INTRODUCTION TO A MATROID AND ITS REPRESENTABILITY

HIDENORI SHINOHARA

Abstract. This paper introduces a matroid. A matroid is a mathematical structure that abstracts the concept of linear independence. The goal of this paper is to discuss the representability of a matroid with several examples and to introduce an important conjecture related to the representability of a matroid.

1. Introduction to Matroid

A matroid is a mathematical structure that abstracts the concept of linear independence. A linearly independent set of vectors has a lot of good properties. Interestingly, a lot of sets of other mathematical objects often share those properties. For example, any subset of a linearly independent set of vectors is always linearly independent. Consider a subset of edges of a graph that does not contain any cycle. Then any subset of it does not contain any cycle. The matroid theory is an attempt to mathematically formalize those properties.

Definition 1.1. A matroid $M = (E, \mathcal{I})$ is a pair such that E is a finite set of elements, and $\mathcal{I}$ is a family of subsets of E with the following properties:

- $\emptyset \in \mathcal{I}$
- For any $A \in \mathcal{I}$, any subset of A is in $\mathcal{I}$.
- For any $A, B \in \mathcal{I}$ such that $|A| < |B|$, there always exists $x \in B - A$ such that $A \cup \{x\} \in \mathcal{I}$.

E is called the ground set, $\mathcal{I}$ is called a family of independent sets. A subset of E is called independent if and only if it is in $\mathcal{I}$. In this paper, we will put our focus on a matroid with a finite ground set.

There are some basic matroids that are important in the following discussion. We will start by introducing a column matroid. A column matroid is constructed from a matrix over a field $\mathbb{F}$.

Definition 1.2. Let a matrix A with m rows over $\mathbb{F}$ be given. A column matroid M of A is a matroid with a ground set $\mathrm{E} = \{1, 2, \cdots m\}$. A subset of E is independent in M if and only if the set of the corresponding column vectors is linearly independent.

Theorem 1.3. *A column matroid is indeed a matroid.*

Proof. First, an empty set of vectors is linearly independent by definition. Suppose there exists a linearly independent set of vectors that has a linearly dependent subset. Let $A = \{a_1, \cdots, a_k\} \subseteq B = \{b_1, \cdots, b_n\}$ be such sets. Since A is linearly dependent, there exist constants $c_1, \cdots, c_k$ such that $c_1a_1 + \cdots + c_ka_k = 0$ and

Date: April 28, 2016.

not all c_i's are 0. However, that implies that we can find constants $d_1, \cdots, d_n$ such that $d_1b_1 + \cdots + d_kb_k = 0$ and not all d_i's are 0. This is a contradiction since B is supposed to be independent. Therefore, such a subset must not exist, and thus all subsets of linearly independent sets are linearly independent. Now we want to prove the third property. Let $A = \{a_1, \cdots, a_k\}, B = \{b_1, \cdots, b_n\}$ be linearly independent sets, and assume that $k < n$. Suppose for each $i = 1, \cdots, n$, $b_i \in span\{a_1, \cdots, a_k\}$. It means that the span of B is a subspace of the span of A, which has a smaller dimension than n. That is a contradiction. Therefore, there exists i such that $b_i \notin span\{a_1, \cdots, a_k\}$. For such i, $\{a_1, \cdots, a_k, b_i\}$ should be linearly independent. Since a column matroid satisfies the three properties, it is indeed a matroid. □

Definition 1.4. A uniform matroid $U_{r,k}$ is a matroid such that $E = \{1, \cdots, k\}$ and $\mathcal{I} = \{X \mid X \subseteq E, |X| \leq r\}$.

It is easy to see that a uniform matroid is indeed a matroid.

Here are some important results that will show up later in this paper.

Theorem 1.5. *All maximal independent sets have the same size.*

Proof. Let X, Y be maximal independent sets of some matroid. Suppose $|X| \neq |Y|$. Without loss of generality, $|X| < |Y|$. By the third property of a matroid, there exists $e \in Y - X$ such that $X \cup \{e\}$ is independent. It is a contradiction since X is a maximal independent set. Therefore $|X| = |Y|$. □

This is indeed true in linear algebra. Given a matrix, any maximal independent subset of column vectors always has the same size. In linear algebra, this number is often referred to as the *dimension* of a vector space or the *rank* of a matrix. In the matroid theory, we use the term *rank* as well.

Definition 1.6. The rank of a matroid is the size of a maximal independent set.

The rank of a column matroid is equal to the rank of the matrix since the subset of a ground set is independent if and only if the subset of column vectors is linearly independent.

Definition 1.7. Let $M = (E, \mathcal{I})$ be given. $e \in E$ is called a loop if $\{e\} \notin \mathcal{I}$.

We will conclude this chapter by introducing the notion of isomorphic matroids.

Definition 1.8. Let $M_1 = (E_1, \mathcal{I}_1), M_2 = (E_2, \mathcal{I}_2)$ be given. M_1, M_2 are isomorphic to each other if there exists a bijective mapping $\phi : E_1 \to E_2$ such that $\forall X \subseteq E_1, X \in \mathcal{I}_1 \iff \{\phi(e) : e \in X\} \in \mathcal{I}_2$.

Two isomorphic matroids have the same structure.

2. Introduction to representability

We will start this chapter by defining the representability of a matroid.

Definition 2.1. A matroid $M = (E, \mathcal{I})$ is representable over a field $\mathbb{F}$ if there exists a matrix A over $\mathbb{F}$ such that the column matroid of A is isomorphic to M.

Therefore, if the matroid indeed succeeded in abstracting the concept of linear independence, there should be some matroids that are *not* representable over some fields. If all matroids are representable over every field, it means that we are simply discussing linear algebra using different terms.

Before introducing some unrepresentable matroids, we will start by introducing a nice property of representable matroids.

Theorem 2.2. *Let $M = (E, \mathcal{I})$ be a matroid that is representable over $\mathbb{F}$. Let r be a rank of M and $k = |E|$. Then there exists a matrix $A \in \mathbb{F}^{r \times k}$ such that M is isomorphic to the column matroid of A.*

Proof. Let B a matrix over $\mathbb{F}$ such that the column matroid of B is isomorphic to M. It is easy to see that the number of columns of B is k. From linear algebra, we know that elementary row operations preserve the linear independence of column vectors. Let R be the reduced row echelon form of B. Since R must have a rank of r, it only has r leading zeros. In other words, R has exactly r non-zero row vectors. Removing zero rows clearly does not affect the linear independence. Therefore, we found a matrix in $\mathbb{F}^{r \times k}$ whose column matroid is isomorphic to M. □

This property is useful when proving that a matroid is unrepresentable over some field.

