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 linearly 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 linearly 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 and investigate in them.

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 the 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 discussions. 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 $\{1, 2, \cdots m\}$. A subset of E is independent in M if and only if the set of column vectors corresponding to it is linearly independent.

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

Proof. Prove it! □

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

Date: March 10, 2016.

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 matroid, any maximal independent subset of column vectors always has the same size.

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

Definition 1.7. The rank of a column matroid is equal to the rank of the matrix.

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 linearly 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.

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

Theorem 2.2. *$U_{2,4}$ is not representable over $GF(2)$.*

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

Proof. prove it □

Now, we will introduce Fano matroid. Fano matroid can be constructed from Fano plane. 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 Fano matroid mathematically.

Definition 2.3. Fano matroid. A set of vertices is independent if it has at most three points and is not a line.

Theorem 2.4. *Fano matroid is indeed a matroid*

Proof. Prove it! □

Here is an interesting property of Fano matroid

Theorem 2.5. *If Fano matroid is representable over a field F, $1 + 1 = 0$ in that field.*

Proof. meh □

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

Corollary 2.6. *Fano matroid is not representable over $\mathbb{R}$.*

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

Theorem 2.7. *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. I'll use rank here. □

3. More discussion on matroid representability

This chapter will introduce a new concept, a matroid minor, which is crucial when discussing the matroid representability. Rota's conjecture will be also introduced at the end of the chapter. (I am thinking of adding a sketch of the proof by the end of the semester if I can understand the outline)

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

Definition 3.1. Let $M = (E, \mathcal{I})$, $X \subseteq E$ be given. $M \backslash X$ denotes a deletion of X in M and is defined to be $(E - X, \{I \in \mathcal{I} \mid X \cap I = \emptyset\})$

Note that $M \backslash e$ for some element $e \in E$ is equivalent to $M \backslash \{e\}$.

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

Proof. Let $M' = (E', \mathcal{I}') = M \backslash X$. Since $\emptyset \in \mathcal{I}$ and $X \cap \emptyset = \emptyset$, $\emptyset \in \mathcal{I}$. Let $I \in \mathcal{I}', J \subseteq I$. Since $I \in \mathcal{I}$, $J \in \mathcal{I}$. Since $J \subseteq I$ and $I \cap X = \emptyset$, $J \cap X = \emptyset$. Therefore, $J \in \mathcal{I}'$. Let $A, B \in \mathcal{I}'$ such that $|A| < |B|$. Since $A, B \in \mathcal{I}'$, we know that $A, B \in \mathcal{I}$. Therefore, we can find $x \in B - A$ such that $(A \cup \{x\}) \in \mathcal{I}$. Since $(A \cup \{x\}) \subseteq (A \cup B)$ and $X \cap A = X \cap B = \emptyset$, $X \cap (A \cup \{x\}) = \emptyset$. Therefore, $A \cup \{x\} \in \mathcal{I}'$. Thus we have found such $x \in B - A$ that $A \cup \{x\} \in \mathcal{I}'$. Since $M' = M \backslash X$ follows the three properties, it is indeed a matroid. □

Definition 3.3. 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 3.4. *Contraction by an element indeed generates a matroid.*

Proof. If e is a loop, M/e is obviously a matrod since we know that deletion always generates a matroid. Suppose otherwise. Let $\mathcal{I}'$ denote the 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. □

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. The 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 $\mathcal{I}$. $\square$

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

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

Proof. Let $M = (E, \mathcal{I}), e \in E, \{e\} \notin \mathcal{I}$. The 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, the independent sets of $M \backslash e$ is identical to $\mathcal{I}$. $\square$

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

Definition 3.7. 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 3.8. *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 the 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 the 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 the independent set, the independent set of (M/e) is $\mathcal{I}$. Therefore, the independent set 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 the independent sets of (M/f). Since contraction by an element does not add new elements to the independent sets, e is a loop in (M/f). Since deletion by a loop does not change the independent sets, the independent sets of $(M/f)/e$ is $\mathcal{I}'$. Now we confirmed that $(M/e)/f$ and $(M/f)/e$ have the same independent sets. Therefore, $(M/e)/f = (M/f)/e$.

(3) Neither of them is a loop, and $\{e, f\} \in \mathcal{I}$.
The 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, the 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 independent sets. Therefore $(M/e)/f = (M/f)/e$.

(4) Neither of e, f is a loop, but $\{e, f\} \notin \mathcal{I}$.
The 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 the independent sets, the independent sets of $(M/e)/f$ is $\mathcal{I}'$. By applying the same argument, the 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, $(M/e)/f = (M/f)/e$. □

List of topics I could discuss further:

- More properties about contraction deletion
  - $(M/e)\backslash f = (M\backslash f)/e$?
  - Therefore, any minor can be represented as $(M\backslash A)/B$

3.1. What do contraction and deletion mean in graphs and vector spaces?

3.2. Why do these matter?
Because if a matroid is representable over some field $\mathbb{F}$, its minor is always representable over $\mathbb{F}$.

Theorem 3.9. *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. prove! □

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.

3.3. The introduction of Rota's conjecture.

Theorem 3.10. *For any finite field $\mathbb{F}$, there are only finitely many unrepresentable matroids all of whose minors are representable. In other words, there are only finitely many excluded minor.*

References

[1] "WHAT IS A MATROID?" Oxley
[2] "On Matroid Representability and Minor Problems" Hlineny
[3] "Solving Rotas Conjecture" Geelen, Gerards, Whittle
[4] "Advanced Graph Theory, lecture 1" Rudi Pendavingh
[5] "Matroids You Have Known" Neel, Neudauer