REPRESENTATIONS OF MATROIDS AND THE EXCLUDED MINOR THEOREMS

ANUSHKA MURTHY

Abstract. In this expository paper, we consider the question of when a matroid is representable over some field. First, we start by introducing the concept of a matroid as a generalization of linear dependence, and we also discuss the graph-theoretic context in which matroids arise. We then formulate precise definitions for what it means for a matroid to be "representable" over a field, and demonstrate how questions of representability arise by providing examples of matroids that are representable and non-representable over various fields. Having established these preliminaries, we develop the theory of Matroid Operations, which will illuminate more analogies with the corresponding operations that arise in Graph and Matrix Theory. This discussion leads to an excluded minor characterization for binary matroids, and we provide several more necessary and sufficient conditions for a matroid to be binary. Finally, we give a self-contained proof for the excluded minor characterization of regular matroids that was first found by Tutte (1958).

Contents

1. Introduction

A matroid is a combinatorial structure that generalizes the notion of linear independence. These structures were introduced by Whitney in 1935, and they provide a unifying link between Graph Theory and Linear Algebra. Furthermore, they have

Date: August 2021.

applications in combinatorial optimization and in approaching combinatorial problems such as establishing logarithmic concavity of the coefficients of the chromatic polynomial of a graph.

In addition to the numerous applications in which matroids appear, the intrinsic theory of matroids has been deeply studied. This paper aims to highlight some of this work by covering the classic results that have been established in relation to the question of whether a matroid can be represented as a matrix over some finite field. Our paper builds up to a proof of the following characterization of regular matroids by Tutte [15], which appears as *Theorem 5.7* in this paper:

Theorem 1.1. *A matroid is regular if and only if it has no minor isomorphic to $U_{2,4}$, F_7, or F_7^*.*

We start by showing how to construct a matroid with a precise definition that generalizes the concept of linear independence. Then, we motivate why the concept of representability is a subject of study by showing that there are matroids that are representable over all fields, some fields, or no fields. From here, we move to Section 3 where we introduce the concepts of Circuits and Bases, which allows us to give another equivalent definition of matroids that will allow us to study their excluded minors. In section 4, we start with the simpler problem of giving an excluded minor characterization for binary matroids. In particular, we show that a matroid is binary if and only if it has no minor isomorphic to $U_{2,4}$. We also give several additional characterizations of binary matroids.

In section 5, we tackle the problem of characterizing regular matroids. The proof we give is due to Gerards, as it is relatively shorter and easier to understand compared to Tutte's original proof. The idea behind the proof is to give an equivalent characterization of regular matroids based on whether they have a representation with a totally unimodular signing, which allows us to determine the matroid's excluded minors by observing how the representation matrix can be transformed into the matrix of a given minor.

2. Preliminary Definitions and Examples

2.1. Constructions of matroids.

Consider a vector space V over a field $\mathbb{F}$. Recall from linear algebra that we call k vectors $v_1, \ldots, v_k$ *linearly independent* if the only solution to $c_1v_1 + \cdots + c_kv_k = 0$ is $c_1 = \cdots = c_k = 0$. One of the starting points of Matroid Theory is to provide a generalization of this notion of linear independence. This allows us to formulate a precise definition of a matroid:

Definition 2.1. A *matroid* M is a pair $(E, \mathcal{I})$ where E is a finite set and $\mathcal{I}$ is a collection of subsets of E satisfying the following axioms:

(1) $\emptyset \in \mathcal{I}$.
(2) If $K \in \mathcal{I}$, then every subset of K is a member of $\mathcal{I}$.
(3) If $X, Y \in \mathcal{I}$ and $|X| > |Y|$, there is a member $x \in X - Y$ such that $Y \cup \{x\} \in \mathcal{I}$.

We refer to E as the *ground set* of M, and sets in $\mathcal{I}$ as *independent sets*. An immediate consequence of Property (3) is that the maximal independent sets of M have the same size. We refer to this size as the *rank* of M.

Definition 2.2. The *rank function* $r(X)$ of some subset X of E maps X to $|S|$, where S is any independent set contained in X with maximum size.

Matroids are often called "cryptomorphic" because there are several equivalent ways to define them. One of these alternate definitions, which involves the concepts of *circuits* and *bases*, will be discussed in Section 3. For now, we give some examples of matroids, most of which are crucial for the main results of this paper.

Example 2.3. Let $E = \{1, 2\}$. We have 5 matroids on E, with $\mathcal{I}$ defined as follows:

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

However, if we consider the bijection from E onto itself that switches 1 and 2, we have a bijection between the ground sets of matroids (2) and (3) such that a subset of E is independent in (2) if and only if its image is independent in (3). In general, we call such a bijection between two matroids M and M' an *isomorphism*. In this case, we have (2) $\cong$ (3). Therefore, E gives rise to 4 non-isomorphic matroids.

Definition 2.4. Suppose we set $E = [n] = \{1, \ldots, n\}$. Fix r such that $0 \leq r \leq n$. If we define $\mathcal{I}$ to be all subsets of E with size at most r, then $M = (E, \mathcal{I})$ defines a matroid. We call this the *uniform matroid* $U_{r,n}$.

Example 2.5. The matroid (5) in *Example 2.3* is isomorphic to $U_{2,2}$. Furthermore, (4) isomorphic to $U_{1,2}$ and (1) is isomorphic to $U_{0,2}$.

Proposition 2.6. *Consider a graph $G = (V, E)$. Let E be the ground set and $\mathcal{I}$ be the collections of edges that do not contain a cycle. Then the resulting construction defines a matroid.*

Proof. Properties (1) and (2) follow from the definition of a cycle. For property (3), we need the following two lemmas:

Lemma 2.7. *Let $T = (V, E)$ be a tree. Then*

(1) $|V| = |E| + 1$
(2) Any new edge in T produces a cycle.

Proof. We prove the first part using induction on $n = |V|$. The base case $n = 1$, 2 is clear. Assume the statement is true for $k < n$. Given a tree with n vertices, remove a leaf. This produces a tree with $n - 1$ vertices, so we have $n - 1 = (|E| - 1) + 1$. If we add back the vertex, we will have $n = |E| + 1$.

For the second part, we notice that for any vertices $x, y \in V$, there is a path from x to y since T is connected, so adding an edge between these vertices produces a cycle. □

Lemma 2.8. *If G is acyclic with k connected components, then $|V| = |E| + k$*

Proof. This follows because each connected component of G is a tree, and by the previous lemma $|V_i| = |E_i| + 1$. □

Returning to the proof of Proposition 2.6, let I_1, I_2 be acyclic subsets of the edges of G such that $|I_2| > |I_1|$. Define G_1 and G_2 to be graphs with edge sets I_1 and I_2. If some edge e completes a cycle in G_1, the vertices x and y of e must be contained in $V(G_1)$, and there must be a path from x to y. We thus have three cases to consider:

(1) $V(G_2) - V(G_1)$ is non-empty: Then we can add an edge e in I_2 containing an element of$V(G_2) - V(G_1)$, and $I_1 \cup \{e\}$ will be acyclic.
(2) Assume $V(G_2) \subset V(G_1)$, $T_1, \ldots, T_k$ are connected components of G_1, and there's an edge $e \in I_2$ connecting elements of different connected components. Then $I_1 \cup \{e\}$ is acyclic since there was no path between the connected components in G_1.
(3) Assume $V(G_2) \subset V(G_1)$, $T_1, \ldots, T_k$ are connected components of G_1, but the edges of I_2 only connect vertices in the same connected components of G_1.

To treat the third case, let $E_{G_k}(T_i)$ denote edges of G_k with vertices in T_i, for $k = 1, 2$. We have

$$|E_{G_1}(T_1)| + \cdots + |E_{G_1}(T_k)| = |I_1| < |I_2| = |E_{G_2}(T_1)| + \cdots + |E_{G_2}(T_k)|$$

.

Therefore, there exists some i such that $|E_{G_1}(T_i)| < |E_{G_2}(T_i)|$. Since $E_{G_2}(T_i)$ induces an acyclic graph with vertices $V(T_i) \cap V(G_2)$ and m connected components, we apply Lemma 2.8 to obtain

$$|E_{G_2}(T_i)| = |V(T_i) \cap V(G_2)| - s \leq |V(T_i)| - 1 = |E_{G_1}(T_i)|.$$

This is a contradiction, so the third case is not possible. □

We call the resulting matroid $M(G)$. A matroid is *graphic* if it is isomorphic to $M(G)$ for some graph G.

2.2. **Foundations of Representability.**

Having provided some illustrative examples of matroids, we claim that *Definition 2.1* is equivalent to our usual definition of linear independence from linear algebra.

