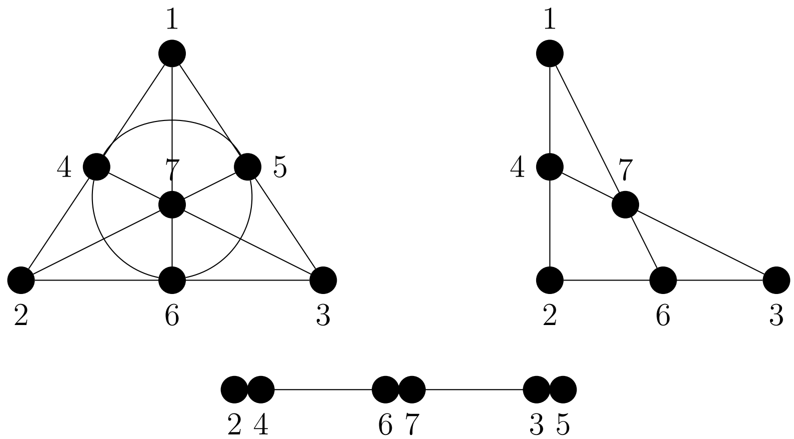

Figure 3.2: The Fano plane F_7 (top left), the deletion $F_7 \setminus 5$ (top right), and the contraction $F_7/1$ (bottom). See Example 3.2.1.

Proposition 3.2.3. *Let M be a matroid and e be either a loop or coloop. Then $M \setminus e = M/e$.*

Proof. Let e be a loop. Then e is in no bases of M. Therefore all $B \in \mathcal{B}(M)$ are in $\mathcal{B}(M \setminus e)$. Likewise, contracting e does not does not change the bases of M, hence $B \in \mathcal{B}(M)$ implies that $B \in \mathcal{B}(M/e)$. Then $\mathcal{B}(M \setminus e) = \mathcal{B}(M/e)$ and this gives the result.

Now suppose that e is a coloop in M. Then e is in every basis of M, hence all bases in M/e are of the form $B - e$ for some $B \in \mathcal{B}(M)$. This is precisely the form of the all bases of $M \setminus e$, and the result follows. □

Example 3.2.4. Consider the three matroid representations in Figure 3.2. The matroid on the top left is the Fano plane, the projective geometry on seven points. Any three colinear points or four non-colinear points form a circuit and we interpret the center circle as a line, so $\{4, 5, 6\}$ form a circuit. The bases of F_7 are the 3-element sets of non-colinear points. In particular, $B_1 = \{1, 2, 3\}$ and $B_2 = \{2, 5, 6\}$ are bases of F_7.

The matroid on the top right of Figure 3.2 is the deletion $F_7 \setminus 5$; note that $B_1 \in \mathcal{B}(F_7 \setminus 5)$, but clearly $B_2 \notin \mathcal{B}(F_7 \setminus 5)$. It is also worth noting that $F_7 \setminus 5$ is isomorphic to $M(K_4)$, as can be seen by comparing Figures 3.2 and 2.3; indeed, it is not difficult to see that $F_7 \setminus e \cong (M(K_4))$ for all e. The matroid at the bottom is $F_7/1$. The image of B_1 in $F_7/1$, $\{2, 3\}$, is a basis for $F_7/1$, but B_2 is a dependent set.

If G is a graph, and $X \subseteq E(G)$, then it is clear that $M(G) \setminus X = M(G \setminus X)$. Therefore $M(G) \setminus X$ is also graphic, as $G \setminus X$ is also a graph. Similarly, let A be a matrix over a field $\mathbb{K}$ with columns indexed by a set E, and vector matroid $M(A)$. Let $X \subseteq E$ and let $A \setminus X$ be the matrix obtained from A by deleting the columns with indices in X. Then it is clear from the definition of deletion that $M(A) \setminus X = M(A \setminus X)$. It follows that $M(A) \setminus X$ is also representable over $\mathbb{K}$.

The next two propositions show that contractions of graphic matroids are graphic and that contractions of representable matroids are also representable. Thus all minors of graphic (representable) matroids are graphic (representable). A class of matroids all of whose minors are also members of the same class is said to be *closed under minors*.

Proposition 3.2.5. *Every minor of a graphic matroid is graphic.*

Proof. Let G be a graph, and $X \subseteq E(G)$. We know that $M(G) \setminus X$ is graphic; it remains to be shown that $M(G)/X = M(G/X)$ for all $X \subseteq E$. The proof is by induction on $|X|$.

For the base case, $X = e$. If e is a loop, then $G \setminus e = G/e$ is also a graph, hence $M(G)/e = M(G) \setminus e = M(G \setminus e) = M(G/e)$. Now say e is not a loop. Let

$Y \subseteq E(G) - e$. Let v_e be the vertex obtained by contracting e in G. Observe that e is in a cycle in G if and only if v_e is a vertex in a cycle in G/e. Then $Y \cup e \in \mathcal{I}(M(G))$ if and only if $Y \in \mathcal{I}(M(G/e))$, i.e. $\mathcal{I}(M(G)/e) = \mathcal{I}(M(G/e))$.

Now say $|X| = n$. By induction, the proposition holds for $|X'| = n - 1$. So $\mathcal{I}(M(G)/\{e_1, \ldots, e_{n-1}\}) = \mathcal{I}(M(G/\{e_1, \ldots, e_{n-1}\}))$. The remainder of the argument is identical to that in the base case, and this completes the proof. □

Proposition 3.2.6. *A matroid M is representable over a field $\mathbb{K}$ if and only if every minor of M is also representable over $\mathbb{K}$.*

Proof. Let A be a matrix representing M over $\mathbb{K}$ with columns indexed by a set E. Let $X \subseteq E$. We know that $M(A) \backslash X = M(A \backslash X)$ is representable over $\mathbb{K}$; moreover, M^* is also $\mathbb{K}$-representable. Then by the definition of contraction, $M(A)/X = (M^*(A) \backslash X)^*$ is representable over $\mathbb{K}$.

Now suppose that every minor of M is representable over $\mathbb{K}$. Then M is representable over $\mathbb{K}$ as M is a minor of itself. □

In the proof of the previous proposition, we took the direct sum of two matrices representing distinct matroids to obtain a third matroid. The next section more closely examines the extension of the direct sum operation to matroids.

3.2.2 Direct sums

There are several ways to characterize matroid connectivity. Whitney [19] first developed the notion in terms of graph connectivity, using the rank function; Welsh [17] defines connected matroids via their circuit sets; Oxley [11] discusses both of these approaches and others as well. Our approach will be via direct sums, as in [7] and [11].

Given two matroids M_1 and M_2 with disjoint ground sets E_1 and E_2 respectively, we define the *direct sum* of M_1 and M_2, written as $M_1 \oplus M_2$, to be the matroid on $E_1 \sqcup E_2$ with bases

$$\mathcal{B}(M_1 \oplus M_2) = \{B_1 \sqcup B_2 : B_1 \in \mathcal{B}(M_1) \text{ and } B_2 \in \mathcal{B}(M_2)\}.$$

It is not immediately evident that $M_1 \oplus M_2$ is indeed a matroid, but the proof is routine.

Proposition 3.2.7. *Let M_1 and M_2 with disjoint ground sets E_1 and E_2 respectively, and let $M = M_1 \oplus M_2$. Then M is a matroid with bases as described above.*

Proof. We show that M satisfies the basis axioms. Clearly $\mathcal{B}(M) \neq \emptyset$, hence (B1) is satisfied. Now say $B, B' \in \mathcal{B}(M)$. Then $B = B_1 \sqcup B_2$ where $B_1 \in \mathcal{B}(M_1)$ and $B_2 \in \mathcal{B}(M_2)$ and $B' = B'_1 \sqcup B'_2$ where $B'_1 \in \mathcal{B}(M_1)$ and $B'_2 \in \mathcal{B}(M_2)$. If $x \in B' - B$, then either $x \in B'_1 - B_1$ or $x \in B'_2 - B_2$. In the first case there exists a $y \in B_1 - B'_1$ such that $(B_1 - x) \cup y \in \mathcal{B}(M_1)$; the argument for the second case is identical. In either case there exists a $y \in B - B'$ such that $(B' - x) \cup y \in \mathcal{B}(M)$ and (B2) is satisfied. □

A matroid M is *connected* if it cannot be expressed non-trivially as a direct sum of matroids; equivalently, M is connected, for all $x, y \in M$, there is a $C \in \mathcal{C}(M)$ such that $x, y \in C$. If M is not connected, M is said to be *separable*. If $M = M_1 \oplus M_2$ is separable, then we call M_1 and M_2 the *components* of M. Evidently M_1 and M_2 are minors of M; in particular $M_1 = M \setminus M_2$ and $M_2 = M \setminus M_1$. A *separation* of M is a partition (X, Y) of $E(M)$ such that $r(X) + r(Y) = r(M)$. A k-separation of M is a partition (X, Y) of $E(M)$ such that $|X|, |Y| \geq k$ and $r(X) + r(Y) - r(M) < k$.

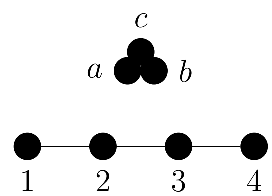

Figure 3.3: The matroid $M = U_{2,4} \oplus U_{1,3}$. See Example 3.2.8.