Here are some matroids that are not representable over some fields to show that not all matroids are representable over every field.

Theorem 2.3. *$U_{2,4}$ is not representable over $GF(2)$.*

A matroid is called a *binary matroid* if it is representable over $GF(2)$.

Proof. We know that $U_{2,4}$ has a rank of 2. If $U_{2,4}$ is representable over $GF(2)$, there exists a matrix $A \in GF(2)^{2\times 4}$ such that A's column matroid is isomorphic to $U_{2,4}$. Since $GF(2)$ only has two elements, there are only four possible column vectors of size 2. $\left\{ \begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix} \right\}$ A must not contain $\begin{pmatrix}0\\0\end{pmatrix}$ since it is a loop. Since A has 4 columns and there are only 3 different column vectors, we know that there are two columns in A that have the exact same column vectors. This is a contradiction since a subset of such two elements will not be independent. Therefore, $U_{2,4}$ is not representable over $GF(2)$. □

Remark 2.4. $U_{2,4}$ is representable over some field such as $\mathbb{R}$. For example, the column matroid of $\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & 2 & 3 & 4\end{pmatrix}$ is isomorphic to $U_{2,4}$.

Now, we will introduce the Fano matroid. The Fano matroid can be constructed from the Fano plane. The Fano matroid is one of the examples of matroids that are representable over $GF(2)$, but not over $\mathbb{R}$. We will start by defining the Fano matroid mathematically.

Definition 2.5. The Fano matroid is a matroid with a ground set $\{1, 2, \cdots, 7\}$. Each number corresponds to the vertex in the figure 1. A set S of elements is independent if it satisfies one of the following:

(1) $|S| < 3$,
(2) $|S| = 3$ and the corresponding vertices are not on the same line.

S is always dependent if $|S| > 3$.

For example, $\{4, 5\}$ and $\{1, 2, 3\}$ are independent, but $\{1, 4, 2\}$, $\{1, 5, 7\}$, and $\{4, 5, 6\}$ are not independent as each of them is on one line.

Theorem 2.6. *The Fano matroid is indeed a matroid.*

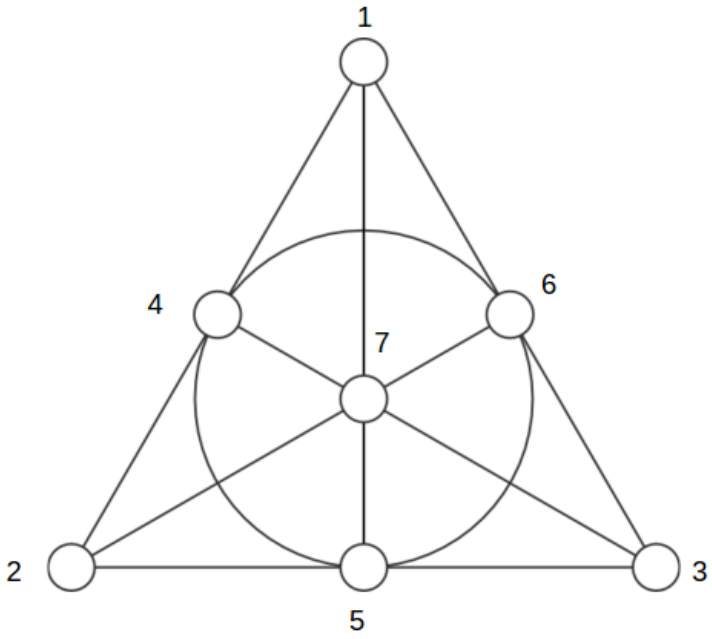

FIGURE 1. Fano plane

Proof. An empty set is independent since it contains less than 2 elements. Any independent set has at most three elements, so any proper subset of it has at most two elements. Therefore, any subset of independent sets is always independent. The third property can be proved by checking each case. Since any set with 2 or fewer elements is independent, we only need to care about the case when we have a set with 2 elements and a set of three elements. Let $A = \{a_1, a_2, a_3\}$, $B = \{b_1, b_2\}$ be independent sets. It is easy to see from the figure that there must be exactly one line that goes through both b_1 and b_2. Let x denote the third point on such line. Then, adding any element other than b_1, b_2, x to B will generate an independent set of three elements. Therefore, we just need to make sure that $A \neq \{b_1, b_2, x\}$. That cannot be the case since $\{b_1, b_2, x\}$ is dependent and A is independent. Therefore, there must be an element $a \in A - B$ such that $B \cup \{a\}$ is independent. Since the Fano matroid satisfies all three properties, it is indeed a matroid. □

Here is an interesting property of the Fano matroid

Theorem 2.7. *If the Fano matroid is representable over a field* $\mathbb{F}$*,* $1 + 1 = 0$ *in that field.*

Proof. Suppose the Fano matroid is representable over a given field $\mathbb{F}$. Let $A \in \mathbb{F}^{3\times 7}$ such that A's column matroid is isomorphic to the Fano matroid. Let R be a row reduced echelon form of A. Then the first three columns should be identical to I_3 since R has a rank of 3. Since $\{1, 2, 4\}$ is dependent, $R_{3,4}$ is 0. Applying the same argument to $\{2, 3, 5\}, \{1, 3, 6\}$, we get the following:

$$\begin{pmatrix} 1 & 0 & 0 & ? & 0 & ? & ? \\ 0 & 1 & 0 & ? & ? & 0 & ? \\ 0 & 0 & 1 & 0 & ? & ? & ? \end{pmatrix}$$

All of $4, 5, 6, 7$th columns have to contain at least two nonzero elements. If it is a zero vector, it will be a loop, and if it only has exactly one nonzero element, it will be parallel to one of the first three columns. Since multiplying a nonzero constant to some column does not affect the linearly independency, assume that the first non-zero elements of 4, 5, 6th columns, are all 1. Therefore, we get the following matrix.

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & ? \\ 0 & 1 & 0 & ? & 1 & 0 & ? \\ 0 & 0 & 1 & 0 & ? & ? & ? \end{pmatrix}$$

Let $a = R_{2,4}, b = R_{3,5}$. Since both the 4th columnn and the 5th column contain at least two nonzero elements, neither a nor b is 0

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & ? \\ 0 & 1 & 0 & a & 1 & 0 & ? \\ 0 & 0 & 1 & 0 & b & ? & ? \end{pmatrix}$$

Since $\{4, 5, 6\}$ is dependent, $R_{3,6}$ must be $-ab$.