Lemma 2.9. *Let V be a vector space over a field $\mathbb{F}$. If we set E to be any finite subset of V and $\mathcal{I}$ to be all collections of linearly independent vectors in E, then $M = (E, \mathcal{I})$ is a matroid.*

Proof. Properties (1) and (2) follow from the definition of linear independence. Let X and Y be linearly independent sets with $|X| > |Y|$. If W is the span of $X \cup Y$, then $dim(X) \leq dim(W)$. Suppose $Y \cup \{x\}$ is linearly dependent for any $x \in X$. Then we would have $dim(X) \leq dim(W) \leq dim(Y)$, which is a contradiction since $dim(X) > dim(Y)$. Therefore, M satisfies Property (3). □

Another way to phrase the construction in *Lemma 2.9* is as follows: Given a matrix A over a field $\mathbb{F}$, let E be the set of column labels of A, and $\mathcal{I}$ be the multiset of labels of linearly independent columns. We refer to the resulting matroid as a *vector matroid* $M[A]$.

Definition 2.10. If a matroid M is isomorphic to a vector matroid $M[A]$ over a field $\mathbb{F}$, we say M is *representable* over $\mathbb{F}$. We call $M[A]$ an *F-representation* of M. If $\mathbb{F}$ is $\mathbb{F}_2$, we say M is *binary*. If $\mathbb{F}$ is $\mathbb{F}_3$, we say M is *ternary*. A matroid that is representable over every field is called *regular*.

We can now give an equivalent definition of graphic matroids that shows they are binary.

Definition 2.11. Let G be a graph. Consider a matrix $A = (a_{i,j})$ where the rows of A represent the vertices of G, the columns of A represent the edges of G, and

$$a_{i,j} = \begin{cases} 1 & v_i \in e_j \\ 0 & \text{otherwise} \end{cases} \tag{2.12}$$

Then we call A the *vertex-edge incidence matrix* of G.

Theorem 2.13. *Let G be a graph and A_G be its vertex-edge incidence matrix. Consider the vector matroid $M[A_G]$. Then the independent sets of $M[A_G]$ are the sets of edges that do not contain a cycle, so $M(G) = M[A_G]$ and graphic matroids are binary.*

Proof. One can prove $M(G) = M[A_G]$ by unravelling the definition of linear independence in the context of adjacency matrices to show that the columns of A_G are dependent if and only if the associated edges contain a cycle. Viewing A_G as a matrix over $\mathbb{F}_2$ shows that $M(G)$ is binary. □

Of course, there exist matroids that aren't binary:

Example 2.14. We can verify that $U_{2,k}$ is binary for $k = 2, 3$ by providing explicit $GF(2)-$representations

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

and

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

However, $U_{2,4}$ is not binary. To see this, we note that the maximal independent sets in $U_{2,4}$ have size 2, so the vector space spanned by the columns of a $GF(2)-$representation for $U_{2,4}$ have dimension2. The two-dimensional vector-space over $GF(2)$ only has 3 non-zero vectors and 4 vectors total, so any binary representation of $U_{2,4}$ will have a pair of linearly dependent columns. Therefore, $U_{2,4}$ cannot have a binary representation. On the other hand, $U_{2,4}$ is ternary, as it has the representation

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

In light of the previous examples, a natural question is when we can determine whether a matroid is binary. We can also formulate similar questions about when a matroid is ternary or regular. To answer these questions, we must define the concepts of Bases and Circuits, as well as discuss various matroid operations such as Duals and Minors.

3. Circuits and Matroid Operations

3.1. Bases and Circuits.

Definition 3.1. Given a matroid M, we say a set is a *basis* if it is a maximal independent set. We say a set is a *circuit* if it is a minimal dependent set.

Property (2) of matroids guarantees that a matroid is uniquely determined by its collection of bases (and therefore circuits). We now give an alternate way to define a matroid, and show that it is indeed equivalent to the original definition we provided.

Definition 3.2. We call $M = (E, \mathcal{B})$ a matroid if E is a finite set and $\mathcal{B}$ satisfies the following properties:

(1) $\mathcal{B}$ is non-empty.
(2) If B_1 and B_2 are distinct members of $\mathcal{B}$ and there exists some $s \in B_1 - B_2$, then there exists $p \in B_2 - B_1$ such that $(B_1 - \{s\}) \cup \{p\} \in \mathcal{B}$.

The second criterion is referred to as the *Basis Exchange Property.*

Proposition 3.3. *Let E be a finite set. Then a collection $\mathcal{B}$ of subsets of E forms the collection of bases for a matroid on E if and only if $\mathcal{B}$ satisfies the axioms of Definition 3.2.*

Proof. Let $\mathcal{B}$ be the collection of bases of some matroid $M = (E, \mathcal{I})$. Since $\mathcal{I}$ contains the empty set, there is at least one maximal member of $\mathcal{I}$ so $\mathcal{B}$ is non-empty.

Now let B_1 and B_2 be distinct bases and $s \in B_1 - B_2$. Since $B_1 - \{s\} \subset B_1$, it is also an independent set. From the remark after *Definition 2.1*, we know $|B_1| = |B_2|$ so $|B_1 - \{s\}| < |B_2|$. From Property (3) of *Definition 2.1*, there exists $p \in B_2 - (B_1 - \{s\})$ such that $(B_1 - \{s\}) \cup \{p\}$ is independent. Since $p \in B_2$, $p \neq s$ so $|(B_1 - \{s\}) \cup \{p\}| = |B_2|$. Therefore, $B_1 - \{s\}) \cup \{p\}$ is maximal so $B_1 - \{s\}) \cup \{p\} \in \mathcal{B}$. This means that $\mathcal{B}$ satisfies all the axioms of *Definition 3.2.*

Conversely, suppose $\mathcal{B}$ is a collection of subsets of E satisfying the axioms of *Definition 3.2.* Define $\mathcal{I}$ to be all subsets of elements of $\mathcal{B}$. Since $\mathcal{B}$ is non-empty and the empty set is a subset of every set, $\emptyset \in \mathcal{I}$ so we have Property (1) in *Definition 2.1.* By our definition of $\mathcal{I}$, we have Property (2) as well.

Suppose $\mathcal{I}$ does not satisfy Property (3). Then there exist $I_1, I_2 \in \mathcal{I}$ such that $|I_1| < |I_2|$ and $I_1 \cup \{x\}$ is dependent for all $x \in I_2 - I_1$. I_1 and I_2 are each contained in at least one basis B_1 and B_2. Choose these bases so $B_1 \cap B_2$ has maximum size. If there is some $y \in (I_2 \cap B_1) - I_1$, then $I_1 \cup \{y\}$ must be independent, which would imply that $\mathcal{I}$ satisfies Property (3). This is a contradiction, so we assume $(I_2 \cap B_1) \subset I_1$. In other words,

$$I_2 - B_1 = I_2 - I_1 \tag{3.4}$$

Suppose there exists some $x \in B_2 - (I_2 \cup B_1)$. Since $x \in B_2 - B_1$, we can apply the second axiom of *Definition 3.2* to find some $y \in B_1 - B_2$ such that $(B_2 - \{x\}) \cup \{y\} \in \mathcal{B}$. Since $I_2 \subset (B_2 - \{x\}) \cup \{y\}$, this set has a larger intersection with B_1 than, B_2, which contradicts our choice of B_1 and B_2. Therefore, $B_2 - (I_2 \cup B_1)$ must be empty. This means $B_2 - B_1 = I_2 - B_1$, and when we combine this with *Equation 3.4* we get

$$B_2 - B_1 = I - 2 - I_1 \tag{3.5}$$

Finally, suppose there exists some $y \in B_1 - (I_1 \cup B_2)$. Since $y \in B_1 - B_2$, we can apply the second axiom of *Definition 3.2* to find some $x \in B_2 - B_1$ such that $(B_1 - \{y\}) \cup \{x\} \in \mathcal{B}$. Since $I_1 \subset (B_1 - \{y\}) \cup \{x\}$, this set has a larger intersection with B_2 than, B_1, which contradicts our choice of B_1 and B_2. Therefore, $B_1 - (I_1 \cup B_2)$ must be empty. This means $B_1 - B_2 = I_1 - B_2 \subset I_1 - I_2$, so

$$|B_1 - B_2| \leq |I_1 - I_2| \tag{3.6}$$

Since $|B_1| = |B_2|$, $|B_1 - B_2| = |B_2 - B_1|$ so we may apply *Equations 3.5* and *3.6* to obtain

$$|I_2 - I_1| = |B_2 - B_1| = |B_1 - B_2| \leq |I_1 - I_2|$$

Then we have

$$|I_2| = |I_1 \cap I_2| + |I_2 - I_1| \leq |I_1 \cap I_2| + |I_1 - I_2| = |I_2|$$

This contradicts our assumption that $|I_1| < |I_2|$, so $\mathcal{I}$ must satisfy Property (3), and $M = (E, \mathcal{I})$ is a matroid. By construction, $\mathcal{B}$ is the collection of bases for M. □

One can give the following equivalent definition of a matroid in terms of its circuits. We will omit the proof of the statement that this definition is equivalent to our original definition as it is similar to the proof above.

