6-2016

A Dual Fano, and Dual Non-Fano Matroidal Network

Stephen Lee Johnson
California State University - San Bernardino

A Dual Fano, and Dual Non-Fano Matroidal Network

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

---

by

Stephen Lee Johnson

June 2016

A Dual Fano, and Dual Non-Fano Matroidal Network

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Stephen Lee Johnson

June 2016

Approved by:

Dr. Chris Freiling, Committee Chair	Date
Dr. Wenxiang Wang, Committee Member	
Dr. Jeremy Aikin, Committee Member	
Dr. Charles Stanton, Chair, Department of Mathematics	Dr. Corey Dunn Graduate Coordinator, Department of Mathematics

Abstract

Matroidal networks are useful tools in furthering research in network coding. They have been used to show the limitations of linear coding solutions. In this paper we examine the basic information on network coding and matroid theory. We then go over the method of creating matroidal networks. Finally we construct matroidal networks from the dual of the fano matroid and the dual of the non-fano matroid, and breifly discuss some coding solutions.

Acknowledgements

To Dr. Freiling for all his hard work, and to my parents for their support.

Table of Contents

List of Figures

Chapter 1

Introduction

Network coding is a relatively new field that started in 2000 with a paper by Ahlswede, et. al., [ACLY00]. The general idea of network coding is that every node in a network determines what data to send based on the data that is received. Most current networks use routing to send information from selected in-edges to selected out-edges. In [ACLY00], network coding was shown to be more efficient than the standard network routing method. The field has grown considerably since its beginnings.

Network coding has an ingrained sense of dependence. The way in which the data flows in a network requires that data is generated from some source node and then sent through in-edges to other nodes. These intermediate nodes then send the information to other intermediate nodes, and eventually the information is received by the receiver nodes. The messages can be considered independent and the output from any of the intermediate nodes depends on the nodes inputs.

Matroid theory is another field that is based on the idea of independence. A matroid is defined by a ground set, but also by its set of independent sets.

Dependence is the common trait between network coding and matroid theory and a method has been created to allow a network to take advantage of this idea. Using the circuits (minimal dependent sets) of a matroid, a network can be created. This type of network is called a matroidal network.

In the literature there have been several matroids that have been turned into specific networks. Two of the most famous matroidal networks are the fano network, and the non-fano network, see [DFZ07]. Several useful results have been proven about these

two networks, and they have been used to show limitations in the field of network coding. In matroid theory there is an idea of matroid duality. A matroid and its dual can, in simple terms, be viewed as being complements of each other.

In this paper we will discuss the basic ideas of network coding and matroid theory. We will look in further detail at matroid duals and matroid representation. From there we will go over the process of creating matroidal networks. Finally we will create non-unique matroidal networks from the duals of the fano and non-fano matroids.

Chapter 2

Networks and Matroids Defined

2.1 Networks

The concept of a network that will be used in this paper is defined in several places in the literature, but our development will parallel that found in "Networks, Matroids, and Non-Shannon Information Inequalities" by Dougherty, Freiling, and Zeger [DFZ07]. The reader is encouraged to read this paper in order to get a better understanding of what this idea of a network is, but in this paper we will only briefly go over the important definitions to get a general idea of the type of network we will be working with. All definitions in this section are found in [DFZ07].

Definition 2.1 (Network)**.** A network is a finite, directed, acyclic multi-graph with node set ν and edge set ϵ, together with a finite set μ called the message set, a source mapping

$$S : \nu \to 2^{\mu}$$

and a receiver mapping

$$R : \nu \to 2^{\mu}.$$

Definition 2.2 (Source)**.** Given a node x, if $S(x)$ is nonempty, then x is a source, and the elements of $S(x)$ are called the messages generated by x.

Definition 2.3 (Receiver)**.** Given a node x, if $R(x)$ is nonempty, then x is a receiver, and the elements of $R(x)$ are the messages demanded by x.