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & ? \\ 0 & 1 & 0 & a & 1 & 0 & ? \\ 0 & 0 & 1 & 0 & b & -ab & ? \end{pmatrix}$$

We need to look into the seventh column. The seventh column actually cannot contain any zero. For example, suppose $R_{1,7} = 0$. Then, $\{2, 3, 7\}$ would be dependent. That's a contradiction. Similar arguments apply to the case of $R_{2,7} = 0, R_{3,7} = 0$. By multiplying a non-zero constant, we get:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & a & 1 & 0 & ? \\ 0 & 0 & 1 & 0 & b & -ab & ? \end{pmatrix}$$

Since $\{3, 4, 7\}$ is dependent, $R_{2,7} = a$. And since $\{1, 5, 7\}$ is dependent, $R_{3,7} = b, R_{2,7} = ab$.

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

$\{2, 6, 7\}$ is dependent as well. By observing those three columns, it is easy to see that $-(-ab) + ab$ must be 0. Since neither a nor b is 0, $ab(1 + 1) = 0$ implies $1 + 1 = 0$. □

This theorem is powerful, since this implies that the Fano matroid is not representable over $\mathbb{R}$.

Corollary 2.8. *Fano matroid is not representable over* $\mathbb{R}$.

Proof. In $\mathbb{R}$, $1+1 \neq 0$. Therefore, the Fano matroid is not representable over $\mathbb{R}$. □

Theorem 2.9. *If a matroid $M = (E, \mathcal{I})$ only contains at most 3 non-loop elements, it is representable over any field $\mathbb{F}$.*

A matroid is called *regular* if it can be represented over any field.

Proof. It is easy to see that all the loop elements will be associated with zero vectors. Therefore, it suffices to show the proposition for matroids with $|E| \leq 3$. If $E = \emptyset$, we are done. Since $0 < |E| \leq 3$, the rank of the matroid must be at most 3. Since E does not contain any loop and it is not empty, the rank of the matroid must be at least 1.

(1) $rank(M) = 1$
A matrix $A \in F^{1\times|E|}$ filled with 1 will give a column matroid that is isomorphic to M. Every column vector is linearly independent, but a set with at least two vectors is always linearly dependent.
(2) $rank(M) = 2$
It is easy to see that $|E| \geq 2$.
- $|E| = 2$
  It is easy to see that $\mathcal{I} = \{S \mid S \subseteq E\}$. It means that $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ will give an isomorphic matroid.
- $|E| = 3$
  Without loss of generality, $E = \{1, 2, 3\}$, and let $\{1, 2\}$ be independent since there must be at least one independent set of size 2. Since E does not contain any loop element, $\{3\}$ must independent. By the property of matroids, at least one of $\{1, 3\}, \{2, 3\}$ must be independent.
  (a) $\{1, 3\}$ is independent, but $\{2, 3\}$ is not.
  $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.
  (b) $\{2, 3\}$ is independent, but $\{1, 3\}$ is not.
  Similar to the previous case.
  (c) Both of them are independent.
  $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.

(3) $rank(M) = 3$
Since the rank is 3, $\mathcal{I} = \{S \mid S \subseteq E\}$. I_3 will give a column matroid which is isomorphic to M.

Therefore, in any case, M is representable. □

3. More discussion on matroid representability

This chapter will introduce a new concept, a matroid minor, which is crucial when discussing the matroid representability.

In order to introduce a matroid minor, we first need to introduce two operations on matroids: deletion and contraction.

Definition 3.1. Let $M = (E, \mathcal{I})$, $e \in E$ be given. $M\backslash e$ is defined to be $(E - \{e\}, \{I \in \mathcal{I} \mid e \notin I\})$.

Theorem 3.2. *Let $M = (E, \mathcal{I})$, $e \in E$ be given. $M\backslash e$ is indeed a matroid.*

Proof. Let $M' = M\backslash e = (E', \mathcal{I}')$. $\emptyset \in \mathcal{I}'$ since $\emptyset \in \mathcal{I}$ and $e \notin \emptyset$. Let $I \in \mathcal{I}'$ and $J \subseteq I$. Since $e \notin I$, $e \notin J$. Since $I \in \mathcal{I}'$, $I \in \mathcal{I}$. Since $J \subseteq I$, $J \in \mathcal{I}$. Therefore, $J \in \mathcal{I}'$. Let $A, B \in \mathcal{I}'$ such that $|A| < |B|$. Since $A, B \in \mathcal{I}'$, they are in $\mathcal{I}$. Let $x \in B - A$ such that $A \cup \{x\} \in \mathcal{I}$. Since $e \notin B$, $e \notin x$. Therefore, $e \notin A \cup \{x\}$. It means that we have found $x \in B - A$ such that $A \cup \{x\} \in \mathcal{I}'$. Since M' satisfies the three properties, it is indeed a matroid. □

The above is the definition of deletion by an element. It is also possible to define deletion by a subset of E.

Definition 3.3. Let $M = (E, \mathcal{I}), X = \{x_1, \cdots, x_k\} \subseteq E$. $M\backslash X$ is defined to be $(((M\backslash x_1)\backslash x_2)\cdots)\backslash x_k)$.

The following theorem shows that the order of deletion does not matter.

Theorem 3.4. *For any given matroid $M = (E, \mathcal{I})$, $(M\backslash e)\backslash f = (M\backslash f)\backslash e$ for any $e \neq f \in E$.*

Proof. First, it is easy to see that $(M\backslash e)\backslash f$ and $(M\backslash f)\backslash e$ have the same ground set, which is $E\backslash\{e, f\}$. Therefore, it suffices to check the family of independent sets. The family of independent sets of $M\backslash e$ is $\mathcal{I}' = \{I \in \mathcal{I} \mid e \notin I\}$. The family of independent sets of $(M\backslash e)\backslash f$ is $\mathcal{I}'' = \{I \in \mathcal{I}' \mid f \notin I\}$. Obviously, $\mathcal{I}'' \subseteq I$, and, for any $I \in \mathcal{I}$, $I \in \mathcal{I}''$ if and only if $e \notin I$ and $f \notin I$. Therefore, the family of independent sets of $(M\backslash e)\backslash f = \{I \in \mathcal{I} \mid \{e, f\} \cap I = \emptyset\}$. Now, it is easy to see that $(M\backslash e)\backslash f = (M\backslash f)\backslash e$. □

Here are a few simple yet useful results about deletion.