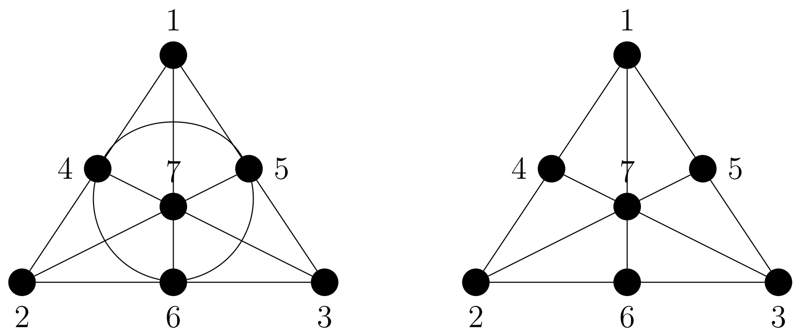

Figure 3.4: The Fano matroid F_7 (left) and the non-Fano matroid F_7^- (right). See Example 3.2.9.

A matroid is n-connected if there is no positive integer $k < n$ such that M has a k-separation.

Example 3.2.8. Recall that the uniform matroid $U_{r,n}$ is the matroid on n elements with all sets of cardinality less than r independent. Consider the matroid M in Figure 3.3. $M = U_{2,4} \oplus U_{1,3}$ with $E_1 = [4]$ and $E_2 = \{a, b, c\}$. Then $\{1, 2, a\}$ is a basis for M, as is any set in $E_1 \sqcup E_2$ of the form $B \cup B'$ where $B \in \mathcal{B}(U_{2,4})$ and $B' \in \mathcal{B}(U_{1,3})$. Similarly, the circuits of M are of the form $C \cup C'$ where $C \in \mathcal{C}(U_{2,4})$ and $C' \in \mathcal{C}(U_{1,3})$, so e.g., $\{1, 2, 3, a, b\} \in \mathcal{C}(M)$.

We end this chapter with an example showing a non-representable matroid.

Example 3.2.9. Recall the Fano matroid F_7 from Example 3.2.1. The non-Fano matroid F_7^- is obtained from F_7 by relaxing the requirement that $\{4,5,6\}$ forms a circuit. Both are shown in Figure 3.4. Let A be the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

with columns indexed by [7]. It is not hard to see that A is representation of F_7 over $\mathbb{F}_2$. The relaxation of the requirement that $\{4,5,6\}$ form a circuit gives a representation of F_7^- over $\mathbb{F}_3$. We claim that if $M \in \{F_7, F_7^-\}$ is representable over a field $\mathbb{K}$, then A is the only representation of M over $\mathbb{K}$. This will prove the following.

Proposition 3.2.10. *The Fano matroids F_7 is representable over $\mathbb{K}$ if and only if the characteristic of $\mathbb{K}$ is 2. The non-Fano matroid F_7^- is representable over $\mathbb{K}$ if and only if the characteristic of $\mathbb{K}$ is 3.*

There are several ways to prove this result; we prefer this method found in [11].

We can always assume that $A = [I_3|D]$, so the columns of I_3 represent elements $1,2,3$ in M. We may write $[1\ 1\ 1]^T$ for column 7, as 7 is a member of dependent sets containing $1,2,3$. So column 4 must be $[1\ a\ 0]^T$, 5 must be $[1\ 0\ b]^T$, and 6 must be $[0\ 1\ c]^T$. Note that $\{1,6,7\}$ is a circuit, hence $c = 1$. Likewise $\{3,4,7\}$ is a circuit, hence $a = 1$. Finally, $\{2,5,7\}$ is a circuit and this forces $b = 1$. The proposition follows.

We may now produce a non-representable matroid, namely $M = F_7 \oplus F_7^-$. If M were representable over some field $\mathbb{K}$, then one or both of F_7, F_7^- would be representable over fields of character other than 2 (respectively, 3).

Chapter 4

Regular matroids

A representable matroid M is one which is isomorphic to a vector matroid $M(A)$, where A is a matrix over some field $\mathbb{K}$. A *regular matroid* is one which has a totally unimodular representation over $\mathbb{R}$; we shall show that such a matroid is in fact representable over any field. Much of the theory of regular matroids was developed by Tutte [15], who characterized regular matroids not only in terms of representability, but also, in an important result, in terms of *excluded minors*, those matroids which are minimal obstructions to representability over some field.

4.1 Representability

This section will be devoted to proving the following theorem, due to Tutte [15], which establishes three equivalent definitions of a regular matroid. Recall that a matrix A over $\mathbb{R}$ is *totally unimodular* if every square submatrix A' of A is such that $\det(A') \in \{0, \pm 1\}$. If we wish to emphasize this aspect of a regular matroid M, we shall simply say that M is totally unimodular.

Theorem 4.1.1. *Let M be a matroid. Then the following are equivalent:*

(i) M is totally unimodular.

(ii) M is representable over every field.

(iii) M is representable over $\mathbb{F}_2$ and another field of characteristic $\neq 2$.

Generally, we shall follow the presentation of the basic theory of regular matroids in terms of representability in the standard reference [11]; this presentation is more modern but essentially the same as Tutte's.

A basic operation in linear algebra is transforming a matrix A into row echelon form via a process some authors refer to as "pivoting", which transforms the j^{th} column of A into the i^{th} standard basis vector, provided $a_{ij} \neq 0$. Briefly, each row k where $k \neq i$ is replaced by row $k - (a_{kj}/a_{ij})$ row j, resulting in all zero entries in column j other than a_{ij}; then row i is multiplied by $1/a_{ij}$ and this sets $a_{ij} = 1$. The following lemma shows that a matrix obtained from a totally unimodular matrix by a pivot operation is again totally unimodular.

Lemma 4.1.2. *Let A be a totally unimodular matrix. If B is obtained from A by a pivoting operation on an entry a_{ij}, then B is totally unimodular.*

Proof. Let B' be a square submatrix of B; we will show that $\det(B') \in \{0, \pm 1\}$. Say A' is the corresponding submatrix of A. Say i is a row in B' (and so also in A'). Recall from linear algebra that scaling a row or column of a matrix by a constant c changes the determinant by a factor of c; also recall that replacing a row r by a linear combination of r and a scalar multiple of another row does not change the determinant. Therefore, $\det(B') = \det(A')$.

Now suppose i is not a row in B'. If j is a column of B', then the j^{th} column of B' is zero, hence $\det(B') = 0$. Suppose j is not a column in B'. Construct matrices A'' and B'' by adjoining row i and column j to A' and B' respectively. As in the previous case, $\det(A'') = \det(B'')$ and, as the only non-zero entry in column j in B'' is 1, we have $\det(A'') = \det(B'') = \det(B')$, hence $\det(B') \in \{0, \pm 1\}$. □

The previous lemma will allow us to prove the following lemma, which makes precise the relation between a regular matroid and its totally unimodular matrix representation.

Lemma 4.1.3. *Let M be a matroid of rank $r \neq 0$ and let $B = \{b_1, \dots, b_r\}$ be a basis for M. Then M is regular if and only if there is a totally unimodular matrix of the form $[I_r|D]$ representing M.*

Proof. If such a matrix represents M, then clearly M is regular by definition.

Recall that any representable matroid M on a ground set E with m elements has a standard representation of the form $[I_r|D]$, where r is the rank of the matroid, I_r the $r \times r$ identity matrix and D an $r \times (m - r)$ matrix. Therefore, if $M \cong M(A)$ for some totally unimodular matrix A, Lemma 4.1.2 guarantees that we may pivot successively on r non-zero elements of A to obtain a totally unimodular matrix A' with r standard basis vectors. Interchanging rows or columns to put A' into the desired form will change the determinant by at most a sign change, hence M is represented by a totally unimodular matrix of the desired form. □

Lemma 4.1.4. *Let D_1 be a matrix with all entries in $\{0, \pm 1\}$ such that $[I_r|D_1]$ is a representation of a binary matroid M over $\mathbb{K}$ where $\mathbb{K}$ has characteristic $\neq 2$. Let*

$[I_r|D_2]$ *be obtained from* $[I_r|D_1]$ *by pivoting on an entry* $d_{ij} \in D_1$. *Then every entry in* D_2 *is also in* $\{0, \pm 1\}$.

Proof. It is clear from the construction of D_1 and the definition of the pivoting operation that all entries of D_2 in row i and column j are in $\{0, \pm 1\}$. Consider the entries in the other rows and columns of D_2, i.e. those d_{kl} for $k \neq i$ and $l \neq j$. Again by construction of D_1, after the pivoting operation all such $d_{kl} \in D_1$ will be replaced in D_2 by $(1/d_{ij})(d_{ij}d_{kl} - d_{kj}d_{il}) \in \{0, \pm 1\}$ unless $(d_{ij}d_{kl} - d_{kj}d_{il}) \in \{\pm 2\}$. Assume that this is the case; then D_1 has a submatrix D_1' such that $\det(D_1') \in \{\pm 2\}$.