Definition 3.7. Define $M = (E, \mathcal{C})$ to be a matroid if E is finite and $\mathcal{C}$ satisfies the following properties:

(1) $\emptyset \notin \mathcal{C}$
(2) If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subset C_2$, $C_1 = C_2$.
(3) If $C_1, C_2 \in \mathcal{C}$ and $x \in C_1 \cap C_2$, then $(C_1 \cup C_2) - x$ contains a member of $\mathcal{C}$.

Proposition 3.8. *If $\mathcal{C}$ is a collection of subsets of a finite set E, then $\mathcal{C}$ is a collection of circuits of some matroid on E if and only if it satisfies the axioms in Definition 3.7.*

Definition 3.9. A 1-element circuit is called a *loop*, and a 2-element circuit is called a *parallel pair*. A matroid is *simple* if it has no loops or parallel pairs.

We end this section with a simple property of Circuits.

Proposition 3.10. *Suppose I is an independent set of a matroid M, and $I \cup e$ is dependent for some $e \notin I$. Then $I \cup e$ contains a unique circuit, and this circuit contains e.*

Proof. The fact that $I \cup e$ contains a circuit follows from the definition of a circuit and the fact that this set is dependent. Such a circuit must contain e since I is independent. If $I \cup e$ contains two circuits C_1 and C_2, then $e \in C_1 \cap C_2$ so by Property (3) of *Definition 3.7*, $(C_1 \cup C_2) - e$ is a circuit. However, this is not possible since this set is contained in I. □

Definition 3.11. Given a basis B and some $e \in E - B$, $B \cup e$ is dependent since B is maximal, and by the proposition above there exists a unique circuit contained in $B \cup e$ that contains e. We call this the *fundamental circuit* of B with respect to e, denoted $C(B, e)$.

3.2. **Duals.** We begin by showing that the "dual" operation defines a matroid.

Proposition 3.12. *Suppose $M = (E, \mathcal{I})$ is a matroid with $\mathcal{B}$ as its collection of bases. If we let*

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

Then B^* is the collection of bases for a matroid M^* on E.

Proof. Since $\mathcal{B}$ is non-empty, so is B^*. Let $E - B_1$ and $E - B_2$ be two elements of B^*. We notice $(E-B_1)-(E-B_2) = B_2-B_1$, and assume there exists $x \in B_2-B_1$. From Axiom 2 of *Definition 3.2*, there exists $y \in B_1-B_2$ such that $(B_1-y)\cup x \in \mathcal{B}$. Then $E-((B_1-y)\cup x) = ((E-B_1)-x)\cup y$. Since $B_1-B_2 = (E-B_2)-(E-B_1)$, B^* satisfies both axioms of *Definition 3.2* so B^* is the collection of bases for some matroid on E by *Proposition 3.3*. □

We refer to the resulting matroid M^* as the *dual* of M. It follows from the definitions that $(M^*)^* = M$.

Definition 3.13. Independent and dependent sets in M^* are called *coindependent* and *codependent* sets of M. The bases and circuits of M^* are called *cobases* and *cocircuits* of M. A loop of M^* is called a *coloop* of M. If M^* is simple then M is *cosimple*.

Sometimes, we denote the rank function of M^* by r^*. More explicitly, $r^*(E)$ is the size of the maximum-sized coindependent set contained in E.

We notice that the definition of B^* immediately implies the following lemma:

Lemma 3.14. $r(M^*) + r(M) = |E|$

We also have another useful relation regarding the rank function:

Proposition 3.15. *Suppose X is a subset of E. Then*

$$r^*(X) = |X| + r(E - X) - r(M)$$

Proof. Let I^* be a coindependent set in X with maximum size. By definition, $E - I^*$ contains a basis B. We first claim that $X - I^* = X \cap B$. First, suppose there exists $x \in X - I^*$ such that $x \notin B$. Notice $I^* \cup x \subset X - B$ since $I^* \cap B = \emptyset$, so $I^* \cup x$ is coindependent. Furthermore, it has size strictly greater than I^* since $x \notin I^*$, but this contradicts the fact that I^* has maximum size. Therefore, we must have $X - I^* \subset X \cap B$. Now since $I^* \cap B = \emptyset$, we also have $X \cap B \subset X - I^*$, so the two sets are indeed equal. Therefore, $|X| = |I^*| + |X - I^*| = r^*(X) + |X \cap B|$, and $r^*(X) = |X| - |X \cap B|$.

Now, we want to show $r(E - X) = |B - X|$, so $B - X$ is the maximum-sized independent set contained in $E - X$. Suppose there exists a large independent set $K-X$. By Property 3 for matroids, there exists $x \in (K-X)-(B-X) = K-(B\cup X)$ such that $(B - X) \cup x$ is independent. Therefore, $(B - X) \cup x$ is contained in another basis B'. Since $x \in B'$, B' interesects $K - X$ in one more element than B. But $|B| = |B'|$ since they are both bases, so B must intersect X in one more element than B'. However, this would imply $B' - X$ has strictly greater size than $B - X = I^*$, contradicting our choice of I^* since $X - B'$ is coindependent. Therefore, $B-X$ is the maximum-sized independent set in $E-X$, so $r(E-X) = |B-X|$.

Finally, $r(M) = |B| = |B - X| + |X \cap B| = r(E - X) + (|X| - r^*(X))$, so $r^*(X) = |X| + r(E - X) - r(M)$. □

Proposition 3.16. *If M is a matroid and x and y are distinct elements of of a circuit C, then there exists a cocircuit C^* of M such that $C \cap C^* = \{x, y\}$.*

Proof. See [6]. □

Example 3.17. Let $U_{r,n}$ be a uniform matroid. Then the dual of $U_{n,r}$ is $U_{n-r,n}$ since the bases of $U_{n,r}$ are the r-subsets of $[n]$.

Proposition 3.18. *Let M be an $\mathbb{F}$-representable matroid. Then there exists some matrix A over F such that $[I|A]$ represents M.*

Proof. See [6]. □

Remark 3.19. Assume A has $n-m$ columns. By $[I|A]$, we mean the $m \times n$ $(m < n)$ matrix that results from letting the first m columns be those of the $m \times m$ identity matrix and the remaining $n - m$ columns be the columns of A.

Proof. By definition, there exists a matrix K such that $M[K] = M$. If $r(M) = r$, K has r rows. The following operations preserve the multisets of linearly independent columns of a matrix, so performing these operations on K produces a matrix that still represents M:

(1) Swapping columns (with labels)
(2) Multiplying columns by a non-zero constant
(3) Multiplying rows by a non-zero constant
(4) Adding a row to another

Now, by the operations listed above, we can transform K into a matrix $[I_r|A]$ where I_r is the $r \times r$ identity matrix, so $M = M[I_r|A]$. □

Proposition 3.20. *If M is $\mathbb{F}$-representable, then so is M^*. Furthermore, $[I|A^T]$ represents M^*.*

Definition 3.21. A class of matroids is called *self-dual* if the dual of every matroid in the class belongs to the class. We have shown that $\mathbb{F}$-representable matroids and uniform matroids are self-dual.

Definition 3.22. Let E be the ground set for a matroid M. Given $k \geq 1$, a *k-separation* of M is a partition of E into sets X and Y such that $|X|, |Y| \geq k$ and

$$r(X) + r(Y) - r(M) < k$$

If $r(X) + r(Y) - r(M) = k - 1$, we call this an *exact k-separation.*

Definition 3.23. A matroid M is called *n-connected* if there is no $k < n$ such that M has a k-separation.

Proposition 3.24. *Let M be a matroid and (X, Y) be a partition of E. Then*

$$r(X) + r(Y) - r(M) = r^*(X) + r^*(Y) - r(M^*)$$

Proof. We make use of *Lemma 3.14* and *Proposition 3.15* to obtain

$$\begin{aligned} &r^*(X) + r^*(Y) - r(M^*) = (|X| + r(E - X) - r(M)) \\ &+ (|Y| + r(E - Y) - r(M)) - (|E| - r(M)) \\ &= |X| + |Y| - |E| + r(X) + r(Y) - r(M) = r(X) + r(Y) - r(M) \end{aligned}$$

□

Proposition 3.25. *Suppose an n-connected matroid has at least $2(n-1)$ elements. Then every circuit contains at least n elements.*

Proof. Suppose there exists a circuit C such that $|C| = k \leq n-1$. Since $|E| \geq 2(n-1)$, $|E-C| \geq n-1 \geq k$. Since $r(C) = k-1$ and $r(E-C) \leq r(M)$, we have $r(C)+r(E-C)-r(M) < k$, so $(C, E-C)$ is a k-separation. But $k < n$, which is a contradiction since M is n-connected so it must not have such a k-separation. □

Corollary 3.26. *Every 3-connected matroid with at least 4 elements is simple and co-simple.*

3.3. **Minors.**

We will first give definitions for the deletion and contraction of a matroid, and we will show that if we consider a graphic matroid $M(G)$, then the definitions coincide with the familiar definitions for deletions and contractions from graph theory.