Theorem 3.5. *Let a matroid $M = (E, \mathcal{I}), X \subseteq E$ be given. Let A be an independent set in $M\backslash X$. Then A is independent in M.*

Proof. A family of independent sets of $M\backslash X$ is $\{I \in \mathcal{I} \mid (I \cap X) = \emptyset\}$. It is easy to see that it is a subset of $\mathcal{I}$. Since A is in the subset of $\mathcal{I}$, A must be in $\mathcal{I}$. □

In other words, this means that deletion never "adds" a new element to a family of independent sets.

Theorem 3.6. *The deletion of a loop does not change a family of independent sets.*

Proof. Let $M = (E, \mathcal{I}), e \in E, \{e\} \notin \mathcal{I}$. A family of independent sets of $M\backslash e$ is $\{I \in \mathcal{I} \mid (I \cap \{e\}) = \emptyset\}$. Since $\{e\}$ is a loop, no independent set can contain e. Therefore, a family of independent sets of $M\backslash e$ is identical to $\mathcal{I}$. □

Since we have defined deletion, we are going to define contraction.

Definition 3.7. Let $M = (E, \mathcal{I})$, $e \in E$ be given. M/e denotes contraction of M by e and $M/e = \begin{cases} M\backslash e, \text{if } e \text{ is a loop,} \\ (E - \{e\}, \{I \in \mathcal{I} \mid e \notin I, (I \cup \{e\}) \in \mathcal{I}\}), \text{ otherwise.} \end{cases}$

Theorem 3.8. *Contraction by an element indeed generates a matroid.*

Proof. If e is a loop, M/e is obviously a matroid since we know that deletion always generates a matroid. Suppose otherwise. Let $\mathcal{I}'$ denote a family of independent sets of M/e. First, $\emptyset \in \mathcal{I}, e \notin \emptyset$. Since e is not a loop, $(\emptyset \cup \{e\}) \in \mathcal{I}$. Therefore, $\emptyset \in \mathcal{I}'$. Let $I \in \mathcal{I}', J \subseteq I$. Since $I \in \mathcal{I}$, $J \in \mathcal{I}$. Since $e \notin I$, $e \notin J$. Since $(I \cup \{e\}) \in \mathcal{I}$ and $J \subseteq I$, $(J \cup \{e\}) \in \mathcal{I}$. Therefore, $J \in \mathcal{I}'$. Let $A, B \in \mathcal{I}'$ such that $|A| < |B|$. Let $A' = A \cup \{e\}, B' = B \cup \{e\}$. Since $A, B \in \mathcal{I}'$, $A', B' \in \mathcal{I}$. Since $e \notin A, e \notin B$, $|A'| < |B'|$. Let $x \in B' - A'$ such that $A' \cup \{x\} \in \mathcal{I}$. Since $B' - A' = B - A$, $x \in B - A$. For such x, we just showed that $A \cup \{e\} \cup \{x\} \in \mathcal{I}$. Also, $x \neq e$ since $e \in A'$. Therefore, $A \cup \{x\} \in \mathcal{I}'$. Hence, we have found $x \in B - A$ such that $A \cup \{x\} \in \mathcal{I}'$. Since this follows three properties given in the definition, this is indeed a matroid. Therefore, contraction by an element indeed generates a matroid. □

Now that we have defined contraction of a matroid by an element, we can define contraction by a subset of a ground set.

Definition 3.9. Let $M = (E, \mathcal{I}), X = \{x_1, \cdots, x_k\} \subseteq E$. M/X is defined to be $(((M/x_1)/x_2)\cdots)/x_k)$.

It is not obvious that this is well-defined. In other words, it is not obvious that the order of contraction does not matter. The following theorem shows that the order does not matter.

Theorem 3.10. *For any given matroid $M = (E, \mathcal{I})$, $(M/e)/f = (M/f)/e$ for any $e \neq f \in E$.*

Proof. There are a few cases.

(1) e, f are both loops.
$(M/e)/f = (M\backslash e)/f$ Since deletion of a loop does not change a family of independent sets, f is a loop in $(M\backslash e)$. Therefore, $(M/e)/f = (M\backslash e)\backslash f$. Again, deletion of f does not change a family of independent sets since f is a loop in (M/e). Therefore, we have $(M/e)/f = (E - \{e, f\}, \mathcal{I})$. By symmetry, $(M/e)/f = (M/f)/e$.

(2) One of e, f is a loop, and the other one is not.
Without loss of generality, assume e is a loop. $(M/e)/f = (M\backslash e)/f$. Since deletion of a loop does not change a family of independent set, a family of independent set of (M/e) is $\mathcal{I}$. Therefore, a family of independent sets of $(M/e)/f$ is $\mathcal{I}' = \{I \in \mathcal{I} \mid f \notin I, (I \cup \{f\}) \in \mathcal{I}\}$. On the other hand, it is easy to see that $\mathcal{I}'$ is identical to a family of independent sets of (M/f). Since contraction by an element does not add new elements to a family of independent sets, e is a loop in (M/f). Since deletion by a loop does not change a family of independent sets, a family of independent sets of $(M/f)/e$ is $\mathcal{I}'$. Now we confirmed that $(M/e)/f$ and $(M/f)/e$ have the same family of independent sets. Therefore, $(M/e)/f = (M/f)/e$.

(3) Neither of them is a loop, and $\{e, f\} \in \mathcal{I}$.
A family of independent set of M/e is $\mathcal{I}' = \{I \in \mathcal{I} \mid e \notin I, (I \cup \{e\}) \in \mathcal{I}\}$. Since $\{e, f\} \in \mathcal{I}$, $\{f\} \in \mathcal{I}'$. Therefore, f is not a loop in M/e. Hence, a family of independent sets of $(M/e)/f$ is $\mathcal{I}'' = \{I \in \mathcal{I}' \mid f \notin I, (I \cup \{f\}) \in \mathcal{I}'\}$. $\mathcal{I}''$ is actually equivalent to $S = \{I \in \mathcal{I} \mid e \notin I, f \notin I, (I \cup \{e, f\}) \in \mathcal{I}\}$. We can prove $\mathcal{I}'' = S$ by starting to show that $\mathcal{I}'' \subseteq S$. Let $I \in \mathcal{I}''$. Since I is an independent set of $(M/e)/f$, we know that $e, f \notin I$. Since $(I \cup \{f\}) \in \mathcal{I}'$, we also know that $((I \cup \{f\}) \cup \{e\}) \in \mathcal{I}$. Therefore, $(I \cup \{e, f\}) \in \mathcal{I}$. Thus $I \in S$, and $\mathcal{I}'' \subseteq S$. Now, we want to show that $S \subseteq \mathcal{I}''$. Let $I \in S$. By the definition of S, we know that $e, f \notin I$. Since $(I \cup \{e, f\}) \in \mathcal{I}$, we know that $(I \cup \{e\}) \in \mathcal{I}$. Since $((I \cup \{f\}) \cup \{e\}) \in \mathcal{I}$ and $e \notin (I \cup \{f\})$, we know that $(I \cup \{f\}) \in \mathcal{I}'$. Since $f \notin I$ and $(I \cup \{f\}) \in \mathcal{I}'$, $I \in \mathcal{I}''$. Hence, $S \subseteq \mathcal{I}''$.