Let $D^{\#}$ be the matrix obtained by replacing all non-zero entries in D_1 by 1. Then $[I_r|D^{\#}]$ is a representation of M over $\mathbb{F}_2$ hence $[I_r|D_1]$ represents M over $\mathbb{F}_2$. Then $\det(D_1') = 0$ over $\mathbb{F}_2$. We claim that $\det(D_1') = 0$ over $\mathbb{K}$ as well. To prove the claim, let B be a basis for M and $|B| = r$. Say the rows of D_1' are indexed by $\{p_1, \ldots, p_g\}$ and the columns by $\{c_1, \ldots, c_g\}$. Then $\det(D_1') \neq 0$ over $\mathbb{F}_2$ if and only if $B - \{p_1, \ldots, p_g\} \cup \{c_1, \ldots, c_g\}$ is a basis for M over $\mathbb{F}_2$, and this is the case if and only if $B - \{p_1, \ldots, p_g\} \cup \{c_1, \ldots, c_g\}$ is a basis for M over $\mathbb{K}$, hence $\det(D_1') \neq 0$ over $\mathbb{K}$. But this contradicts our previous assertion on $\det(D_1') \in \{\pm 2\}$ over $\mathbb{K}$. □

Note that in particular the above result holds for $\mathbb{K} = \mathbb{R}$.

We require the following technical lemma in order to prove that (iii) implies (ii) in our main theorem. The proof of the lemma is as in [11]. The matrix $D^{\#}$ is as defined in the proof of Lemma 4.1.4. $G(D^{\#})$ is defined to be the bipartite graph induced by $D^{\#}$, i.e., we take the rows as the vertices on one side of the bipartiton and the columns as the other; a non-zero entry indicates an edge between two vertices. Recall that a *chord* is an edge connecting two non-adjacent vertices of a cycle.

Lemma 4.1.5. *Let* $\mathbb{K}$ *be a field and let* $[I_r|D]$ *be a representation of a binary matroid*

M over $\mathbb{K}$. Let B_D be a basis for the cycle matroid $M(G(D^{\#}))$. If every entry of D corresponding to an edge in B_D is 1, then every other non-zero entry of D has a uniquely determined value in $\{\pm 1\}$.

Proof. Let d be any non-zero entry in D not corresponding to an edge in B_D, and call the corresponding edge in $G(D^{\#})$ e_d. Then $B_D \cup e_d$ gives the fundamental cycle in $G(D^{\#})$ of e_d with respect to B_D, call it C_d. The proof is by induction on $|C_d|$.

C_d contains k edges for some $k \geq 2$, hence there are k rows and k columns of D corresponding to edges in C_d. Take D_d to be the submatrix of D corresponding to those rows and columns. In each row and column of D_d, there are two non-zero entries corresponding to edges in C_d. If D_d contains other non-zero entries, then those entries correspond to chords in C_d. Let d' be such an entry. Thus we have another cycle $C_{d'}$ and $|C_{d'}| < |C_d|$. By induction, $d' \in \{\pm 1\}$, so every every entry of D_d except possibly d is in $\{0, \pm 1\}$.

Let $G(D_d^{\#})$ be the subgraph of $G(D^{\#})$ induced by $V(C_d)$. Take C'_d to be the shortest cycle in $G(D_d^{\#})$ containing e_d. Then D'_d is a submatrix of D_d induced by $V(C'_d)$ with j rows and columns for some $j \leq k$ with exactly two non-zero entries corresponding to edges in C'_d and no others. Moreover, all entries in D'_d are ± 1 except possibly d. If D_d contains no non-zero entries, then the same argument holds, simply by taking $D'_d = D_d$.

Consider $\det(D'_d)$. As D'_d has entries in $\{\pm 1, d\}$, there are exactly two non-zero terms in the summation of the determinant. Therefore, $\det(D'_d) \in \{1+d, 1-d, -1+d, -1-d\}$. Because M is binary, we know that $[I_r|D^{\#}]$ represents M over $\mathbb{F}_2$. This forces $d = 1$ in $D^{\#}$, hence $\det(D'_d) = 0$ over $\mathbb{F}_2$. Then, by an argument identical to that in Lemma 4.1.4, $\det(D'_d) = 0$ over $\mathbb{K}$ as well. Hence d has a unique value in $\{\pm 1\}$. The inductive step simply repeats the previous argument and the result follows. □

We may now prove Theorem 4.1.1.

Proof of Theorem 4.1.1. We will first show that (i) implies (ii); that (ii) implies (iii) is trivial. The bulk of the proof will be devoted to showing that (iii) implies (i).

Let M be totally unimodular. Then by Lemma 4.1.3, M has a totally unimodular representation of the form $A = [I_r|D]$. Let B be a basis of M; we will also use B to denote the corresponding columns of A. Then $\det(B) \in \{\pm 1\}$ over $\mathbb{R}$. Thus $\det(B)$ is non-zero over an arbitrary field $\mathbb{K}$. This implies that B is also a basis for A over $\mathbb{K}$, hence M is representable over $\mathbb{K}$ by A.

Now suppose that M is binary and representable over some field $\mathbb{K}$ with characteristic $\neq 2$. We will show that M is totally unimodular. Let A be the standard representation for M over $\mathbb{K}$. Let B_D be a basis for the cycle matroid of $G(D^{\#})$. We may assume that all entries in D corresponding to elements of B_D are 1. By Lemma 4.1.4, all other entries in D are in $\{0, \pm 1\}$. Recall from the proof of Lemma 4.1.4 that, for every square submatrix D' of D, $\det(D') = 0$ over $\mathbb{K}$ if and only if $\det(D') = 0$ over $\mathbb{R}$. It is clear that if $\det(D') = 0$ over $\mathbb{R}$, then $\det(D') = 0$ over $\mathbb{K}$. We will show the converse by proving that if $\det(D') \neq 0$ over $\mathbb{R}$, then $\det(D') \in \{\pm 1\}$ over $\mathbb{R}$.

Say D' has k columns and $\det(D') \neq 0$. Let d_{ij} be a non-zero entry in D'. By pivoting on this entry in D over $\mathbb{K}$, we can reduce column j to a standard basis vector and this will also be a standard basis vector of length k in D'. Moving this column to the i^{th} position in the standard representation does not alter D', only moves it within A. Furthermore, by Lemma 4.1.2, this pivoting operation will result in a matrix all of whose entries are still in $\{0, \pm 1\}$ and this holds of we consider the matrix over $\mathbb{R}$. By repeated pivots over entries in D, we eventually obtain a matrix in which all columns of D' are standard basis vectors of length k. These operations will at most change the sign of $\det(D')$, thus $\det(D') \neq 0$ over $\mathbb{R}$. Furthermore, all entries in D' are in $\{0, \pm 1\}$, hence $\det(D') \in \{\pm 1\}$ over $\mathbb{R}$ and M is totally unimodular. □

The following result shows that the dual of a regular matroid is also regular.

Proposition 4.1.6. *Let M be a regular matroid. Then the dual matroid M^* is also regular.*

Proof. By Corollary 3.1.12, if M is representable over a field $\mathbb{K}$, then M^* is also representable over $\mathbb{K}$. Thus if M is representable over every field, so is M^*. □

Theorem 4.1.1, together with Corollary 3.1.12 and the discussion following Proposition 2.1.1, immediately proves the following.

Proposition 4.1.7. *Let M be a graphic matroid. Then M and its dual M^* are both regular.*

4.2 Regular matroid decomposition and excluded minors

4.2.1 Seymour's decomposition theorem

In the previous section, we characterized the class of regular matroids as those matroids contained in the intersection of binary and ternary matroids and also as the smallest class of matroids containing both graphic and cographic matroids. A celebrated result due to Seymour [12] shows that in fact, all regular matroids can be constructed from graphic and cographic matroids and a particular binary matroid denoted R_{10} which is neither graphic nor cographic. Oxley points out that Seymour's theorem can thus be understood as addressing the question of what other than graphic and cographic matroids is contained in the class of regular matroids. The proof of this theorem is highly complex and technical, but as it provides an important characterization of regular matroids, we state the theorem below, after summarizing the necessary background.

We have already described direct sums of matroids; two related operations are used in Seymour's theorem. As usual, we follow the standard reference [11]. Let M, N be matroids with at least two elements and $E(M) \cap E(N) = \{e\}$ such that e is neither a loop nor a coloop of M or N. The *2-sum* of M and N, $M \oplus_2 N$, has ground set $(E(M) \cup E(N)) - e$ and circuits

$$\{C \in \mathcal{C}(M) : e \notin C\} \cup \{C \in \mathcal{C}(N) : e \notin C\} \\ \cup \{(C_1 \cup C_2) - e : C_1 \in \mathcal{C}(M), C_2 \in \mathcal{C}(N), e \in C_1 \cap C_2\}.$$

If one considers the geometric representation of a matroid, informally, a 2-sum is easily understood as identifying two matroids at a point. A 3-sum of binary matroids can likewise be informally understood as identifying two matroids along a 3 point line, i.e., a 3-element circuit of M. More formally, we require that M_1 and M_2 be binary matroids on ground sets E_1 and E_2 respectively with both ground sets having at least seven elements. Say $E_1 \cap E_2 = T$ where T is a 3-element circuit of both M_1

and M_2 but $T \cap \mathcal{C}^*(M_1) = T \cap \mathcal{C}^*(M_2) = \emptyset$. The *3-sum* $M_1 \oplus_3 M_2$ is a matroid with ground set $(E_1 \cup E_2) - T$ with circuits $C \in \mathcal{C}(M_1 \setminus T), C' \in \mathcal{C}(M_2 \setminus T)$, and also the non-empty minimal sets of the form $(C_1 \cup C_2) - T$ where $C_1 \in \mathcal{C}(M_1)$, $C_2 \in \mathcal{C}(M_2)$, and $C_1 \cap T = C_2 \cap T \neq \emptyset$. It is a result due to Brylawski that the direct sums, 2-sums, and 3-sums of regular matroids are again regular; see for example [11] or [12].