Definition 3.27. Let $M = (E, \mathcal{I})$ be a matroid. The *deletion* $M\backslash e$ has independent sets

$$\{I \subset E - e : I \in \mathcal{I}\}$$

If e is a loop, define the *contraction* M/e to be $M\backslash e$. Otherwise, define the independent sets of M/e to be

$$\{I \subset E - e : I \cup e \in \mathcal{I}\}$$

Both matroids have ground set $E - e$. We note that $M^*/e = (M\backslash e)^*$ and $M^*\backslash e = (M/e)^*$.

Definition 3.28. A *minor* of M is a matroid obtained through a sequence of deletions and contractions of M. If the ground set of a minor is smaller than the ground set of M, we say it is a *proper minor* of M.

Using the definition above, we observe the following:

Proposition 3.29. *Let G be a graph with some edge e. Then*

(1) $M(G)\backslash e = M(G\backslash e)$
(2) $M(G)/e = M(G/e)$

Definition 3.30. A class of matroids is *minor-closed* if all minors of matroids in the class also belong to the class.

Proposition 3.31. *The class of graphic matroids is minor-closed.*

Proof. This follows by induction on the number of minor operations, along with the previous proposition. □

Example 3.32. If $U_{r,n}$ is the uniform matroid,

$$U_{r,n}\backslash e = \begin{cases} U_{r,n-1} & r < n \\ U_{r-1,n-1} & r = n \end{cases}$$

and

$$U_{r,n}/e = \begin{cases} U_{r-1,n-1} & r < n \\ U_{r,n-1} & r = n \end{cases}$$

Therefore, the class of uniform matroids is minor-closed.

Example 3.33. Let M have an $\mathbb{F}$-representation denoted by A. $M\backslash e$ can be represented by A with the column corresponding to e deleted. Since $\mathbb{F}$-representable matroids are self-dual, M/e is $\mathbb{F}$-representable. Therefore, the class of $\mathbb{F}$-representable matroids is minor-closed.

Definition 3.34. Given a minor-closed class of matroids $\mathcal{M}$, we say that M is an *excluded minor* if M is not in $\mathcal{M}$ but any contraction or deletion of M is.

We now introduce the idea of 1- and 2-sums, which allows us to "piece" together a new matroid from multiple matroids. After we have given the definitions for 1- and 2-sums, we state a few propositions without proof that will allow us to prove *Proposition 3.39*, which establishes a connection between 1- and 2-sums and the excluded minors of a minor-closed class of matrices.

Definition 3.35. Given matroids M_1 and M_2 with $E_1 \cap E_2 = \emptyset$, the *direct sum* $M_1 \bigoplus M_2$ is the matroid with ground set $E_1 \cup E_2$ and independent sets

$$I_1 \cup I_2 : I_1 \in \mathcal{I}_1, I_2 \in \mathcal{I}_2$$

.

Our final goal for the section is to show that the excluded minors for the class of $\mathbb{F}$-representable matroids are 3-connected. The following two propositions are the starting point for this, and their proofs, which can be found in [6], have been ommitted for the sake of brevity.

Proposition 3.36. *A matroid is connected if and only if it cannot be expressed as the direct sum of two non-empty matroids.*

Proposition 3.37. *The class of $\mathbb{F}$-representable matroids is closed under direct and 2-sums.*

We now examine the structure of the minors of matroids expressed as 1- and 2-sums

Proposition 3.38. *If $M = M_1 \bigoplus M_2$, then M has minors isomorphic to M_1 and M_2.*

Proof. This follows since $M_1 = (M_1 \bigoplus M_2)\backslash E(M_2)$ and $M_2 = (M_1 \bigoplus M_2)\backslash E(M_1)$. □

Proposition 3.39. *If $M = M_1 \bigoplus_2 M_2$, then M has minors isomorphic to M_1 and M_2.*

Proof. The proof of this statement is much longer and can be found in [14] as (2.2). □

With these propositions in place, we may show that the excluded minors of the class of $\mathbb{F}$-representable matroids are 3-connected. In fact, we have the following more general statement:

Proposition 3.40. *Let $\mathcal{M}$ be a minor-closed class of matroids closed under direct and 2-sums. Then its excluded minors are 3-connected.*

Proof. Suppose M is an excluded minor for $\mathcal{M}$ that is not (2−)connected. By *Proposition 3.36*, M can be expressed as the direct sum of two non-empty matroids M_1 and M_2. By *Proposition 3.38*, M_1 and M_2 are isomorphic to proper minors of M

(they are proper since both matroids are non-empty), so we must have $M_1, M_2 \in \mathcal{M}$ since M is an excluded minor. By our assumption, we would have $M \in \mathcal{M}$ since the class is closed under direct sums, which is a contradiction. Therefore, M must be (2−)connected.

Suppose M is not 3-connected. We have just shown that it must be 2-connected, ie. it has an exact 2-separation (X,Y) but no 1-separation. By a theorem of Seymour, M can be written as the 2-sum of matroids M_1 and M_2 such that $E(M_1) = X \cup e$, $E(M_2) = Y \cup e$, and $e \notin X \cup Y$. From *Proposition 3.38*, M has minors isomorphic to M_1 and M_2. We notice $|E(M)| = |X| + |Y|$ and $|E(M_1)| = |X| + 1$. If we had $|E(M)| = |E(M_1)|$, we would have $|Y| = 1$, which contradicts the fact that (X, Y) is a 2-separation. Therefore, $|E(M_1)| < |E(M)|$. We similarly show $|E(M_2)| < |E(M)|$, so M_1 and M_2 are proper minors of M. But this would imply $M_1, M_2 \in \mathcal{M}$, and then $M \in \mathcal{M}$ since the class is closed under 2-sums. Therefore, M is 3-connected.

□

Corollary 3.41. *The excluded minors of the class of $\mathbb{F}$-representable matroids are 3-connected.*

Proof. This follows from the previous proposition and *Proposition 3.37*. □

4. Characterizations of Binary Matroids

Our first goal is to prove the following theorem, proved by Tutte in [15]:

Theorem 4.1. *A matroid is binary if and only if it has no minor isomorphic to $U_{2,4}$*

Suppose we knew the following statement:

Proposition 4.2. *The only excluded minor for binary matroids is $U_{2,4}$.*

Consider a matroid M. If M is binary, then *Proposition 4.2* would imply that M has no minor isomorphic to $U_{2,4}$. Now suppose M is not binary. Either M is an excluded minor for binary matroids, or it contains a proper minor that is an excluded minor for binary matroids. In either case, M must contain a minor isomorphic to $U_{2,4}$ since this is the only excluded minor for binary matroids. Therefore, it suffices to prove *Proposition 4.2* to establish *Theorem 4.1*. To prove the proposition, we make use of the following lemma, whose proof can be found in [6]:

Lemma 4.3. *Let M be a matroid, and assume that u and v are distinct elements of $E(M)$ such that $\{u, v\}$ is coindependent. If $M\backslash u$ and $M\backslash v$ are binary, then there exists a unique binary matroid N with ground set $E(M)$ such that $N\backslash u = M\backslash u$ and $N\backslash v = M\backslash v$. N has the same rank as M.*

Now we may proceed with the proof of *Proposition 4.2*:

Proof. As we have shown, $U_{2,4}$ is an excluded minor for binary matroids. Now, suppose M is an arbitrary excluded minor for binary matroids with rank r. Since all matroids with fewer than 4 elements are binary, we assume $|E(M)| \geq 4$. From *Corollary 3.41*, M and M^* are 3-connected. Thus, from *Corollary 3.26*, M has no 1- or 2-element circuits or cocircuits. Thus, if x and y are distinct elements, r(M) = r$(M - \{x, y\})$. By the definition of an excluded minor, $M\backslash x$ and $M\backslash y$ are both

binary. From *Lemma 4.3*, there exists a binary matroid N such that $N\backslash x = M\backslash x$ and $N\backslash y = M\backslash y$. Furthermore, r(N) = r(M). Since M is not binary, $N \neq M$. Therefore, there exists a minimal set Z such that Z is a basis of one of N or M and a circuit of the other. We will denote the matroid where Z is independent by M_I and the matroid where Z is dependent by M_C.