Definition 2.4 (Alphabet)**.** An alphabet is a finite set A with at least two elements.

Definition 2.5 (Message)**.** A message is a variable with domain A^k.

Definition 2.6 ($In(x)$ and $Out(x)$)**.** The union of the set of messages generated by x and the in-edges of x is $In(x)$, and the union of the set of messages demanded by x and the out-edges of x is $Out(x)$.

In general what we have is a multi-graph with several nodes. Some of these nodes generate certain messages, which are finite strings of elements from the alphabet, and some of these nodes want to receive certain messages. There are still other "intermediary" nodes that receive information and then pass the information on. The goal of the network is that the receiver nodes are able to obtain the messages they require from the information they receive on their in-edges. There are a couple of interesting types of networks. In a multicast network, there is only one source node, but every receiver node wants all of the source messages. In a multiple-unicast network, every source node sends a unique message, and each message is required by one specific receiver node.

Definition 2.7 ((k,n) code)**.** With $k, n \in \mathbb{Z}^+$, and where k is called the source dimension, and n is called the edge capacity, a (k,n) code assigns edge functions to the networks edges, and decoding functions to the network's receivers.

There are different types of solutions for networks, but in this paper we will focus on linear solutions. For a solution to be linear, we assume that the alphabet is composed of the elements of a finite ring. Then every message is a vector of length k. The edge functions transfer information in the form of vectors of length n. For the solution to be linear, the functions must only use vector addition and multiplication. Basically the (k, n) code tells the network how to send the messages from node to node, and it tells the nodes how to read the messages that are sent. When the (k, n) code satisfies the goal of the network, all the receiver nodes get the messages they want, the network is said to have a (k, n) solution. When a (k, n) solution exists, the network has an achievable linear coding rate of k/n. When the (k, n) solution is such that $k = n = 1$, then the network is called scalar linearly solvable. When the (k, n) solution happens to be $k = n$ the network is called vector linearly solvable.

The coding capacity of a network is the $sup(k/n)$ over all the (k, n) solutions for the network over an alphabet. When there exists a (k, n) solution so that k/n is equal to the capacity, then the capacity is achievable.

Finding achievable coding rates for a particular network is one of the major themes of network coding. It is rarely an easy task determining the exact coding capacity of a network; however, we can usually find bounds on the coding capacity. A useful tool in this process is to utilize information inequalities. Here, one assumes that the messages sent are independent, identically distributed uniform random variables. Then you are free to use information inequalities to try to find the largest possible k/n. There are many useful results in the literature. In [DFZ07] it is shown that Shannon inequalities are not sufficient in finding the best upper bounds. Still, finding these upper bounds is not an easy task.

This is the general overview of what we mean when we refer to a network in this thesis. Specifically, this paper will be concentrating on matroidal networks. So, what is a matroid?

2.2 Matroids

There are several different, but equivilant, definitions of Matroids. Here we will define matroids in terms of independence. Except where indicated otherwise, the definitions, lemmas, and theorems in this section come from James Oxley's book Matroid Theory [Oxl11].

Definition 2.8 (Matroid)**.** A matroid M is a finite set E, along with a set $\mathcal{I}$ of subsets of E, such that:

1. The empty set is in $\mathcal{I}$.
2. If X is in $\mathcal{I}$, then every subset of X is also in $\mathcal{I}$.
3. If X and Y are both in $\mathcal{I}$, and $|X|$ is larger than $|Y|$, then there is some element $x \in X - Y$ such that $Y \cup \{x\}$ is also in $\mathcal{I}$.

The finite set E is called the ground set, and the elements of the set $\mathcal{I}$ are all of the independent subsets of E. All of the subsets of E that are not in $\mathcal{I}$ are called dependent sets. Sometimes the ground set is denoted $E(M)$ and the independent sets $\mathcal{I}(M)$ to distinguish between different matroids.