The matroid R_{10} is represented over $\mathbb{F}_2$ by the following matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

R_{10} has several interesting properties. It is a 3-connected regular matroid that is neither graphic nor cographic; in particular, R_{10} contains both $M(K_{3,3})$ and $M^*(K_{3,3})$ as minors. Moreover, the only regular 3-connected matroid having an R_{10} minor is R_{10} itself.

Theorem 4.2.1 (Seymour's Decomposition Theorem)**.** *Every regular matroid M can be constructed using direct sums, 2-sums, and 3-sums, starting with graphic matroids, cographic matroids, and R_{10}.*

4.2.2 Tutte's excluded minors theorem

This section briefly discusses a theorem due to Tutte [16] which characterizes regular matroids via excluded minors. The proof of this theorem is quite complex; Oxley [11] devotes a large section to what he describes as "the most elementary proof known".

Theorem 4.2.2 (Tutte 1958)**.** *A matroid is regular if and only if it has no minor isomorphic to* $U_{2,4}$*,* F_7*, and* F_7^**.*

From Example 3.2.9, we know that F_7 is binary but not ternary. To see that F_7 is the minimal minor not representable over a field of characteristic $\neq 2$, we recall two other previous examples. Example 3.2.1 showed that $F_7 \setminus e \cong M(K_4)$ for all e, therefore deletions of F_7 are graphic, hence regular. We also saw that contractions of F_7 give a rank 2 matroid with three dependent pairs and any three elements forming a dependent set. This is exactly a 3-cycle with each edge replaced by a pair of parallel edges, hence contractions of F_7 are graphic and regular. By Corollary 3.1.12, a matroid M is representable over a field $\mathbb{K}$ if and only if its dual M^* is also representable over $\mathbb{K}$, hence the result for F_7^* follows.

The difficulty in proving Tutte's excluded minor theorem lies in showing the converse - that $U_{2,4}$, F_7 and F_7^* are indeed the only excluded minors for the class of regular matroids. Showing that this holds for F_7 and F_7^* is the bulk of Oxley's material on this theorem.

Showing that any excluded minor for binary matroids must be $U_{2,4}$ is more straightforward, as the next proposition shows. Our proof follows that given in [7].

Proposition 4.2.3. $U_{2,4}$ *is an excluded minor for the class of regular matroids. In particular a matroid is binary if and only if it does not contain a* $U_{2,4}$ *minor.*

Sketch of proof. The proof in one direction has already been shown in previous examples throughout this thesis. We know that from Example 2.1.13 that $U_{2,4}$ is not graphic, hence cannot be binary. To see that it is the minimal such minor, note that removing any one element from $U_{2,4}$ we obtain a matroid on three elements with a 2-element basis. This is exactly a 3-cycle, hence $U_{2,4} \setminus e$ is graphic hence binary for all e. If we contract an element in $U_{2,4}$, we obtain $U_{1,3}$ and this is the matroid of the graph consisting of three parallel edges between two vertices.

Suppose M is a non-binary matroid. We claim that M has a $U_{2,4}$ minor. We will use the fact that for binary matroids, $|C \cap C^*|$ is even for all circuits C and cocircuits C^* (this is proven in Proposition 5.2.5 below). Therefore M has a circuit C and cocircuit C^* such that $|C \cap C^*|$ is odd. This means $|C \cap C^*| \geq 3$ as $|C \cap C^*| \neq 1$ by Proposition 3.1.4; say $\{x, y, z\} \subseteq C \cap C^*$. It follows that $r(M) \geq 2$, hence $H = E - C^*$ is a hyperplane of rank ≥ 1 and H contains a rank $r(M) - 2$ flat F. Assume that F can be chosen so that $C \cap F$ is a basis for F, so $C = \{x, y, z, e_1, \ldots, e_{r(M)-2}\}$ and $B(F) = \{e_1, \ldots, e_{r(M)-2}\}$.

We claim that F is covered by 4 distinct hyperplanes $H, F \cup x, F \cup y$, and $F \cup z$. All are indeed hyperplanes as all have rank $r(M) - 1$. To see that they are distinct, suppose without loss of generality that $F \cup x = F \cup y$. Then $\{x, y, e_1, \ldots e_{r(M)-2}\}$ is a basis for M, a contradiction. Contracting a basis for F leaves us with a rank 2 matroid. Any other elements in F will be loops after this; deleting these loops leaves four rank 1 flats, and we conclude that M contains a $U_{2,4}$ minor. □

4.3 Orientability

We now extend our characterization of regular matroids to allow for the notion of an orientation placed on a matroid. As a matroid abstracts certain common properties of graphs and vector spaces over arbitrary fields, an oriented matroid can intuitively be understood as abstracting similar properties from directed graphs and vector spaces over ordered fields. For material on oriented matroids, Björner et al [4] is the standard reference; Taylor [14] gives a compact and easily accessible presentation of the basic material.

Let M be a matroid on a ground set E. A *signed subset* of E is a map $X : E \to \{0, +, -\}$. Define $\underline{X} \coloneqq \{e \in E : X(e) \neq 0\}$; the set $\underline{X}$ is called the *support* of X. We also define the sets $X^+ \coloneqq \{e \in E : X(e) = +\}$ and $X^- \coloneqq \{e \in E : X(e) = -\}$. An *oriented matroid* $M = (E, \mathcal{C})$ is a non-empty set E with a collection of signed subsets having the following properties:

$(C'1)$ $\mathcal{C} \neq \emptyset$.

$(C'2)$ If $C \in \mathcal{C}$ then $-C \in \mathcal{C}$.

$(C'3)$ If $C_1, C_2 \in \mathcal{C}$ and $\underline{C_1} \subseteq \underline{C_2}$, then either $C_1 = C_2$ or $-C_1 = C_2$.

$(C'4)$ If $C_1, C_2 \in \mathcal{C}$ such that $C_1 \neq -C_2$, and $e \in C_1^+ \cap C_2^-$, there exists $C_3 \in \mathcal{C}$ such that $C_3^+ \subseteq (C_1^+ \cup C_2^+) - e$ and $C_3^- \subseteq (C_1^- \cup C_2^-) - e$.

The elements of $\mathcal{C}$ are called *signed circuits*. It is clear from these axioms that an oriented matroid satisfies the circuit axioms for standard matroids, hence an oriented matroid is indeed a matroid. As in the case with standard matroids, there are several equivalent axiom systems for oriented matroids, but in this paper we are only concerned with the oriented circuit axioms.

In one of the earlier works to introduce the notion of orientability for matroids, Minty [10] defines an orientable matroid M as one which admits a partition of all of its circuits into (C^+, C^-) and all of its cocircuits into (C^{*+}, C^{*-}) such that

$$|C^+ \cap C^{*+}| + |C^- \cap C^{*-}| = |C^+ \cap C^{*-}| + |C^- \cap C^{*+}|.$$

We will say a matroid that meets this condition is *orientable in the sense of Minty.* This is equivalent to saying that we may take a binary representation A of M and change some of the 1's to -1 in such a manner as to make the rows of A and A^T orthogonal to each other. Thus we have the following proposition.

Proposition 4.3.1. *A matroid is orientable in the sense of Minty if and only if it is regular.*

In the standard text on orientable matroids, Björner et al. [4] define an *orientable* matroid M as one whose circuits are the supports of the signed circuits of an oriented matroid. The following definition, given in [8], extends orientability in the sense of Minty to offer a more direct definition of an orientable matroid, based on the observation that if the intersection of the supports of a signed circuit and signed cocircuit is non-empty, then there is at least one coordinate where the signs agree and one where they differ. Then a matroid M is orientable if there is a partition of all of its circuits into (C^+, C^-) and all of its cocircuits into (C^{*+}, C^{*-}) such that, for all $C \in \mathcal{C}$ and $C^* \in \mathcal{C}^*$,

$$(C^+ \cap C^{*+}) \cup (C^- \cap C^{*-}) \neq \emptyset \text{ if and only if } (C^+ \cap C^{*-}) \cup (C^- \cap C^{*+}) \neq \emptyset. \quad (4.1)$$

With this definition, the following proposition is not difficult to prove.

Proposition 4.3.2. *Let M be a matroid representable over the reals. Then M is* *orientable.*

Proof. Let A be a representation of M over $\mathbb{R}$. Then the circuits of M correspond to elements of $\ker(A)$ and by duality, the row space $\mathrm{im}(A^T)$ corresponds to the cocircuits of M. As $\ker(A) = \mathrm{im}(A^T)^\perp$, any $x \in \ker(A)$ will be orthogonal to any vector in the row space of A, hence the non-zero terms in $x^T y$ cannot all have the same sign. $\square$

It follows from the above proposition that all regular matroids are orientable, but not all orientable matroids are regular.

Example 4.3.3. Recall the matroid $U_{2,4}$, which can be represented by the following matrix over $\mathbb{R}$.