Suppose Z did not contain x. Then Z is a basis of exactly one of $N\backslash x$ or $M\backslash x$, which is not possible since the resulting matroids are equal. Therefore, Z contains x, and the same reasoning shows that Z contains y.

Since $Z - \{x, y\}$ is independent in $M' = N\backslash u\backslash v = M\backslash u\backslash v$, there exists a basis element B for M' containing $Z - \{x, y\}$. Since $\{x, y\}$ is coindependent, r(M) = r(M')= r(N), so B is also a basis for M and N. Now, $|B| = r(M) = |Z - \{x, y\}| + 2$, so There are 2 elements a and b in $B - Z$. We now claim $B = \{a, b\}$.

Suppose we had $z \in B - \{a, b\}$. From the fact that M is an excluded minor, we know $M/z\backslash x$ and $M/z\backslash y$ are binary. Since $\{x, y\}$ is still coindependent in M/z, we know by *Lemma 4.3* that there exists a unique binary matroid N' with ground set $E(M) - z$ such that $N'\backslash x = M/z\backslash x$ and $N'\backslash y = M/z\backslash y$. But M/z and N/z satisfy this property, so we must have $M/z = N' = N/z$. However, $Z - z$ is a basis of exactly one of M/z or N/z, which is a contradiction. Therefore, we must have $B = \{a, b\}$. In particular, r(M)=2.

Since M is a rank 2 simple matroid with at least 4 elements, it must contain a minor isomorphic to $U_{2,4}$. As no two excluded minors can properly contain each other, we conclude M is isomorphic to $U_{2,4}$.

□

We now give several equivalent characterizations of binary matroids. These characterizations were proved in [4], [5], [7], [10], and [16]. Our first step is to prove the following lemma:

Lemma 4.4. *If e is an element of an independent set I of a matroid M, then M has a cocircuit C^* such that $C^* \cap I = \{e\}$.*

Proof. Let B be a basis element of M containing I. By definition, B^* is a basis element of M^* that does not contain e, so $B^* \cup \{e\}$ is dependent. Thus, we may apply *Proposition 3.10* to conclude that there is a unique circuit C^* of M^* (so a cocircuit of M) that is contained in $B^* \cup \{e\}$ and contains e. Since B^* and B are disjoint, we must have $C^* \cap I = \{e\}$. □

Theorem 4.5. *Let M be a matroid. The following statements are equivalent:*

(1) M is binary.
(2) If C is a circuit and C^* is a cocircuit, $|C \cap C^*|$ is even.
(3) If C_1 and C_2 are distinct circuits, then $C_1 \triangle C_2$ contains a circuit.
(4) If C_1 and C_2 are distinct circuits, then $C_1 \triangle C_2$ is a disjoint union of circuits
(5) The symmetric difference of any set of circuits is either empty or contains a circuit.
(6) The symmetric union of any set of circuits is a disjoint union of circuits.
(7) If B is a basis and C is a circuit, then $C = \triangle_{e \in C-B} C(e, B)$.

(8) M has a basis B such that if C is a circuit, then $C = \triangle_{e \in C-B} C(e, B)$.

Proof. **(6)** $\implies$ **(4)**

This is immediate from the statement of (6).

(4) $\implies$ **(3)**

This is immediate from the statement of (4).

(7) $\implies$ **(8)**

(7) provides the basis needed for the statement of (8).

(3) $\implies$ **(2)**

Suppose M does not satisfy **(2)**. Then there exists some pair (C, C^*) such that $|C \cap C^*|$ is odd. Choose the pair with minimum intersection size. Since $|C \cap C^*| \neq 1$, we must have $|C \cap C^*| \geq 3$. Take $x, y, z \in C \cap C^*$. Since $x, z \in C^*$, by *Proposition 3.16* there exists some circuit of M that intersects with C^* at $\{x, z\}$. Therefore, the intersection of this circuit with $(C \cap C^*) - y$ contains x. Let C_1 be a circuit satisfying the conditions of the previous sentence such that $C_1 \cup C$ is minimal.

Since $x \in C_1 \cap C$ and $y \in C - C_1$, there exists a circuit $C_2 \subset (C \cup C_1) - x$ containing y. Now since $y \in C_2 \cap C$ and $x \in C - C_2$, there exists a circuit $C_3 \subset (C \cup C_2) - y$ containing x. This gives us

$$(C \cup C_3) \subset (C \cup C_2) \subset (C \cup C_1) \tag{4.6}$$

Since $x \in C_3$, $y \notin C_3$, and $C \cup C_1$ is minimal, the above sets must all be equal. Then $C_2 - C = C_3 - C$, so $C_2 \triangle C_3 \subset C$. However, $C_2 \neq C_3$ since $x \in C_3 - C_2$, so we can apply our assumption of **(3)** to conclude that $C_2 \triangle C_3$ contains a circuit. Thus, $C_2 \triangle C_3 = C$, so $(C_2 \cap C^*) \cup (C_3 \cap C^*) = C \cap C^*$. These sets are also disjoint, so they partition $C \cap C^*$.

$C_3 \cap C^*$ and $C_2 \cap C^*$ are non-empty since $x \in C_3 \cap C^*$ and $y \in C_2 \cap C^*$, and they have smaller size than $C \cap C^*$. Since $C \cap C^*$ has the smallest odd intersection, $|C_3 \cap C^*|$ and $|C_2 \cap C^*|$ must be even. But $C_3 \cap C^*$ and $C_2 \cap C^*$ partition $C \cap C^*$, so $|C \cap C^*|$ must be even. This is a contradiction, so M must satisfy **(2)**.

(2) $\implies$ **(5)**

Suppose **(5)** were false. Then we would have some collection $C_1, \ldots, C_n$ such that $C_1 \triangle \ldots \triangle C_n$ is non-empty and independent. If we let $x \in C_1 \triangle \ldots \triangle C_n$, then by *Lemma 4.4* there exists a cocircuit C^* such that

$$C^* \cap (C_1 \triangle \ldots \triangle C_n) = \{x\} \tag{4.7}$$

However, by our assumption of **(2)**, $|C^* \cap C_i|$ is even for all i, so $|C^* \cap (C_1 \triangle \ldots \triangle C_n)|$ should be even as well. This is a contradiction from *Equation 4.7*, so M must satisfy **(5)**.

(5) $\implies$ (6)

Suppose **(6)** were false. Let $\mathcal{F}$ denote collections of circuits $C_1, \ldots, C_n$ such that $C_1 \triangle \ldots \triangle C_n$ is not a disjoint union of circuits, and consider an element of $\mathcal{F}$ with minimum size. Since $C_1 \triangle \ldots \triangle C_n$ is not a disjoint union of circuits, at least 2 circuits in $C_1, \ldots, C_n$ must be distinct, so the symmetric difference is not empty. Thus, from our assumption of **(5)**, $C_1 \triangle \ldots \triangle C_n$ contains a circuit C'. This implies

$$|C_1 \triangle \ldots \triangle C_n \triangle C'| < |C_1 \triangle \ldots \triangle C_n| \tag{4.8}$$

Since $C_1 \triangle \ldots \triangle C_n$ has minimum size in $\mathcal{F}$, $C_1 \triangle \ldots \triangle C_n \triangle C'$ must not be an element of $\mathcal{F}$, so it is a disjoint union of circuits. This also implies $C_1 \triangle \ldots \triangle C_n$ is a disjoint union of circuits, so M must satisfy **(6)**.

(6) $\implies$ (7)

We first notice that at this point in the proof, we have shown that **(5)** and **(6)** are equivalent. Indeed, we just showed **(5)** $\implies$ **(6)** in the previous step, and we have also shown (6) $\implies$ (4) $\implies$ (3) $\implies$ (2) $\implies$ (5).

Suppose **(7)** were false. Let C be a circuit and B be a basis, so $C \neq \triangle_{e \in C-B} C(e, B)$ and $C \triangle (\triangle_{e \in C-B} C(e, B))$ is non-empty. However, we do have $C - B = \triangle_{e \in C-B} C(e, B) - B$, so $C \triangle (\triangle_{e \in C-B} C(e, B)) \subset B$. Since we have assumed **(6)**, we may also assume **(5)** and conclude $C \triangle (\triangle_{e \in C-B} C(e, B))$ is dependent. This is a contradiction, so M must satisfy **(7)**.