Combining these two results, we know that $S = \mathcal{I}''$. By the symmetry, $(M/e)/f$ and $(M/f)/e$ have the same family of independent sets. Therefore $(M/e)/f = (M/f)/e$.

(4) Neither of e, f is a loop, but $\{e, f\} \notin \mathcal{I}$.
A family of independent set of M/e is $\mathcal{I}' = \{I \in \mathcal{I} \mid e \notin I, (I \cup \{e\}) \in \mathcal{I}\}$. Since $\{e, f\} \notin \mathcal{I}$, f is a loop in M/e. Therefore, $(M/e)/f = (M/e)\backslash f$. Since the deletion of a loop does not change a family of independent sets, a family of independent sets of $(M/e)/f$ is $\mathcal{I}'$. By applying the same argument, a family of independent set of $(M/f)/e$ is $\mathcal{I}'' = \{I \in \mathcal{I} \mid f \notin I, (I \cup \{f\}) \in \mathcal{I}\}$. We want to show that $\mathcal{I}' = \mathcal{I}''$. By the symmetry, it suffices to show that $\mathcal{I}' \subseteq \mathcal{I}''$. Let $I \in \mathcal{I}'$. Since $\{e, f\}$ is dependent, $f \notin I$. (Otherwise, $I \cup \{e\}$ would be dependent.) Since both $(I \cup \{e\})$ and $\{f\}$ are independent, we

can grow $\{f\}$ by adding elements from $(I \cup \{e\})$ until they have the same size. Since $\{e, f\}$ is dependent, we never add e. In other words, we add every element from $\mathcal{I}$. It means that $I \cup \{f\}$ is independent. Therefore, $I \in \mathcal{I}''$, and thus $\mathcal{I}' \subseteq \mathcal{I}''$. By symmetry, $\mathcal{I}'' \subseteq \mathcal{I}'$. Therefore, $\mathcal{I}' = \mathcal{I}''$.

Therefore, in any case, $(M/e)/f = (M/f)/e$. □

Here is a simple result about contraction.

Theorem 3.11. *Let a matroid $M = (E, \mathcal{I}), X \subseteq E$ be given. Let A be an independent set in M/X. Then A is independent in M.*

Proof. A family of independent sets of M/X is clearly a subset of $\mathcal{I}$ from the definition of contraction. Since A is in the subset of $\mathcal{I}$, A must be in $\mathcal{I}$. □

In other words, this means that contraction never "adds" a new element to a family of independent sets just like deletion.

Now that we have defined contraction and deletion, we can define a *minor* of a matroid.

Definition 3.12. A minor of a matroid is a matroid that can be obtained by a sequence of contraction and deletion operations. (possibly no operation)

Therefore, most matroids have more than one minor. To define the matroid minor more concisely, we will prove the following theorem.

Theorem 3.13. *Let a matroid $M = (E, \mathcal{I})$ and $e \neq f \in E$ be given. Then $(M/e)\backslash f = (M\backslash f)/e$.*

Proof. There are a few cases.

(1) Both e and f are loops. This case is easy to prove since neither contraction nor deletion add any new elements to a family of independent sets. In other words, f is a loop in (M/e) and e is a loop in $(M\backslash f)$. $(M/e)\backslash f = (M\backslash e)\backslash f = (M\backslash f)\backslash e = (M\backslash f)/e$

(2) e is a loop, but f is not a loop. $(M/e)\backslash f = (M\backslash e)\backslash f$ since e is a loop. $(M\backslash f)/e = (M\backslash f)\backslash e$ since e is a loop in $(M\backslash f)$. We know that the order of deletion does not matter, so they are equivalent.

(3) e is not a loop, but f is a loop. Since the deletion of f does not change a family of independent sets, both M and $(M\backslash f)$ have the same family of independent sets, although their ground sets are not identical. Therefore, (M/e) and $(M\backslash f)/e$ have the same family of independent sets from the definition of contraction. Since we know that contraction does not add a new independent set, f is a loop in (M/e). Therefore, deletion of f does not change the family of independent sets. Hence, we know that $(M/e)\backslash f$ and $(M\backslash f)/e$ have the same ground set and the same family of independent sets, so they are identical.

(4) Neither e nor f is a loop. Let $X \subseteq E - \{e, f\}$. X is independent in $(M/e)\backslash f$ if and only if X is independent in (M/e). X is independent in (M/e) if and only if $(X \cup \{e\})$ is independent in M. On the other hand, X is independent in $(M\backslash f)/e$ if and only if $X \cup \{e\}$ is independent in $(M\backslash f)$. $X \cup \{e\}$ is independent in $(M\backslash f)$ if and only if $X \cup \{e\}$ is independent in M. Therefore, X is independent in $(M/e)\backslash f$ if and only if X is independent in $(M\backslash f)/e$. Since $(M/e)\backslash f$ and $(M\backslash f)/e$ have the same ground set and the same family of independent sets, they are identical.

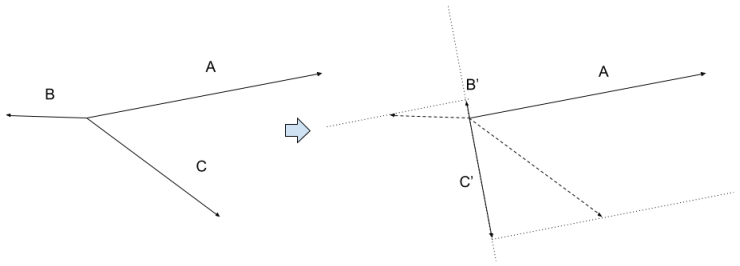

FIGURE 2. Contraction by a vector A

Therefore, in every case, $(M/e)\backslash f$ is identical to $(M\backslash f)/e$. □

By this theorem, we know that any series of operations can be expressed as $(M/A)\backslash B$ where A, B are disjoint subsets of E. Therefore, the following definition is equivalent to the previous definition.