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}.$$

The dual matrix is

$$A^* = \begin{bmatrix} -1 & -1 & 1 & 0 \\ -1 & -2 & 0 & 1 \end{bmatrix}$$

We know that $U_{2,4}$ is not graphic and so not regular, but it is orientable. By considering only the signs of elements of $\ker(A)$, we see that $U_{2,4}$ has signed circuits $C_1 = (+,+,-,0), C_2 = (+,+,0,-), C_3 = (+,0,-,+), C_4 = (0,+,+,-)$, and their negatives. Considering the dual matroid A^*, we see that $U_{2,4}$ has signed cocircuits $C_1^* = (0,+,+,+), C_2^* = (+,0,+,+), C_3^* = (-,+,0,+), C_4^* = (+,-,+,0)$, and their negatives. It is not hard to see by inspection that $U_{2,4}$ is orientable under (4.1). However $U_{2,4}$ is not orientable in the sense of Minty. Let $E = \{e_1, \dots, e_4\}$ and label the columns of A, A^* likewise from left to right. Take $C = C_1$ and $C^* = C_4^*$, then

$(C^+ \cap C^{*+}) \cup (C^- \cap C^{*-}) = e_1 \cup \emptyset = e_1$ and $(C^+ \cap C^{*-}) \cup (C^- \cap C^{*+}) = e_2 \cup e_3$, hence

$$|C^+ \cap C^{*+}| + |C^- \cap C^{*-}| \neq |C^+ \cap C^{*-}| + |C^- \cap C^{*+}|.$$

Evidently, the duals and minors of orientable matroids are also orientable. It is also clear that not all matroids are orientable. In particular, F_7 is not orientable and is in fact a minimal example of a non-orientable matroid as all matroids on six or fewer elements are orientable [5]. The non-orientability of F_7 was first shown by Bland and Las Vergnas (1978), who proved it "by exhaustive enumeration of possibilities" [4]. An interesting alternate proof of this fact, given by De Loera et al. [5], uses a system of polynomial equations which have a solution if and only if a given binary matroid is orientable. The following proposition is given as an exercise in [8].

Proposition 4.3.4. *F_7 is not orientable.*

Proof. Number the elements of F_7 as in Examples 3.2.4 and 3.2.9. Suppose F_7 is orientable. We may assume the all circuits containing 1 are positively oriented, so we have (using a superscript to denote orientation) $C_1 = (1^+, 2^+, 4^+), C_2 = (1^+, 6^+, 7^+)$, and $C_3 = (1^+, 3^+, 5^+)$. Then by (4.1), there must exist a cocircuit $C_1^* = (1^+, 4^-, 5^-, 7^-)$. Now look at the circuits $C_4 = (4, 5, 6), C_5 = (3, 4, 7)$, and $C_6 = 2, 5, 7$. By (4.1), C_1^* forces (without loss of generality) the following orientations: $C_4 = (4^+, 5^-, 6), C_5 = (3, 4^+, 7^-), C_6 = (2, 5^+, 7^-)$ where the unlabeled elements in each circuit are not elements of C_1^* hence have no forced orientation. Using the orientations on these six circuits we deduce that we have cocircuits $C_2^* = (3^-, 5^+, 6^-, 7^+)$ and $C_3^* = (2^-, 4^+, 6^-, 7^+)$. Now look at C_4, and say we place a positive orientation on 6, so $C_4 = (4^+, 5^-, 6^+)$. Then $(C_4^+ \cap C_2^{*+}) \cup (C_4^- \cap C_2^{*-}) = \emptyset$ but

$(C_4^+ \cap C_2^{*-}) \cup (C_4^- \cap C_2^{*+}) = \{6\} \cup \{5\} \neq \emptyset$ hence F_7 is not orientable. □

The following proposition, as given in [4], establishes a fundamental relation between regular and orientable matroids.

Proposition 4.3.5. *Let M be a matroid. Then M is regular if and only if M is binary and orientable.*

Proof. Let M be binary and orientable. As M is binary, it contains no $U_{2,4}$ minor; furthermore, because M is orientable, it contains neither F_7 nor F_7^*. Then by Tutte's excluded minor theorem, M is regular. Now suppose that M is regular. Clearly M is binary and orientable. □

We may, analogous to the case of standard matroids, define oriented bases $\mathcal{B}$ of oriented matroids. Likewise, we have a notion of a fundamental oriented circuits $C(e, B)$ where $B \in \mathcal{B}$ and $e \in E - B$ and fundamental oriented cocircuits $C^*(e, B)$ where $e \in B$. The fundamental circuits and cocircuits of oriented regular matroids motivate the theory we develop in the next chapter.

Chapter 5

Circuit and Cocircuit Lattices of Regular Matroids

Given a directed graph G, one may assign real number *preflow* values to each oriented edge; one may consider such an assignment to be a real-valued function on the edge set of G. A *flow* on G is an assignment of preflow values with no accumulation at any vertex, i.e., the incoming flow value equals the outgoing flow value at each vertex. Consider the set of of all preflows as a vector space, then the set of all flows is a linear subspace. The set of all integer-valued flows then forms a lattice (used here in the discrete group sense) denoted $\Lambda(G)$ within this subspace. The dual lattice, denoted $\Lambda(G)^{\#}$, is defined to be the set of all fractional flows having integer dot products with integral flows.

By taking the quotient $\Lambda(G)^{\#}/\Lambda(G)$, Bacher, de la Harpe, and Nagnibeda [1] define a finite abelian group, commonly referred to as the *Jacobian* of the graph, denoted $\mathrm{Jac}(G)$, whose order is the same as the number of spanning trees of G. While the work of Bacher, et al comes largely from the perspective of algebraic geometry, Biggs [3] integrates their work into the wider field which encompasses results from areas as diverse as electrical engineering and chip-firing games on graphs.

The first section of this chapter characterizes the circuit and cocircuit lattices of regular matroids. In the second section, we survey recent results generalizing the Jacobian to the setting of regular matroids; in the final part we extend certain related results due to Eppstein [6] from a graph-theoretic setting to a matroidal one.

5.1 Integral circuits and cocircuits

Our presentation of the background material in this section is drawn primarily from [2] and [13]; for background on lattices, see [9].

Let A be a totally unimodular matrix representing a regular matroid M with entries in $\mathbb{Q}$. Then $\Lambda_A(M) := \{\ker(A) \cap \mathbb{Z}^E\}$ is the *circuit lattice* of M with respect to the representation A. As our previous discussion of vector matroids and regular matroids in particular has shown, M may be represented by more than one matrix, indeed even by more than one totally unimodular matrix. However, Lemma 4.1.2 shows that we may transform one unimodular representation into another by a series of row and column operations. Recall that an *isometry* of lattices Λ and Λ' is a group isomorphism $\varphi : \Lambda \to \Lambda'$ such that both φ and φ^{-1} preserve the bilinear form on the lattices. Then by the previous discussion, the *isometry class* of $\Lambda_A(M)$, denoted $\Lambda(M)$ is independent of A. We briefly note that this discussion indicates another way of viewing a regular matroid, namely as an equivalence class of totally unimodular matrices.

We also define $\Lambda_A^*(M)$, the cocircuit lattice of M with respect to A as $\Lambda_A^*(M) =$

$\mathrm{row}(M) \cap \mathbb{Z}^E$ (here row denotes the row space of A). As in the case of the circuit lattice, and by identical reasoning, the isometry class of $\Lambda^*_A(M)$ is independent of A; this isometry class is denoted $\Lambda^*(M)$. Recall that given M, we may always choose A to be an $r \times m$ totally unimodular matrix $[I_r|D]$ and take the set of column vectors of I_r as a basis B. Then the dual matroid M^* is represented by the matrix $A^* := [-D^T|I_{m-r}]$, and the row spaces of A and A^* are orthogonal. From this it is evident that $\Lambda(M)$ and $\Lambda^*(M^*)$ are isometric. Now consider the totally unimodular matrix $X = A^{*T}$; clearly $AX = 0$. As the rank of X is the dimension of $\ker(A)$, the columns of X form an ordered basis $\beta(M, B)$ for $\Lambda(M)$; this is sometimes called the *fundamental basis* of $\Lambda(M)$ with respect to B.

The following theorem, a folklore result proved by Taylor [14] shows that in fact, every basis of M generates the entire circuit lattice. Our proof essentially follows that given by Taylor, although we have attempted to streamline and clarify certain aspects. Recall that the corank of a matroid is the rank of the dual matroid.

Theorem 5.1.1. *Let M be an oriented matroid. Then the following are equivalent.*

(i) M is regular.

(ii) Every basis of M generates the entire circuit lattice of M.

(iii) The rank of $\Lambda(M)$ equals the corank of M.

Proof. The basic strategy of the proof is to show that *(i)* implies *(ii)* implies *(iii)*, then that *(iii)* implies *(i)*. In order to prove the final implication, we will however need to also show that *(ii)* implies *(i)* and this is the bulk of the proof.

Assume M is regular. By regularity of M, we may represent M over $\mathbb{Q}$ by some matrix A. We will first show that property (ii) holds, then that (ii) implies (iii). Let

$B_i \in \mathcal{B}$ and let $C(B_i)$ be the set of fundamental circuits associated to B_i. Denote the circuit lattice generated by $C(B_i)$ as Λ_i. Likewise define $C^*(B_i)$ as the set of fundamental cocircuits of B_i and denote the cocircuit lattice as Λ_i^*. The circuits of M are the minimal dependent sets and these correspond to the elements of $\ker(A) \cap \mathbb{Z}^E$ with minimal support. We know that the dimension of $\ker(A)$ is the corank of M, hence the rank of $\Lambda(M)$ is at least the corank of M. For each B_i, the fundamental circuits $C(B_i)$ are independent considered as vectors over $\mathbb{Q}$, thus $C(B_i)$ generates all of $\ker(A)$. Now fix one such B_i, and call it B. Then $C(B)$ forms a basis for $\ker(A) \cap \mathbb{Z}^E$ over $\mathbb{Q}$, hence over $\mathbb{Z}$ as well; we conclude that every basis of M generates the entire circuit lattice of M. Note that this implies that the size of a spanning set of independent circuits, i.e. the rank of $\Lambda(M)$, equals the corank of M.