(1) $\implies$ (3)

From our assumption of **(1)**, M is binary so there is an isomorphism $\phi : E(M) \mapsto V(r, 2)$ where r= r(M). If C_1 and C_2 are circuits of M, we have

$$\sum_{e \in C_1} \phi(e) = 0 = \sum_{e \in C_2} \phi(e)$$

so

$$\sum_{e \in C_1} \phi(e) + \sum_{e \in C_2} \phi(e) = 0$$

Now, since $C_1 \triangle C_2 = (C_1 \cup C_2) - (C_1 \cap C_2)$ and each element of $C_1 \cap C_2$ gets double counted in $C_1 \cup C_2$, we have

$$\sum_{e \in C_1 \triangle C_2} \phi(e) = \sum_{e \in C_1} \phi(e) + \sum_{e \in C_2} \phi(e) - 2 \sum_{e \in C_1 \cap C_2} \phi(e) = 0$$

Therefore, $C_1 \triangle C_2$ is dependent and must contain a circuit. We have established **(3)**.

(8) $\implies$ (1)

Before we start the proof, we need the following lemma:

Lemma 4.9. *Let X and Y be collections of subsets of a finite set E such that every member of X contains a member of Y, and every member of Y contains a member of X. Then X and Y have the same minimal members.*

Proof. Let M_X be a minimal member of X. Then M_X contains a member S_Y of Y. Now, S_Y contains a member of X, but this must be M_X since it is minimal. Therefore, M_X is a member of Y. Furthermore, M_X cannot properly contain a member of Y since such a member would in turn contain a member of X, so M_X is a minimal member of Y. One similarly shows that a minimal member M_Y of Y is a minimal member of X. Therefore, X and Y have the same minimal members. □

Now that we have this lemma, we can prove the last step. We first construct a candidate representation of M. First, consider a basis B of M satisfying the conditions of **(8)**. Let A be the fundamental circuit incidence matrix for B and r=r(M), so $[I_r|A]$ is a binary representation of the vector matroid $M[I_r|A]$. We notice that at this point in the proof, the fact that $M[I_r|A]$ is binary means that it satisfies conditions **(2)-(7)**. Furthermore, if $e \in E(M) - B$, the fundamental circuit $C_M(e, B)$ is also a circuit of $M[I_r|A]$. We will thus denote these circuits as $C(e, B)$ from now on.

The next step in our proof is to show that M = $M[I_r|A]$. Let C be a circuit of M, so C= $\triangle_{e\in C-B}C(e, B)$ by **(8)**. As we showed above, C(e,B) is a circuit of $M[I_r|A]$, so by **(6)** $C = \triangle_{e\in C-B}C(e, B)$ is a disjoint union of circuits of $M[I_r|A]$. In particular, every circuit of M is dependent in $M[I_r|A]$. Equivalently, any independent set of $M[I_r|A]$ is independent in M.

Now suppose C' is a circuit of $M[I_r|A]$. If $x \in C' - B$, then since $C' - x$ is independent, there exists a basis B' of $M[I_r|A]$ such that $B' \subset (B \cup C') - e$. Therefore, C' is the fundamental circuit of (e, B') in $M[I_r|A]$.

Since B' is independent in $M[I_r|A]$, it is also independent in M. Furthermore, $|B'| = r = r(M)$ since B' is a basis of $M[I_r|A]$, but this means it is also a basis element of M. If we consider $C_M(e, B')$, this is a disjoint union of circuits of $M[I_r|A]$ since it is a circuit of M. However, $C_M(e, B')$ contains e and is contained in $B' \cup e$, but C' is the unique circuit satisfying these conditions. Thus, we must have $C' = C_M(e, B')$, so any circuit of $M[I_r|A]$ is a circuit of M.

Every dependent set of M contains a circuit of M, which is a dependent set in $M[I_r|A]$. In addition, every dependent set in $M[I_r|A]$ contains a circuit of $M[I_r|A]$ which is a circuit of M. Thus, we may apply **Lemma 4.9** where X and Y are the collections of dependent sets of M and $M[I_r|A]$ to conclude that M and $M[I_r|A]$ have the same set of circuits. Since a matroid is uniquely determined by its circuits, M=$M[I_r|A]$ and is binary. We have established **(1)** and completed the proof of *Theorem 4.5.* □

From the previous theorem, Seymour found in [12] that we can also relax the conditions of (2) to give another characterization for binary matroids.

Theorem 4.10. *Let M be a matroid. The following statements are equivalent:*

(1) M is binary.
(2) If C is a circuit and C^* is a cocircuit, $|C \cap C^*| \neq 3$.
(3) M has no minor isomorphic to $U_{2,4}$.

Proof. We have already shown in *Theorem 4.1* that **(3)** implies **(1)**. Furthermore, we have shown in our previous theorem that **(1)** implies **(2)** since $|C \cap C^*|$ must

be even. It remains to show **(2)** implies **(3)**.

Suppose M has a minor X isomorphic to $U_{2,4}$. Let S be some 3-element subset of the ground set of X. Since the maximal independent sets of X and X^* have size 2, S is a circuit and a co-circuit of X. Therefore, there exist a circuit and cocircuit of M whose intersection is S, so the size of their intersection is 3. We have thus established **(2)** $\implies$ **(3)** by showing the contrapositive. □

5. The Case of Regular Matroids

5.1. Initial Observations and Motivation of Proof.

Now that we have given several characterizations of binary matroids, we will prove the more difficult excluded minor characterization for regular matroids. From the previous section, we know that $U_{2,4}$ is not binary and it is straightforward to check that all its proper minors are regular. Therefore, $U_{2,4}$ is an excluded minor for the class of regular matroids. The following lemma will help us conclude that F_7 and its dual are also excluded minors for this class.

Lemma 5.1. *F_7 is representable over $\mathbb{F}$ if and only if char($\mathbb{F}$)=2.*

Definition 5.2. Let M be a matrix. We let $M^{\#}$ denote the matrix obtained from replacing every non-zero entry with a 1.

Proof. As we have shown, F_7 is representable over any field of characteristic 2 with the following vector matroid:

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

Now suppose F_7 is representable over a field $\mathbb{F}$. Since F_7 has rank 3, it is represented by some vector matroid $M = [I_3|D]$. Label the columns of F_7 as $\{1, \ldots, 7\}$, and consider the basis B= $\{1, 2, 3\}$.

For $e \in \{4, \ldots, 7\}$, we notice that C= $\{m : m \in B,$ the entry of D in row m and column e is non-zero$\} \cup \{e\}$ is a circuit contained in $B \cup e$ that contains e. Therefore, this is the unique fundamental circuit C(e,B). From this observation, we conclude

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

Where $*$ denotes any non-zero element of $\mathbb{F}$, but two elements denoted with $*$ could have different values. Since we could divide the columns by non-zero scalars, we may assume

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & x & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & y & z & 1 \end{bmatrix}$$

Where x,y, and z are non-zero. Let $M_{a,b,c}$ denote the 3×3 matrix formed by columns a,b,c of M.

Since $\{2, 5, 7\}$ is dependent, we must have det($M_{2,5,7}$)= 1-y=0, so y=1. We can show x and z must be 1 in a similar manner by observing that $\{3, 4, 7\}$ and $\{1, 6, 7\}$

are also dependent. Finally, since $\{4,5,6\}$ is a dependent set in F_7, we must have $\det(M_{4,5,6})$=-2=0. We thus conclude that char($\mathbb{F}$)=2. □

Since duality preserves representability, the above lemma shows that F_7 and its dual are not ternary, and particularly not regular. Furthermore, it is shown in [1] that proper minors of F_7 are ternary. Therefore, F_7 and its dual are excluded minors for ternary matroids. Now, since F_7 and its dual are binary, their proper minors are binary. Since the proper minors of F_7 are binary and ternary, they must be regular, so F_7 is an excluded minor for regular matroids. By duality, F_7^* is also an excluded minor for regular matroids.

It was actually proved by Tutte in [15] that these are the only excluded minors for the regular matroids. In other words, we have the following theorem:

Theorem 5.3. *A matroid is regular if and only if it has no minor isomorphic to $U_{2,4}$, F_7, or F_7^*.*

From our proof of *Theorem 4.1*, it suffices to show the following statement:

Theorem 5.4. *A binary matroid is regular if and only if it has no minor isomorphic to F_7, or F_7^*.*

Tutte's proof of this statement was very long, and it uses various tools from Algebraic Geometry. The proof we present in this section is due to Gerards [3], and it is self-contained. The key to this proof is the observation by Tutte that a matroid M is representable over every field if and only if $M \cong M[A]$ for a totally unimodular matrix A. Therefore, our first step will be to rephrase **Theorem 5.4** in terms of matrices.

Definition 5.5. Given a $\{0,1\} - matrix$ M, a *signing* of M is a matrix Y over $\{0,1,-1\}$ such that $Y^{\#} = M$.