Two of the main examples of matroids come from linear algebra, and graph theory. In linear algebra, we can take E to be a finite subset of a vector space over

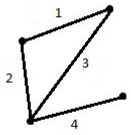

Figure 2.1: Graph G

some field. Then a matroid M can be defined on E with $\mathcal{I}$ being made up of the sets that are linearly independent in the vector space. These matroids are called "matric" or "representable" and can be represented with some matrix over a field. For example, given a matrix A with entries in $\mathbb{R}$, with

$$A = \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \hline 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{array}$$

We take the ground set to be the set of column vectors of the matrix, so $E_v = \{1, 2, 3, 4\}$, and the independent sets are $\mathcal{I}_v = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$. So, E and $\mathcal{I}$ together form a representable matroid, M_v. We will discuss representability in further detail later.

In graph theory, matroid M can be formed by taking the edge set, E, of a graph G, as the ground set. The elements of I can be defined to be the subsets of E that have no cycles. Looking at graph G in Figure 2.1, we can take the ground set to be the edge set, $E_g = \{1, 2, 3, 4\}$. We can take the independent sets to be $\mathcal{I}_g = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 4\}\{1, 3, 4\}, \{2, 3, 4\}\}$. Then E and I together are a matroid M_g. These types of matroids are called "graphic" matroids or "cycle" matroids.

Bases and circuits are closely related to the independent and dependent sets of a matroid M.

Definition 2.9 (Basis of a Matroid)**.** A basis, B, of a matroid is a maximal independent set in $\mathcal{I}$.

In our previous "matric" matroid, M_v, a basis would be $\{1, 2\}$, and in our

"graphic" matroid, M_g, a basis would be $\{1, 2, 4\}$.

Lemma 2.10. If B_1 and B_2 are bases of a matroid, M, then $|B_1| = |B_2|$.

Proof. Suppose that $|B_1| < |B_2|$. Both B_1 and B_2 are in I. By the third condition for M to be a matroid, there is an element $x \in B_2 - B_1$ such that $B_1 \cup x \in I$. Since B_1 is a bases of M, this is a contradiction to the fact that it is a maximal independent set. □

Now lets make a set whose elements are all of the bases of a matroid. Lets call that set $\mathcal{B}$.

Lemma 2.11. The set $\mathcal{B}$ of bases of a matroid M, has the following properties:

1. $\mathcal{B}$ is not empty.
2. If $B_1, B_2 \in \mathcal{B}$ and there is an $a \in B_1 - B_2$, then there is a $b \in B_2 - B_1$ so that $(B_1 - a) \cup b \in \mathcal{B}$.

Proof. Part 1 is obvious by condition (1) in Definition 2.8. To see part 2, B_1 and B_2 are in $\mathcal{B}$, and there is an $a \in B_1 - B_2$, so $B_1 \neq B_2$, and $B_1 - a \in I$. Then since $|B_1| = |B_2|$, $|B_1 - a| < |B_2|$. By (3) in Definition 2.8, there is a $b \in B_2 - (B_1 - a)$, (thus $b \neq a$), so that $(B_1 - a) \cup b \in I$, where $b \in B_2 - B_1$. Since $(B_1 - a) \cup b$ is in I, there is a bases, B_3 that contains $(B_1 - a) \cup b$. Now notice that $|B_3| = |(B_1 - a) \cup b|$, so $B_3 = (B_1 - a) \cup b$. By Lemma 2.10 $|B_3| = |B_1|$. □

Just as bases are the maximal independent sets in I. The minimal dependent sets of a matroid are also important.

Definition 2.12 (Circuit)**.** In a matroid, M, a minimal dependent set is a circuit, and the set of circuits will be called $\mathcal{C}$.

When we consider our two previous examples, a circuit in M_v would be the set $\{1, 2, 3\}$. Of course a circuit in M_g would be the set $\{1, 3, 2\}$. Circuits become more interesting when we look at matroid representability, but there are some important properties to look at.