We now show that if each basis generates $\Lambda(M)$, then M is regular (this is (ii) $\Rightarrow$ (i)). Now suppose that all Λ_i are equal and fix a basis B_0. Let A' be the matrix $[I_r|D]$ where the columns of I_r correspond to B_0 and the columns of D are constructed according to their dependencies in their fundamental circuits in $\mathcal{C}(B_0)$. This implies that all entries in all columns of D are in $\{0, \pm 1\}$. Now A' defines some matroid M_0 and the circuits of M_0 are the minimal support elements of $\ker(A') \cap \mathbb{Z}^E$. We will first show that $\mathcal{C}(M) \subseteq \mathcal{C}(M_0)$, then that A' is totally unimodular hence M_0 is regular, and finally we show that $\mathcal{C}(M_0) \subseteq \mathcal{C}(M)$.

By construction, $\mathcal{C}(B_0) \subseteq \mathcal{C}(M_0)$ and by assumption $\mathcal{C}(B_0)$ generates the circuit lattice of M (recall that the B_i are bases of M). Thus a circuit C in M must correspond to a linear dependence in the columns of A'. We need to show that this dependence in A' has minimal support in $\ker(A) \cap \mathbb{Z}^E$, i.e., is a circuit of M'. Suppose not. Then there exists a circuit $C_0 \in \mathcal{C}(M_0)$ such that $\underline{C_0} \subsetneq \underline{C}$. Since C_0 is an element of $\ker(A)$, we can write $C_0 = \sum_i^k q_i c_i$ where $q \in \mathbb{Q}$ and $c_i \in \mathcal{C}(B_0)$. Let j be the least common denominator of the q_i, so jC_0 is an integer linear combination of the c_i, hence jC_0 is in the circuit lattice of M. But this says that jC_0 is a dependent set in M whose support is properly contained in C, contradicting the fact that C is a circuit in M. Thus we conclude that $\mathcal{C}(M) \subseteq \mathcal{C}(M_0)$.

Now we show that A' is unimodular, hence M_0 is regular. We claim that it suffices to show that every support-minimal dependent set of columns of A' can be written with coefficients in $\{\pm 1\}$. Let A'' be a square submatrix of rank r such that the columns of A'' are a basis for A'. We may assume that $\det(A'') \in \{\pm 1\}$ by scaling columns if necessary; such a basis is called a unimodular basis. Consider a column $x \in A' \setminus A''$. Then there is a unique linear dependence between the columns in A'' and x; this gives the fundamental circuit $C(x, A'')$. If the non-zero coefficients of this dependency are in $\{\pm 1\}$, then by Cramer's rule, the non-zero entries of x must also be in $\{\pm 1\}$. To see this, let $A''_{i,x}$ be the matrix obtained by replacing the i^{th} column of A'' with x. Then if $\det(A'') \in \{\pm 1\}$, $\det(A''_{i,x}) \in \{0, \pm 1\}$ for all i. This shows that any basis obtained from a unimodular basis by exchanging one column is also a unimodular basis. As any basis can be obtained from any other by a series of exchanges, it is enough that A' have a unimodular basis. But A' has rank r and contains I_r as a submatrix, and these give a unimodular basis for A'. Thus it suffices to show that all support minimal dependencies of columns of A' may written with coefficients in $\{\pm 1\}$.

Suppose there is such a dependency in A'. Then $a_1 e_1 + \cdots + a_k e_k = 0$ where the e_i are columns of A' and the a_i are non-zero integers such that not all a_i have the same absolute value. This dependence is in $\ker(A)$, hence can be written as an integral linear combination of elements of $\mathcal{C}(B_0)$. Therefore, there is some linear combination of signed circuits in M giving this dependency, and the support of these signed circuits is a dependent set in M, call it C_M. Note that C_M is by definition a circuit in M_0, but is not necessarily a circuit in M. So we have two cases: either C_M is a circuit in M or it is not. Suppose it is; then C_M has minimal support in M. Because all Λ_i are equal, C_M is in Λ_0. Hence $C_M - (a_1e_1 + \cdots + a_ke_k)$ is also in the integral span of $\mathcal{C}(B_0)$. Choose $n \in \mathbb{Z}$ so that at least one term in $nC_M - (a_1e_1 + \cdots + a_ke_k)$ cancels; as not all a_i have the same value, not all terms will cancel. Then there is some other cycle in M' with support strictly contained in $\underline{C_M}$ and this is a contradiction. So suppose that C_M is not a circuit in M, then there is some circuit C'_M in M such that $\underline{C'_M} \subsetneq \underline{C_M}$. But $\mathcal{C}(M) \subseteq \mathcal{C}(M_0)$ hence C'_M is also a circuit in M_0 and we again have a contradiction on the assumption that $C_M \in \mathcal{C}(M_0)$. This shows that every linear dependency in the columns of A' with minimal support must have coefficients in $\{\pm 1\}$, and it follows that M_0 is regular.

Now we show that $\mathcal{C}(M) \subseteq \mathcal{C}(M_0)$; this will complete the proof that if every basis of M generates the entire circuit lattice of M, then M is regular. Let Λ'_j be the lattice generated by the fundamental circuits associated to $B_j \in \mathcal{B}(M_0)$. Because M_0 is regular, all Λ'_j are equal; by hypothesis, all Λ_i are also equal. By construction of A', $\Lambda_0 = \Lambda'_0$. Therefore M and M_0 have the same circuit lattice and a common basis, hence $\mathcal{C}(M) \subseteq \mathcal{C}(M_0)$. As the elements of $\mathcal{C}(M_0)$ are the minimal support elements of $\ker(A) \cap \mathbb{Z}^E$, so are the elements of $\mathcal{C}(M)$. Therefore A is a totally unimodular representation for M, i.e., M is regular.

The final step is to show that if $\text{rank}(\Lambda) = \text{corank}(M)$, then M is regular. We prove the contrapositive. We know that M is regular if and only if every basis of

M generates the entire circuit lattice of M. So suppose M is not regular. Then there exist $B_1, B_2 \in \mathcal{B}(M)$ which generate different circuit lattices. So there is some fundamental circuit $C \in \mathcal{C}(B_2)$ which is not in the $\mathbb{Z}$-span of $\mathcal{C}(B_1)$. We will produce an integrally linear independent set of circuits of size corank$(M) + 1$; this will show that there is no $C_1 \in \mathcal{C}(B_1)$ in the integral span of $(C \cup \mathcal{C}(B_1)) - C_1$. Let $C_1 \in \mathcal{C}(B_1)$ and suppose that $C_1 = aC + a_2C_2 + \cdots + a_kC_k$ where the $a_i \in \mathbb{Z}$ and $C_2, \ldots, C_k \in \mathcal{C}(B_1)$ are distinct from C_1. Because C is not in the $\mathbb{Z}$-span of $\mathcal{C}(B_1)$, $|a| > 1$.

Because $C_1 \in \mathcal{C}(B_1)$, there exists a unique $e_1 \in E - B_1$ such that $e_1 \in \underline{C_1}$ and $e_1 \notin \underline{C_j}$ for $j \neq 1$. So it must be the case that $e_1 \in \underline{C}$, hence $|a| = 1$ as all non-zero coefficients in the dependency of C_1 are in $\{\pm 1\}$. This contradicts the assumption that C is not in the integral span of $\mathcal{C}(B_1)$. It follows that $C \cup \mathcal{C}(B_1)$ is a linearly independent set of circuits of size corank$(M) + 1$ and this completes the proof. □

Note that, by duality, we may apply these results to the case of fundamental cocircuits, showing that M is regular if and only if all Λ_i^* are equal. The proof is identical.

5.2 The Jacobian

In the introduction to this chapter, we discussed the graph Jacobian, an abelian group associated to a graph, as defined in [1] and [3]. In this section we generalize this construction to regular matroids.

The *Jacobian* of a matroid M representable over $\mathbb{Q}$, Jac(M) is defined to be the determinant group of $\Lambda(M)$, i.e., the quotient $\Lambda(M)^{\#}/\Lambda(M)$ where $\Lambda(M)^{\#}$ is the *dual lattice*, to $\Lambda(M)$, i.e.

$$\Lambda(M)^{\#} = \{y \in \mathbb{Q}^E : \langle x, y\rangle \in \mathbb{Z}^E \text{ for all } x \in \Lambda(M)\}.$$

Theorem 5.1.1 allows us to prove the following important corollary, which is discussed in [14] though not formally stated there.

Corollary 5.2.1. *Let M be a matroid representable over $\mathbb{Q}$. Then the Jacobian of M is well-defined if and only if M is regular.*

Proof. Theorem 5.1.1 shows that every basis of M generates all of $\mathrm{Jac}(M)$ if and only if M is regular. Therefore if M is not regular, a given basis B_1 of M may not generate the same lattice as another basis B_2 of M. Then each such lattice will have a different dual, hence by definition a different Jacobian. □

From this point we will assume that all matroids we discuss are regular. Moreover, we assume that all matrix representations A are totally unimodular unless otherwise stated.

Theorem 5.2.2. *There are canonical isomorphisms*

$$\Lambda(M)^{\#}/\Lambda(M) \cong \Lambda^*(M)^{\#}/\Lambda^*(M) \cong \frac{\mathbb{Z}^E}{\Lambda_A(M) \oplus \Lambda_A^*(M)} \cong \textit{coker}\ (AA^T)$$

for all A representing M.