Proposition 5.6. *Let $[I_r|X]$ be a GF(2)-representation of a binary matroid M. Then the following are equivalent:*

(1) M is regular.
(2) X has a totally unimodular signing.
(3) $[I_r|X]$ has a totally unimodular signing.

Proof. Let M be regular. Then M has a representation $[I_r|Z]$ such that this matrix is totally unimodular and the identity map of the columns $\{e_1,\ldots,e_n\}$ in $[I_r|Z]$ to $\{e_1,\ldots,e_n\}$ in $[I_r|X]$ is an isomorphism. This implies $Z^{\#} = X^{\#}$, so Z is a totally unimodular signing of X. We have shown that **(1)** $\implies$ **(2)**.

Suppose X has a totally unimodular signing Z. Then $[I_r|Z]$ is a totally unimodular signing of $[I_r|X]$. Furthermore, $M[I_r|Z] = M[I_r|X] = M$, so M is regular. We have completed the proof by showing **(2)** $\implies$ **(3)** and **(3)** $\implies$ **(1)**. □

Suppose

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

Using the previous proposition, we see that *Theorem 5.4* can be rephrased in terms of matrices with the following theorem:

Theorem 5.7. *The following are equivalent for a $\{0,1\}$-matrix $M = [I_r|X]$:*

(1) X has no totally unimodular signing
(2) When viewed over GF(2), $[I_r|X]$ can be transformed into $[I_3|X_F]$ or $[I_4|X_F^T]$ through a sequence of deleting rows and columns, permuting rows and columns, and pivoting.

Indeed, the second statement in the above theorem can be equivalently expressed by saying the vector matroid M has a minor isomorphic to F_7 or F_7^*. To prove this theorem, we need several lemmas, many of which highlight the properties of totally unimodular matrices that will be useful in our proof.

5.2. **Preliminary Lemmas.**

Lemma 5.8. *Let G be a simple, connected, bipartite graph such that the graph becomes disconnected when two distinct vertices from the same vertex class are deleted. Then G is either a path or a cycle.*

Proof. Suppose by contradiction that G is neither a path nor a cycle. This means that some vertex of G has degree at least 3. Since G is connected, there exists a spanning tree T with a vertex of degree at least 3. If we label this vertex v, then since each branch of v must have a path to a distinct vertex with degree 1, T has at least 3 vertices with degree 1. If we label these vertices u, v, and w, we notice at least two of these must be non-adjacent in G since it is not a cycle. Without loss of generality, we may assume u and v are in the same vertex class of G. However, deleting u and v would cause G to remain connected since T remains connected. This is a contradiction, so G must be a path or a cycle. □

Lemma 5.9. *Let D be an $n \times n$ matrix with entries in $\{0, 1, -1\}$. If $G(D^{\#})$ is a cycle, then D is totally unimodular if and only if the number of negative entries in D is congruent to n modulo 2.*

Proof. Since G($D^{\#}$) is a cycle, we could permute the columns of $D^{\#}$ to obtain

$$D_1^{\#} = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 & 1 \\ 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 \end{bmatrix}$$

Since permuting the rows and columns of a matrix only changes its determinant by a sign, we may assume $D_1 = D$. Given D, we can put it in the form

$$D_2 = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 & d_{1n} \\ 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & 1 \end{bmatrix}$$

by iterating through column 1, row 2, column 2, row 3, ..., row n, and multiplying by -1 if the first non-zero element of the row or column we are observing is -1. Notice that each of these multiplications changes the sign of 2 non-zero elements each time, so the number of negative entries in D_2 is congruent to the number of negative entries in D modulo 2. Furthermore, since multiplying a row/column of matrix by a constant multiplies the determinant of a matrix by that constant, we

have $|det(D)| = |det(D_2)|$.

Now, we claim D is totally unimodular if and only if $det(D) \in \{0, 1, -1\}$ If D is totally unimodular, then its determinant must be 0, 1, or -1 since it is a square matrix. Now assume $det(D) \in \{0, 1, -1\}$. If we can show that any proper square sub-matrix of D has determinant in $\{0, 1, -1\}$, we may conclude D is totally unimodular. Notice that deleting a row and column of D leaves a row or column with at most one 1 entry. Since we can obtain any proper square sub-matrix of D through a sequence of deleting a row and column, we conclude any proper square sub-matrix has determinant in $\{0, 1, -1\}$, so D is totally unimodular.

Next, we notice that $det(D_2) = 1 + (-1)^{n-1}d_{1n}$. Since $|det(D)| = |det(D_2)| = |1 + (-1)^{n-1}d_{1n}|$, we have $det(D) \in \{0, 1, -1\}$ if and only if $(-1)^{n-1}d_{1n} = -1$, if and only if $d_{1n} = (-1)^n$. Therefore, D is totally unimodular if and only if $d_{1n} = (-1)^n$. Since the number of negative entries in D_2 is congruent to n modulo 2, we conclude D is totally modular if and only if the number of negative entries in D is congruent to n modulo 2 since D and D_2 have the same number of negative entries modulo 2. □

Lemma 5.10. *Suppose D_1 and D_2 are totally unimodular matrices. If $D_1^{\#} = D_2^{\#}$, then D_2 can be obtained from D_1 by multiplying some rows and columns by -1.*

Proof. The proof of this appears in the paper [2] by Camion, which highlights many properties of totally unimodular matrices. □

Before we prove the final lemmas in this section, we briefly discuss the matrix operation of pivoting as it might not be as familiar as other matrix operations.

Definition 5.11. Suppose M is a $m \times n$ matrix. If a_{ij} is an element of M, a *pivot* about a_{ij} transforms the jth column of M into the ith standard basis vector. More explicitly, we perform the following operations:

(1) For $k \in \{1, 2, \ldots, i-1, i+1, \ldots, m\}$, replace row k by (row k)-($\frac{a_{kj}}{a_{ij}}$)(row i).
(2) Multiply row i by $\frac{1}{a_{ij}}$.

When we pivot about a_{ij}, this entry becomes 1. We call it the *pivot entry.*

The following lemma gives a crucial connection between total unimodularity and pivoting:

Lemma 5.12. *Let X be a totally unimodular matrix. If Y is obtained by pivoting X about a non-zero entry, then Y is totally unimodular.*

Lemma 5.13. *(1) If $G(A_1^{\#})$ is connected then so is $G(A_3^{\#})$.*
(2) If

$$\left[\begin{array}{c|c} \alpha & x^T \\ \hline y & Z \end{array}\right]$$

is square, then its determinant is $\alpha det(Z - \alpha^{-1}yx^T)$.

Proof. The second statement follows by observing that multiplying the rows or columns of a matrix scales its determinant by the same amount, and adding one row to another does not change its determinant.

For the first part, suppose by contradiction that $G(A_3^{\#})$ is disconnected. If A

is the adjacency matrix for a graph G, G is disconnected if and only if A can be written in block diagonal form by permuting the rows and columns since no edge in one connected component is adjacent with the vertices of any other connected component. Therefore, we can transform A_3 into a block diagonal matrix D_3 by permuting its rows and columns. Since we can obtain A_1 by pivoting A_3 about α^{-1}, we can obtain a matrix that is a permutation of the rows and columns of A_1 by pivoting D_3. However, a pivot of D_3 produces another block diagonal matrix, which would imply A_1 can be written in block diagonal form by permuting its rows and columns, so $G(A_1^{\#})$ is disconnected. This is a contradiction, so $G(A_3^{\#})$ is connected. □

5.3. **Proof of Theorem 5.7.**

Suppose X has a totally unimodular signing, and $[I_r|X]$ can be transformed into $[I_3|X_F]$ or $[I_4|X_F^T]$ through the operations described in *Theorem 5.7*. By observing how these operations affect the determinant of a matrix, we would conclude without loss of generality that $[I_3|X_F]$ has a totally unimodular signing, which would imply that F_7 is regular. However, this is a contradiction as we have shown that this matroid is not ternary. Therefore, we must have **(2)** $\implies$ **(1)**.

For the opposite direction, assume X has no totally unimodular signing. Because we can iteratively examine the proper submatrices of X, we may assume every proper submatrix of X does have a totally unimodular signing. Define a simple bipartite graph G(X) as follows:

Label the rows of X as $\{v_1, \ldots, v_r\}$ and the columns of X as $\{v_{r+1}, \ldots, v_n\}$. Let G(X) have vertex classes A=$\{v_1, \ldots, v_r\}$ and B=$\{v_{r+1}, \ldots, v_n\}$, where $v_i \in A$ is adjacent to $v_j \in B$ if and only if X has a 1 in row v_i and column v_j. G(X) must be connected, and it cannot be a path or a cycle, because otherwise its adjacency matrix would be of block diagonal form and therefore unimodular (since the product of the block determinants, would be 0, 1, or -1). This would imply X has a totally unimodular signing, which is a contradiction. By *Lemma 5.8*, we could delete two vertices from the same vertex class and the remaining graph would still be connected. In other words, we can permute the columns of X or X^T to obtain a matrix of the form $[x|y|Z]$ where x and y are column vectors, and G(Z) is connected.