Definition 3.14. Let $M = (E, \mathcal{I})$ be given. Let A, B be disjoint subsets of E. Then a matroid $(M/A)\backslash B$ is called a minor of M.

Moreover, if $A \cup B \neq \emptyset$, we call $(M/A)\backslash B$ a *proper minor*.
Of course, we could have defined a minor as $(M\backslash A)/B$ instead of $(M/A)\backslash B$.

3.1. **What do contraction and deletion mean in graphs and vector spaces?** Deletion of a vector in the vector space is simply removing such a vector from the set. Contraction, however, is more complicated. In vector spaces, contraction can be considered as projection to its orthogonal vector as showin in the figure 2. In graphs, deletion of an edge simply removes an edge. Contraction of an edge combines the two nodes that the edge connects as shown in the figure 3.

3.2. **Why do these matter?** The discussion of contraction and deletion is very important when discussing the representability of matroids since if a matroid is representable over some field $\mathbb{F}$, its minor is always representable over $\mathbb{F}$.

Theorem 3.15. *Let a matroid $M = (E, \mathcal{I})$ such that it is representable over $\mathbb{F}$. Any minor of M is representable over $\mathbb{F}$.*

Proof. It suffices to show that M/e and $M\backslash e$ are both representable over $\mathbb{F}$ for any $e \in E$. Let r be a rank of M, $n = |E|$. Let $e \in E$ be given. Let $A = \begin{pmatrix} u_1 u_2 \cdots u_n \end{pmatrix} \in \mathbb{F}^{r \times n}$ be a matrix such that the column matroid of M is isomorphic to A. Without loss of generality, we can assume $E = \{1, 2, \cdots, n\}$ and $e = n$.

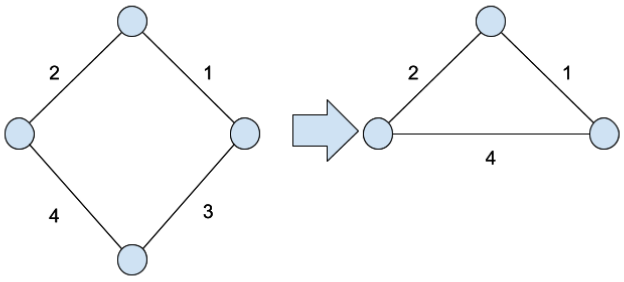

FIGURE 3. Contraction by an edge 3

(1) First, we prove the case of deletion. We claim that $M\backslash e$ is isomorphic to the column matroid of $\begin{pmatrix} u_1 u_2 \cdots u_{n-1} \end{pmatrix}$. We prove so by comparing the independent sets of each matroid. By definition, $M\backslash e = (E - \{e\}, \{I \in \mathcal{I} \mid e \notin I\})$. Let $U = \{u_{i_1}, u_{i_2}, \cdots, u_{i_k}\}$ be a subset of $\{u_1, u_2, \cdots, u_{n-1}\}$. We want to show that U is linearly independent if and only if $\{i_1, i_2, \cdots i_k\}$ is linearly independent in $M\backslash e$. Suppose U is linearly independent. Then $\{i_1, i_2, \cdots i_k\}$ is independent in the column matroid of A. Since $\{i_1, i_2, \cdots i_k\}$ is in $\mathcal{I}$ and does not contain $e = n$, it is independent in $M\backslash e$ as well. Suppose U is linearly dependent. Then $\{i_1, i_2, \cdots i_k\}$ is dependent in the column matroid of A. Since $\{i_1, i_2, \cdots i_k\}$ is not in $\mathcal{I}$ it is dependent in $M\backslash e$ as well. Therefore, $M\backslash e$ is representable over $\mathbb{F}$.

(2) Next, we prove the case of contraction. First, assume e is a loop. Then the corresponding column of A must be a zero vector. It is easy to see that the removal of the corresponding column will yield a matrix whose column vector is isomorphic to $M/e = M\backslash e$. Now, assume that e is not a loop. Then the corresponding column of A must not be a zero vector. We prove the proposition by comparing the independent sets of each matroid. By definition, $M/e = (E - \{e\}, \{I \in \mathcal{I} \mid e \notin I, (e \cup I) \in \mathcal{I}\})$. We claim that M/e is isomorphic to the column matroid of $B \in \mathbb{F}^{r \times n-1}$, where ith column of B, b_i, is $u_i - \dfrac{u_i \cdot u_n}{u_n \cdot u_n} u_n$. (This makes sense since we are assuming that u_n is not a zero vector.) Let $X = \{i_1, i_2, \cdots, i_k\} \subseteq E - \{n\}$ be given.
X is independent in M/e
$\iff$ $X \cup \{n\}$ is independent in M
$\iff$ $\{i_1, i_2, \cdots, i_k, n\}$ is independent in M
$\iff$ $\{u_{i_1}, u_{i_2}, \cdots, u_{i_k}, u_n\}$ is linearly independent
We are going to take a close look at this set of vectors. Let $c_1, c_2, \cdots, c_k, c \in \mathbb{F}$ be given such that $c_1 u_{i_1} + \cdots + c_k u_{i_k} + c u_n = 0$.

$$\begin{aligned}
c_1 b_{i_1} + \cdots + c_k b_{i_k} &= \sum_{j=1,\cdots,k} c_j b_{i_j} \\
&= c_1 u_{i_1} + c_2 u_{i_2} + \cdots + c_k u_{i_k} - \sum_{j=1,\cdots,k} c_j \frac{u_i \cdot u_n}{u_n \cdot u_n} u_n \\
&= -cu_n - \sum_{j=1,\cdots,k} c_j \frac{u_i \cdot u_n}{u_n \cdot u_n} u_n \\
&= -\Big(c + \sum_{j=1,\cdots,k} c_j \frac{u_i \cdot u_n}{u_n \cdot u_n}\Big) u_n \\
&= -\frac{\Big(cu_n \cdot u_n + \sum_{j=1,\cdots,k} c_j (u_i \cdot u_n)\Big)}{u_n \cdot u_n} u_n \\
&= -\frac{(c_1 u_1 + c_2 u_2 + \cdots + c_k u_k + cu_n) \cdot u_n}{u_n \cdot u_n} u_n \\
&= 0.
\end{aligned}$$

Therefore, $\{u_{i_1}, u_{i_2}, \cdots, u_{i_k}, u_n\}$ is linearly independent
$\iff$ $\{b_{i_1}, b_{i_2}, \cdots, b_{i_k}\}$ is linearly independent
$\iff$ $\{i_1, i_2, \cdots, i_k\}$ is independent in the column matroid of B.
Therefore, the column matroid of B is isomorphic to M/e.