The first two isomorphisms in the preceding theorem are shown for the graphic case in [1]; the final isomorphism is shown in [2].

Proof. Biggs [3] defines the orthogonal projection P from $\mathbb{Z}^E \to \Lambda^*(M)$ in the graphic case at length and shows that $\text{Im}(P) = \Lambda^*(M)^\#$. We claim that the map

$$\varphi : \frac{\mathbb{Z}^E}{\Lambda(M) \oplus \Lambda^*(M)} \to \frac{\text{Im}(P)}{\Lambda^*(M)}$$

given by $[z] \to [Pz]$ where $[z] \in \frac{\mathbb{Z}^E}{\Lambda(M) \oplus \Lambda^*(M)}$ and $[Pz] \in \frac{\text{Im}(P)}{\Lambda^*(M)}$ is an isomorphism; this will show the second isomorphism in the statement of the theorem. The surjectivity of the map is clear. To prove injectivity, we need to show that the if $[Pz] = [0]$, then $[z] = 0$. Observe that the claim is equivalent to the statement that $z \in \mathbb{Z}^E$ is in $\Lambda(M) \oplus \Lambda^*(M)$ if and only if Pz is in $\Lambda^*(M)$. This follows from the identity $z = (z - Pz) + Pz$. Now define Q to be the projection from $\mathbb{Z}^E$ to $\Lambda(M)$ and

$$\psi : \frac{\mathbb{Z}^E}{\Lambda(M) \oplus \Lambda^*(M)} \to \frac{\text{Im}(Q)}{\Lambda(M)}$$

given by $[x] \to [Qx]$ where $[x] \in \frac{\mathbb{Z}^E}{\Lambda(M) \oplus \Lambda^*(M)}$ and $[Qx] \in \frac{\text{Im}(Q)}{\Lambda(M)}$. By an identical argument to that just given, we see that ψ is also an isomorphism.

To see the final isomorphism, let

$$\varphi : \frac{\mathbb{Z}^E}{\Lambda_A(M) \oplus \Lambda_A^*(M)} \to \text{coker } (AA^T)$$

be the map given by $[x] \to [Ax]$. Recall that $\Lambda_A^*(M)$ corresponds to the column space of A^T over $\mathbb{Z}$, which we will denote $\text{col}_{\mathbb{Z}}$. Now observe that

$$A(\Lambda_A(M) \oplus \Lambda_A^*(M)) = A(\Lambda_A^*(M)) = A\text{col}_{\mathbb{Z}} = \text{col}_{\mathbb{Z}} AA^T.$$

This equality shows that φ is both well-defined and injective. Recall that A can always be placed in the standard form $[I_r|D]$ with all entries in $\{0, \pm 1\}$. Then $Ax = b$ has a solution in $\mathbb{Z}^E$ for all $b \in \mathbb{Z}^r$, hence φ is also surjective. □

Thus we may refer to any of these isomorphic objects as the Jacobian of M.

Theorem 5.2.3. *Let M be a matroid with totally unimodular representation A. Then the order of* $\operatorname{Jac}(M)$ *equals* $|\mathcal{B}(M)|$.

Proof. By the final isomorphism shown in Theorem 5.2.2, it suffices to show that $|\operatorname{Jac}(M)| = |\operatorname{coker}(AA^T)|$. We claim that $|\operatorname{coker}(AA^T)| = \det(AA^T)$. Recall that, up to isomorphism, the cokernel of a matrix is unchanged by the usual row and column operations. Note that these same operations change the determinant by at most a sign change. We may diagonalize AA^T; after doing so, the determinant is given by the product of the diagonal entries and the cokernel is the direct sum of the $\mathbb{Z}_{d_i}$, where the d_i are the absolute values of the diagonal entries. Thus $|\operatorname{coker}(AA^T)| = \det(AA^T)$. To calculate $\det(AA^T)$, we apply the Cauchy-Binet formula to the $r \times r$ submatrices of A and A^T and find that

$$\det(AA^T) = \sum_{I \in E, |I| = r} \det(A|_I) \det(A^T|_I) = \sum_{I \in E, |I| = r} \det(A|_I)^2.$$

But A is totally unimodular, so $\det(A|_I)^2 = 1$ if I is a basis and 0 otherwise. Thus $\det(AA^T) = |\mathcal{B}(M)|$. □

Biggs [3] shows that the Jacobian of a graph can be calculated from the Smith normal form of the graph Laplacian. A similar process applies to the Jacobian of a matroid. Theorem 5.2.2 shows that $\operatorname{Jac}(M) \cong \operatorname{coker}(AA^T)$ where A is a representation of M. Then in the proof of Theorem 5.2.3, we observed that $\operatorname{coker}(AA^T)$ is given by the direct sum of the diagonalized form of AA^T. The structure theorem for finite abelian groups confirms this observation.

Example 5.2.4. Recall the matroid $M(K_4)$, familiar from previous examples. This matroid has a totally unimodular representation

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

hence

$$AA^T = \begin{bmatrix} 3 & 1 & 1 \\ 1 & 3 & -1 \\ 1 & -1 & 3 \end{bmatrix}.$$

We find that $\det(AA^T) = 16$, so we know that $|\operatorname{Jac}(M(K_4))| = 16$. Diagonalizing AA^T gives the matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & -4 \end{bmatrix}$$

hence $\operatorname{Jac}(M(K_4)) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$; this agrees with the calculation of $\det(AA^T)$. It is known that $\operatorname{Jac}(K_n) \cong (\mathbb{Z}_n)^{n-2}$, hence $\operatorname{Jac}(K_4) \cong \operatorname{Jac}(M(K_4))$.

5.2.1 Parity of the Jacobian in Eulerian and bipartite matroids

Recall that a connected graph G is said to be Eulerian if every vertex has even degree; a graph G is bipartite if its vertex set admits a partition into two subsets such that every edge in G has endpoints in different subsets. The corresponding notions were introduced into matroid theory by Welsh [18]. The majority of the research into these classes of matroids has taken place within the context of the study of binary matroids, but as all regular matroids admit a binary representation, the theory easily carries over. In this final section, we apply these matroidal notions to extend results due to Eppstein [6] on the Jacobian of a graph to the more general setting of regular matroids.

The circuit and cocircuit sets of a binary matroid M on a ground set E of cardinality m can be viewed as subspaces of $\mathbb{F}_2^m$ generated by the indicator vectors of the circuits and cocircuits of M. The following proposition shows the orthogonality of the circuit and cocircuit spaces of a binary matroid.

Proposition 5.2.5. *Let M be a binary matroid. Then, for all circuits $C \in \mathcal{C}(M)$ and cocircuits $C^* \in \mathcal{C}^*(M)$, $|C \cap C^*|$ is even.*

Proof. Let A be a representation of M in standard form over $\mathbb{F}_2$ and let A^* be the standard representation of M^*. We know that the row spaces of A and A^* are orthogonal, so any row in A will have zero dot product with a row in A^*; this is the case over $\mathbb{F}_2$ if and only if there are an even number of non-zero entries in the same position in these two vectors. □

A matroid is said to be an *Eulerian matroid* if there exist disjoint circuits $C_1, \dots, C_k$ such that $E = C_1 + \cdots + C_k$. A *bipartite matroid* is a matroid in which every circuit has even cardinality. The following result is due to Welsh [18].

Theorem 5.2.6. *A binary matroid M is Eulerian if and only if its dual M^* is bipartite.*

Proof. Let M be Eulerian and binary, so $E = C_1 \sqcup \cdots \sqcup C_k$. Let C^* be a cocircuit of M, so $|C_i \cap C^*|$ is even for all i. Say $|C_i \cap C^*| = 2n_i$ where $n \in \{1, \dots, k\}$. Then $|C^*| = \sum_1^k |C_i \cap C^*| = \sum_1^k 2n_i$. This shows that M^* is bipartite. Now suppose M is bipartite. We will show that M^* is Eulerian. The proof proceeds by induction on $|E|$. The base case is trivially true. Now assume that $|E| = n$ and the proposition holds for all matroids with ground sets of cardinality less than n. M must have at least one cocircuit, otherwise there is some element $x \in M$ such that x is in every basis of M^*. But then x is a loop in M, i.e., a one element circuit, contradicting the assumption that M is bipartite. Say $C^* \in \mathcal{C}^*(M)$. If $C^* = E$, then we are done, so say $C^* \subsetneq E$. Let $M' = M \setminus C^*$. A circuit $C' \in \mathcal{C}(M')$ has the form $C_i \cap E'$ where $E' = E - C^*$. Because M is bipartite, all C_i have even cardinality; because M is binary $|C^* \cap C_i|$ is even for all i. Thus $|C_i \cap E'|$ is even for all i and M' is bipartite. But M' is also binary, so by induction, $E' = Z_1 \sqcup \cdots \sqcup Z_k$ where $Z_i \in \mathcal{C}^*(M')$. As a cocircuit in M' is a cocircuit in M, it must be the case that $E = Z \sqcup Z_1 \sqcup \cdots \sqcup Z_k$ where all Z are cocircuits of M. Thus M^* can be partitioned into a set of disjoint circuits, and this is exactly the definition of an Eulerian matroid. □

The following proposition, shown in the graph theoretic case by Spencer Backman, further characterizes binary matroids.