Since $M_1 = [x|Z]$ and $M_2 = [y|Z]$ are proper submatrices of X, they have totally unimodular signings. Suppose Z_1 is the signing of Z in M_1 and Z_2 is the signing of Z in M_2. By *Lemma 5.10*, we can obtain Z_2 from Z_1 by multiplying some rows and columns by -1. Therefore, we may assume $Z_1 = Z_2$, since multiplying rows and columns of the signing of M_1 by -1 would still produce a signing. We conclude that Y can be obtained by permuting the rows and columns of X or X^T where Y has a signing $[x'|y'|Z']$ satisfying the following conditions:

(1) G($Z'^{\#}$) is connected
(2) $[x'|Z']$ and $[y'|Z']$ are totally unimodular.

If we can show that Y can be transformed into X_F by the transformations described in the statement of *Theorem 5.7*, we will have completed the proof.

We first notice $[x'|y'|Z']$ is not totally unimodular, so by *Lemma 5.13* we can pivot this matrix about an element of Z' and obtain another matrix satisfying the two conditions listed in the previous paragraph. If we do this pivot over $\mathbb{R}$, the resulting matrix is still a signing of Y. Also, we notice that if we take the resulting entries modulo 2, this is the same matrix as if we first viewed $[x'|y'|Z']$ over GF(2) and performed the pivot over GF(2).

Let $\mathcal{Z}$ be the collection of matroids that can be obtained from $[x'|y'|Z']$ by a sequence of pivots in Z'. Suppose $[x_1|y_1|Z_1] \in \mathcal{Z}$ with a submatrix W whose determinant is not in $\{0, 1, -1\}$, such that every square matrix smaller than W that is the submatrix of a member of $\mathcal{Z}$ has determinant in $\{0, 1, -1\}$. We then have the following lemma:

Lemma 5.14. *W is a submatrix of* $[x_1|y_1]$ *and can be obtained from* $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ *by multiplying some rows and columns of* $[x_1|y_1|Z_1]$ *by -1.*

Proof. Suppose W intersects Z_1. Define $[x_2|y_2|Z_2]$ to be the matrix obtained by pivoting $[x_1|y_1|Z_1]$ about an element of $W \cap Z_1$. However, $[x_2|y_2|Z_2]$ has a square sub-matrix W' that is smaller than W, but by *Lemma 5.13* we have $|det(W')| = |det(W)|$ since Z_1 has non-zero elements 1 or -1. This is a contradiction to our choice of W, so W must be a square submatrix of $[x_1|y_1]$. These are column vectors, so W is a 2×2 matrix, and the final statement of the lemma follows. □

This means that we can assume $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is a submatrix of $[x_1|y_1]$, and it occurs in the first two rows of $[x_1|y_1]$ since we could permute the rows to achieve this. Let $Y_1 = [x_1|y_1|Z_1]$, so $G(Z^{\#})$ is connected and thus has a shortest path connecting the vertices corresponding to rows 1 and 2. P must have length greater than 2, since otherwise this would imply $[x_1|Z_1]$ or $[x_2|Z_1]$ are not totally unimodular. Therefore, we can obtain a $k \times (k+1)$ submatrix of Y_1 in the form:

$$\left[\begin{array}{cc|ccccccc} 1 & 1 & * & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & \dots & 0 & 0 & * \\ \hline & & * & * & 0 & \dots & 0 & 0 & 0 \\ & & 0 & * & * & \dots & 0 & 0 & 0 \\ & & 0 & 0 & * & \dots & 0 & 0 & 0 \\ & D & \vdots & & \vdots & \dots & \vdots & \vdots & \vdots \\ & & 0 & 0 & 0 & \dots & * & * & 0 \\ & & 0 & 0 & 0 & \dots & 0 & * & * \end{array}\right]$$

.

We achieve this by permuting the rows of Y_1 and the columns of Z_1. The starred entries are either 1 or -1, but we can assume that they are all 1 by iterating through column 3, row 3, column 4, row 4, ..., column k, row k, and multiplying by -1 if the first non-zero entry in the row or column we observe is -1. For the last column, we can multiply by -1 and multiply row 2 by -1. We may assume the block in the top-left corner is still $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ since we could switch columns 1 and 2.

Now, if we pivot the matrix above about the entry in row 3 and column 4 and delete that row and column, we obtain a $(k-1) \times k$ matrix of the form:

$$\left[\begin{array}{cc|ccccccc} 1 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ \hline & & -1 & 1 & 0 & \dots & 0 & 0 & 0 \\ & & 0 & 1 & 1 & \dots & 0 & 0 & 0 \\ & & 0 & 0 & 1 & \dots & 0 & 0 & 0 \\ & D' & \vdots & & \vdots & \dots & \vdots & \vdots & \vdots \\ & & 0 & 0 & 0 & \dots & 1 & 1 & 0 \\ & & 0 & 0 & 0 & \dots & 0 & 1 & 1 \end{array}\right]$$

. By a similar argument as before, we can make all the non-zero entries in the two right blocks 1, and assume the top-left block is $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. If we keep iterating through this process, we will eventually obtain the 3×4 matrix:

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & -1 & 0 & 1 \\ a & b & 1 & 1 \end{bmatrix}$$

. We note that $a, b \in \{0, 1, -1\}$. Furthermore, we notice that the matrices obtained by deleting either column 1 or 2 are totally unimodular. Since $\begin{bmatrix} -1 & 1 \\ b & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ b & 1 \end{bmatrix}$ are square submatrices, we cannot have $b = 1, -1$, otherwise one of these matrices would have determinant 2 or -2. Therefore, b=0. Finally, the matrix obtained by deleting the second column of the 3×4 matrix has determinant $c - 2$, so we need $c = -1$. This means that the 3×4 matrix is X_F when viewed over $\mathbb{F}_2$. We have thus obtained X_F from Y, and our proof is complete.

Acknowledgments

First of all, I thank my mentor Pallav Goyal for suggesting this topic to me, and for answering all my questions throughout the process of learning the material and writing this paper. Without his guidance and support, this project would not have been possible. I also thank Peter May for all the hard work he put into making this REU a success, especially given the constraints of an online format. Next, I thank my professors for their constant support and infectious enthusiasm for math. Finally, I thank my wonderful friends and family for all the love and support they have given me, especially in the difficult circumstances of this summer.

References

[1] Bixby, R.E. On Reid's characterization of ternary matroids. Journal of Combinatorial Theory. 1979.

[2] Camion, Paul. Characterization of totally unimodular matrices. Proceedings of the American Mathematical Society. 1965.

[3] Gerards, A.M.H. A short proof of Tutte's characterization of totally unimodular matrices. Linear Algebra and its Applications. 1989.

[4] Las Vergnas, Michel. Fundamental circuits and a characterization of binary matroids. Discrete Mathematics. 1980.

[5] Lehman, Alfred. A solution of the Shannon Switching Game. Journal of the Society of Industrial and Applied Mathematics. 1964.

[6] Mayhew, Dillon. Lecture Notes for Math 432: Matroid Theory. https://sms.wgtn.ac.nz/Courses/MATH432_2020T2/. 2016.
[7] Minty, G.J. On the axiomatic foundations of the theories of directed linear graphs, electrical networks and network programming. Journal of Mathematics and Mechanics. 1966.
[8] Oxley, J.G. Matroid Theory. Oxford University Press. 1992.
[9] Oxley, J.G. On the interplay between graphs and matroids. Surveys in Combinatorics. 2001.
[10] Rado, R. Note on independence functions. Journal of the London Mathematical Society. 1957.
[11] Crapo, H.H, and Rota, G-C. On the Foundations of Combinatorial Theory: Combinatorial Geometries. MIT Press. 1970.
[12] Seymour, Paul. The forbidden minors of binary clutters. Journal of the London Mathematical Society. 1976.
[13] Seymour, Paul. Matroid representation over GF(3). Journal of Combinatorial Theory. 1979.
[14] Seymour, Paul. Decomposition of regular matroids. Journal of Combinatorial Theory. 1980.
[15] Tutte, W.T. A homotopy theorem for matroids, I, II. Transactions of the American Mathematical Society. 1958.
[16] Tutte, W.T. Lectures on matroids. Journal of Research of the National Bureau of Standards. 1965.
[17] Whitney, J.H. On the abstract properties of linear dependence. American Journal of Mathematics. 1935.