Hence, we have proved that any minor of M is always representable. □

However, neither the converse nor the inverse of this theorem is always true. Any matroid has a representable minor since $U_{0,k}$ is a minor of any matroid. Also, $U_{2,4}$ is not a binary matroid, but any minor of it only contains at most 3 elements, so we know that any minor of $U_{2,4}$ is regular by the theorem. Rota's conjecture is about unrepresentable matroids any of whose minor is representable. It will be discussed in the next chapter.

4. The introduction to Rota's Conjecture

This chapter introduces Rota's Conjecture and an outline of the proof.

Conjecture 4.1 (Rota's Conjecture)**.** *For each finite field $\mathbb{F}$, there are, up to isomorphism, only finitely many excluded minors for the class of $\mathbb{F}$-representable matroids.*

In other words, given a finite field $\mathbb{F}$, let F be a family of all matroids that are representable over $\mathbb{F}$. By the theorem from the previous chapter, we know that F is minor-closed, i.e., any minor of any element in F is in F. Then, an excluded minor is a matroid $M \notin F$ such that any minor of M is in F. The conjecture states that for any finite field $\mathbb{F}$, there are only finitely many excluded minors.

First, we will introduce some results related to excluded minors.

Theorem 4.2. *The Fano matroid is an excluded minor for the class of $\mathbb{F}$-representable matroids if the characteristic of $\mathbb{F}$ is not 2.*

Proof. Let M be the Fano matroid. We know from the previous chapter that M is not representable in a field if the characteristic of the field is not 2. Therefore, it suffices to show that any minor of M is representable in those fields. Since any minor

of a representable matroid is always representable, it suffices to show that M/e and $M\backslash e$ are representable for any e in those fields. It is obvious that $M/1$, $M/2$ and $M/3$ are isomorphic to each other by the symmetry of the Fano plane. For the same reason, each matroid in each of the following sets is isomorphic to other matroids in the same set. $\{M\backslash 1, M\backslash 2, M\backslash 3\}, \{M/4, M/5, M/6\}, \{M\backslash 4, M\backslash 5, M\backslash 6\}$. If we swap 1 with 4, 3 with 5, the Fano place still gives the identical matroid. That implies that deletion or contraction of any of 1, 2, 3, 4, 5, 6 always gives isomorphic matroids. Similarly, if we swap 6 with 7, 3 with 5, the Fano place still gives the identical matroid. That implies that deletion or contraction of any element always gives isomorphic matroids. Now that we have shown the symmetry, it suffices to show that $M/7$ and $M\backslash 7$ are both representable in those fields. $M\backslash 7$ is isomorphic to the column matroid of the following matrix: $\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & -1 \end{pmatrix}$, where -1 is the additive inverse of 1. Similarly, $M/7$ is isomorphic to the column matroid of the following matrix: $\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$. □

Rota's conjecture has been proved for some finite fields. For example, $U_{2,4}$ is the only excluded minor of $GF(2)$, and the proof can be found in [8]. In $GF(3)$, there are 4 excluded minors, which are $F_7, F_7^*, U_{2,5}, U_{3,5}$.[8] In $GF(4)$, there are 7 excluded minors, which are $U_{2,6}, U_{4,6}, P_6, F_7^-, (F_7^-)^*, P_8, P_8''$.[6]

Here is a sketch of proof that $U_{2,4}$ is the only excluded minor of $GF(2)$. The complete proof can be found in [8].

First, we will assume the following lemmas. Proofs of them can be found in [8].

Lemma 4.3. *Let B be a basis of a matroid $M = (S, \mathcal{I})$, and $e \notin B$. Then $B \cup \{e\}$ contains a unique circuit.*

Lemma 4.4. *Let M, N be distinct matroids on the same ground set S. Suppose that there exists $B \subseteq S$ such that*

- *B is a basis of M and N.*
- *There is no X such that $|B \Delta X| = 2$ and X is a basis of exactly one of M and N.*

Then M or N has a $U_{2,4}$ minor.

Theorem 4.5 (Tutte's Theorem)**.** *$U_{2,4}$ is the only excluded minor of $GF(2)$. In other words, a matroid M is representable over $GF(2)$ if and only if $U_{2,4}$ is not M's minor.*

Proof. By theorem 2.4, we know that $U_{2,4}$ is not representable over $GF(2)$. Since any proper minor of $U_{2,4}$ contains at most 3 elements, by theorem 2.9, we know that any proper minor of $U_{2,4}$ is representable over $GF(2)$. Therefore, it suffices to prove that any matroid M that is not representable over $GF(2)$ has a $U_{2,4}$ minor. Let M be such a matroid on a ground set S. We will find a representable matroid N and prove that one of N and M has to have a $U_{2,4}$ minor. First, without loss of generality, assume that $S = \{1, 2, 3, \cdots, n\}$ for some positive integer n. Let B be a basis of M. Without loss of generality, $B = \{1, 2, 3, \cdots, k\}$. Let v_i be a column vector for each $i = 1, 2, \cdots k$ with k elements such that ith element is 1 and other elements are 0. For each $j = k+1, k+2, \cdots n$, let C be the unique circuit in $B \cup \{j\}$.

(The existence is guaranteed by the lemma above). Let $v_j = \sum_{i \in C-s} v_i$. Now, we have defined v_i for $i = 1, \cdots, n$. Let N be a column matroid of $\begin{pmatrix} v_1 v_2 \cdots v_n \end{pmatrix}$. Obviously B is a basis of N from the way we defined N. Now, we want to prove this property: For each $b \in B, s \in S \setminus B, B - b + s$ is a basis of M if and only if it is a base of N. First, from the lemma above, we know that $B \cup \{s\}$ has a unique circuit in N. The same goes for M. Moreover, they must be the same circuit from the way we defined v_i's.

If $B - b + s$ is dependent in M, it contains a circuit C of M. Since C must be included in $B + s$, we know that C is the unique circuit of $B + s$ in M. Since C is also a circuit in N, $B - b + s$ is dependent in N.