Proposition 5.2.7. *Let M be a binary matroid on ground set E of cardinality m. Let χ_F be the characteristic function of $F \subseteq E$. Then there exists some $C \in \mathcal{C}(M)$ and $C^* \in \mathcal{C}^*(M)$ such that $\chi_C + \chi_{C^*} = \chi_E$.*

Proof. The proof is by induction on $|E|$. We take the empty matroid as the base case and the result is trivial. Now consider a matroid M with $|E| = m$. We can delete an element e to obtain a smaller matroid $M \setminus e$. By induction, $\chi_{E(M \setminus e)} = \chi_{C_e} + \chi_{C_e^*}$ where $C_e \in C(M \setminus e)$ and $C_e^* \in C^*(M \setminus e)$. Adding an element cannot remove a circuit, so $C_e \in C(M)$ and either C_e^* or $C_e^* + e \in C^*(M)$. If the latter, we are done, so assume we are in the first case. Without loss of generality, assume $C_e^* \in C_M^*$ for all $e \in M \setminus E$. Note that for any $e, f \in E$, we have $\chi_{C_e^*} + \chi_{C_e} + \chi_{C_f^*} + \chi_{C_f} = \chi_{e,f}$. Now, for any $A \subset E$ with $|A|$ even, we can write χ_A as a sum of indicator vectors for pairs of edges, extending the above equality and obtaining the result. So assume $|E|$ is odd. If M contains an odd circuit C, $|E(M \setminus C)|$ is even and we are done. If M has no odd circuits, then M is bipartite. Hence M^* is Eulerian, hence $E(M)$ can be written as a disjoint union of circuits. It follows that $\chi_{E(M)}$ can be written as a sum of indicator vectors of cocircuits. This completes the proof. □

Example 5.2.8. In Examples 2.1.2 and 2.1.7, we saw the vector matroid associated to the matrix

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

over the real numbers. It is not difficult to see that A is totally unimodular, hence $M(A)$ is regular. Considering the same matrix over $\mathbb{F}_2$ does not change the dependencies among the columns of A, so A over $\mathbb{F}_2$ generates the same matroid. Index the columns of A by $c_1, \ldots, c_5$. The circuits of $M(A)$ are $\{c_1, c_2, c_3, c_4\}, \{c_2, c_3, c_4, c_5\}$ and $\{c_1, c_5\}$; all have even cardinality, i.e., $M(A)$ is bipartite. The dual matrix over $\mathbb{F}_2$ is

$$A^* = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and this generates the dual matroid $M^*(A)$. We can write the column label set as the union of the circuits $\{c_1, c_4, c_5\}$ and $\{c_2, c_3\}$, so $M^*(A)$ is Eulerian.

Theorem 5.2.9. *Let M be Eulerian, with $r(M)$ odd. Then $|\operatorname{Jac}(M)|$ is even.*

Proof. Fix an ordering on the elements of $\mathcal{B}$. Define G to be the graph with vertices indexed by the elements of $\mathcal{B}$. Two vertices are adjacent if the corresponding bases differ by a basis exchange, i.e., if e is an edge between vertices i, j, then deleting an element x from B_i and replacing it with an element of $E - B_i$ gives a basis B_j. Moreover, $x \in B_i$ implies that x is in some cocircuit C_i^*. By Theorem 5.2.6, M^* is bipartite, hence $|C_i^*|$ is even. Therefore, x is involved in an odd number of exchanges. By hypothesis, B_i also has odd cardinality so the corresponding vertex $v_i \in V(G)$ has odd degree. By the so-called Handshake Lemma of graph theory, which states that $\sum_{v \in V(G)} d(v) = 2|E(G)|$ we know that the number of odd degree vertices in G must be even. As each vertex corresponds to a basis it must be the case that $|V(G)|$ is even, hence $|\mathcal{B}(M)|$ is even. □

Example 5.2.10. Let A be the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

over $\mathbb{F}_2$ with columns indexed as $c_1, \ldots, c_5$. The matroid $M(A)$ is regular (in fact, graphic) and Eulerian; we can write the index set of the columns as $\{c_1, c_5\} \cup \{c_2, c_3, c_4\}$. $M(A)$ has rank 3, so Theorem 5.2.8 says that $\mathrm{Jac}(M)$ will be even. Note that if we consider A over $\mathbb{R}$, $M(A)$ does not change. Calculating AA^T, we obtain the matrix

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix}$$

which has Smith normal form

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

Therefore $\mathrm{Jac}(M(A)) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $|\,\mathrm{Jac}(M(A))| = 6$.

Theorem 5.2.11. *Let M be a bipartite matroid such that $|B| = r$ and $|E - B| = m - r$ have the same parity. Then $|\,\mathrm{Jac}(M)|$ is even.*

Proof. Let G be the graph as in the proof of the previous theorem. For any $B \in \mathcal{B}(M)$ and $x \in E - B$, $B \cup x$ contains a unique circuit C. Because M is bipartite, $|C|$ is even, hence $|B| = r$ is odd. The basis exchanges involving an edge in B correspond to a deletion of an element from C, hence any $e \in E - B$ is in an odd number of exchanges. By hypothesis on the parity of $m - r$, there are an odd number of edges not in B, so all $v \in V(G)$ have odd degree. The proof continues as in Theorem 5.2.7. $\square$

Example 5.2.12. Let A be the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

over $\mathbb{F}_2$ with columns indexed $c_1, \ldots, c_6$. Then $M(A)$ has rank 3 and circuits $\{c_1, c_4\}, \{c_2, c_5\}$ and $\{c_3, c_6\}$, all of which have even cardinality, i.e., $M(A)$ is bipartite. Theorem 5.2.10 tells us that $|\operatorname{Jac}(M(A))|$ will be even. Considering A over the reals does not change the matroid, so we may use A to find the Jacobian. Calculating AA^T,

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix},$$

we see that AA^T is already a diagonal matrix. Thus we find that $\operatorname{Jac}(M(A)) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $|\operatorname{Jac}(M(A))| = 8$.

Theorem 5.2.13. *Let M be Eulerian. Then $g = \gcd\{|C| : C \in \mathcal{C}(M)\}$ divides $|\operatorname{Jac}(M)|$.*

Proof. A flow F of $1/g$ units in M will have an integer dot product with any circuit in M, hence (because M is Eulerian) with any integer flow on M (an element of $\Lambda(M)$). Therefore F is an element of $\Lambda^{\#}(M)$; in fact F is an element of $\operatorname{Jac}(M)$ of order g, as $gF \in \Lambda(M)$ but any smaller multiple of F has a non-integer value. $\square$

The following corollary follows immediately.

Corollary 5.2.14. *Let M be a bipartite Eulerian matroid. Then $|\operatorname{Jac}(M)|$ is even.*

Bibliography

[1] Roland Bacher, Pierre de La Harpe, and Tatiana Nagnibeda. The lattice of integral flows and the lattice of integral cuts on a finite graph. *Bulletin de la Société Mathématique de France*, 125(2):167-198, 1997.

[2] Spencer Backman, Matthew Baker, and Chi Ho Yuen. Geometric bijections for regular matroids, zonotopes, and Ehrhart theory. *Forum of Mathematics, Sigma.* (Vol. 7). Cambridge University Press, 2019.

[3] Norman Biggs. Algebraic potential theory on graphs. *Bulletin of the London Mathematical Society* 29(6):641-682, 1997.

[4] Andreas Björner, Michel Las Vergnas, Bernd Sturmfels, Neil White, and Günter M. Ziegler. *Oriented Matroids*, volume 46 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, 1999.

[5] J. A. De Loera, J. Lee, S. Margulies, & J. Miller. Weak orientability of matroids and polynomial equations. *European Journal of Combinatorics*, 50: 56-71, 2015.

[6] David Eppstein. On the parity of graph spanning tree numbers. Information and Computer Science, University of California, Irvine, 1996.

[7] Gary Gordon and Jennifer McNulty. *Matroids: A Geometric Introduction.* Cambridge University Press, 2012.

[8] Winfried Hochstättler. Oriented Matroids-From Matroids and Digraphs to Polyhedral Theory. Techn. Ber. feu-dmo024. Fern Universität in Hagen, 2010.

[9] Jeffrey C. Lagarias. Point lattices. *Handbook of combinatorics (vol. 1).* MIT Press, 1996.

[10] George Minty. On the axiomatic foundations of the theories of directed linear graphs, electrical networks and network-programming. *Journal of Mathematics and Mechanics*, 15(3):485-520, 1996.

[11] James Oxley. *Matroid Theory, second edition.* Oxford University Press, 2011.

[12] Paul D. Seymour. Decomposition of regular matroids. *Journal of combinatorial theory, Series B*, 28(3):305-359, 1980.

[13] Yi Su and David G. Wagner. The lattice of integer flows of a regular matroid. *Journal of combinatorial theory, Series B*, 100(6): 691-703, 2010.

[14] Libby Taylor. On the regularity of orientable matroids. *Discrete Mathematics*, 342(9): 2733-2737, 2019.

[15] William T. Tutte. Lectures on matroids. J. *Research of the National Bureau of Standards (B)*, 69:1-47, 1958.

[16] William T. Tutte. A homotopy theorem for matroids, I and II. *Transactions of the American Mathematical Society*, 88(1):144-160, 1958.

[17] Dominic Welsh. *Matroid theory*. Courier Corporation, 2010.

[18] Dominic Welsh. Euler and bipartite matroids. *Journal of Combinatorial Theory*, 6(4):375-377, 1969.

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