On the other hand, suppose that $B - b + s$ is dependent in N. Let C be a circuit of N in $B - b + s$. Since C must be in $B + s$, we know that C is the unique circuit of $B + s$ in N. Since C is also a circuit in M, $B - b + s$ is dependent in M.

Since $B - b + s$ is independent in N if and only if it is independent in M, we have proved the property.

Now, let X such that $|B \Delta X| = 2$. It means that there exists $b \in B, s \in S \setminus B$ such that $X = B - b + s$. Therefore, X is a basis of M if and only if it is a basis of N. In other words, X is a basis of both M and N or neither of them. Therefore, there is no X such that $|B \Delta X| = 2$ and X is a basis of exactly one of M and N. By lemma, we know that M or N has a $U_{2,4}$ minor. Clearly, it must be M that has $U_{2,4}$ minor. □

However, finding a finite set of excluded minors for some finite case does not solve Rota's conjecture as it is more general. In 2013, Geelen, Gerards and Whittle announced that they have solved Rota's Conjecture. As they mention in [7] that "there is a significant difference between the concrete problem of finding the full set of obstructions for some particular field and the abstract problem of showing that there are finitely many obstructions for an arbitrary finite field", the approach they took was unique in a way that they started out by extending theorems from another field of mathematics to matroids. Here is a brief summary of their proof.

As matroid theory is, in a way, an abstraction of graph theory, they have used several theorems from graph theory. For example, they extended the graph minor theorem to matroids. Note that the minor of a graph can be obtained by deleting edges and vertices and by contracting edges.

Theorem 4.6 (Graph Minor Theorem)**.** *Let F be a minor-closed family of graphs, that is, $\forall G \in F$, any minor of G is in F. Then there are only finitely many graphs H such that $H \notin F$ and any minor of H is in F. In other words, each minor-closed class of graphs has only finitely many excluded minors.*

One special case of this theorem is a set of planar graphs. Any minor of a planar graph is also planar. Therefore, a set S of planar graphs is minor-closed. Kuratowski's theorem indeed states that there are only two excluded minors, $K_{3,3}, K_5$.

Here is the extension of the graph minor theorem to matroids.

Theorem 4.7 (Matroid WQO Theorem)**.** *Let a finite field $\mathbb{F}$ be given and F be a minor-closed family of $\mathbb{F}$-representable matroids. Then there are only finitely many $\mathbb{F}$-representable matroids M such that $M \notin F$ and any minor of M is in F. In other words, for each finite field $\mathbb{F}$ and each minor-closed class of $\mathbb{F}$-representable matroids, there are only finitely many $\mathbb{F}$-representable excluded minors.*

This theorem is theorem 6 from [7].

More precisely, this is an extension from graphs to $\mathbb{F}$-representable matroids.

Although the Matroid WQO Theorem and the graph minor theorem both discuss excluded minors, the Matroid WQO Theorem does not imply Rota's Conjecture. Rota's Conjecture is about a family of representable matroids, so all the excluded minors are non-representable. In other words, obviously, there are never any $\mathbb{F}$-representable excluded minors.

Another important concept is connectivity.

Definition 4.8. A k-separation in a matroid $M = (E, \mathcal{I})$ is a partition (X, Y) of E such that $r_M(X) + r_M(Y) - r_M(E) < k$ and $|X|, |Y| \geq k$.

Definition 4.9. A matroid is k-connected if it has no l-separation for any $l < k$.

Lemma 4.10. *For each field $\mathbb{F}$, each excluded minor for the class of $\mathbb{F}$-representable matroids is 3-connected.*

There are a few basic results about this.

Theorem 4.11. *No matroid has 0-separation.*

Proof. Let I be a maximal independent set. Then $|I| = r_M(E)$. Let $I_X = I \cap X, I_Y = I \cap Y$. Then $|I_X| \leq r_M(X), |I_Y| \leq r_M(Y)$. Therefore, $r_M(X) + r_M(Y) - r_M(E) \geq 0$ □

Theorem 4.12. *$U_{2,4}$ is indeed 3-connected.*

$U_{2,4}$ is an excluded minor for $GF(2)$ as mentioned above, so this theorem should be true.

Proof. Let a partition of E, (X, Y), be given. Without loss of generality, $|X| \leq |Y|$. Consider the case when $|X| = 1$. Then we know that $r_M(X) = 1, r_M(Y) = 2$. Consider the case when $|X| = 2$. Then we know that $r_M(X) = 2, r_M(Y) = 2$. Since $r_M(X) + r_M(Y) - r_M(E) \geq 1$ for any (X, Y), a 1-partition does not exist. Since $r_M(X) + r_M(Y) - r_M(E) < 2$ only if $r_M(X) = 1$, a 2-partition does not exist either. Therefore, $U_{2,4}$ is indeed 3-connected. □

The connectivity is important because it turns out that excluded minors are very highly connected, and that is one of the important parts of the rest of the proof, which can be found in [7].

References

[1] Charles E. Leiserson, Thomas H. Cormen, Clifford Stein, Ronald Rivest. *Introduction to Algorithms*, MIT Press, 1990

[2] David L. Neel, Nancy Ann Neudauer. *Matroids You Have Known*
http://www.maa.org/sites/default/files/pdf/shortcourse/2011/matroidsknown.pdf

[3] Geoff Whittle. *Rota's Conjecture*
http://www.asiapacific-mathnews.com/04/0401/0011_0012.pdf

[4] James Oxley. *WHAT IS A MATROID?*
https://www.math.lsu.edu/~oxley/survey4.pdf

[5] Jayant Apte. *Solving Rota's Conjecture**
http://www.ece.drexel.edu/walsh/Jayant_RotaConjecture1.pdf

[6] Jim Geelen. *The Excluded Minors for GF(4)-Representable Matroids*
https://www.math.uwaterloo.ca/~jfgeelen/Publications/gf4.pdf

[7] Jim Geelen, Bert Gerards, Geoff Whittle. *Solving Rota's Conjecture*
http://www.ams.org/notices/201407/rnoti-p736.pdf

[8] Michel X. Goemans, *Lecture 9 from Advanced Combinatorial Optimization*
`http://math.mit.edu/~goemans/18438F09/lec9.pdf`
[9] Petr Hliněný. *On Matroid Representability and Minor Problems*
`http://www.fi.muni.cz/~hlineny/papers/mrepres-mfcs.pdf`