Lemma 2.13. Let $\mathcal{C}$ be the set of cicuits for matroid M, then $\mathcal{C}$ has the following properties:

1. $\emptyset \notin \mathcal{C}$,
2. if $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$, and
3. if $C_1, C_2 \in \mathcal{C}$, where $C_1 \neq C_2$, and $x \in C_1 \cap C_2$, then there is a $C_3 \in \mathcal{C}$ such that $C_3 \subseteq (C_1 \cup C_2) - x$.

Proof. Properties (1) and (2) are clear. For Property (3), given $C_1, C_2 \in \mathcal{C}$ with $C_1 \neq C_2$. Suppose toward a contradiction that $(C_1 \cup C_2) - x$ does not contain a circuit, then $(C_1 \cup C_2) - x \in I$. Now, there is some $a \in C_2 - C_1$, by Property (2). By the definition of circuit, $C_2 - a \in I$. Next, take $S \subset C_1 \cup C_2$ so that S is a maximal independent set that contains $C_2 - a$. Then $a \notin S$ since C_2 is dependent. Then, since C_1 is in $\mathcal{C}$ there is a $b \in C_1$ where $b \notin S$. Then,

$$|S| \leq |(C_1 \cup C_2) - \{a, b\}| < |(C_1 \cup C_2) - x|.$$

But since $|S| < |(C_1 \cup C_2) - x|$, we see S is not maximal, so we have a contradiction. Thus $(C_1 \cup C_2) - x$ must have a circuit. □

The rank of a matroid is another useful tool.

Definition 2.14 (Rank a Subset of a Matroid)**.** Let $M = (E, \mathcal{I})$ be a matroid, and let $X \subseteq E$. The rank of X is $r(X)$ where $r(X) = max\{|I| : I \subseteq X \text{ and } I \in \mathcal{I}\}$

With this definition we can define the rank of a matroid to be the cardinality of its bases. Knowing the rank of a matroid allows us to talk about a third type of matroid, the uniform matroid. The uniform matroid has a ground set E with size n and a rank k, where $k \geq 0$ and $n \geq k$. The independent sets are the subsets X of E such that $|X| \leq k$. These matroids are noted as $U_{k,n}$. Some uniform matroids will be referred to later in the section on matroid representability.

If we look at our previous matroid examples, the matric matroid M_v, and the graphic matroid M_g, we can find the rank of these two matroids. First we will look at M_v. To find the rank of this matroid we need to check the cardinality of its bases. Since all the bases have the same cardinality it will suffice to look at one of them, and so we will look at $\{1, 2\}$. The cardinality of this basis is obviously 2, so $r(M_v) = 2$. Similarly, for the matroid M_g we can look at the the basis $\{1, 3, 4\}$ and from this we can see that $r(M_g) = 3$. We can also look at the ranks of individual subsets of the ground sets if we

would like. In M_v, if we take the subset $\{1, 2, 3\}$ of the ground set we can find, using the previously mentioned construction, that basis is $\{1, 2\}$ So the rank of this subset would be 2.

The rank function will be very helpful later when we discuss other properties of matroids. One thing the rank function allows us to do is to define spanning or closed sets called flats. From [GM12]:

Definition 2.15 (flats)**.** For ground set E of matroid M. $F \subseteq E$ is a flat if $r(F \cup \{x\}) > r(F)$ of every $x \in E - F$.

So, a flat is a rank maximal subset of the ground set. Adding any element to the subset will increase the rank of the subset. In M_v we can look at the subset $\{1, 4\}$. This subset is rank 1, but if we add any other element of the ground set, our only choices are 2, or 3, we increase the rank of the subset to 2.

A special type of flat is called a hyperplane. Also from [GM12]:

Definition 2.16 (Hyperplane)**.** For ground set E of matroid M. $H \subseteq E$ is a hyperplane of M if H is a flat, and if $r(H) = r(M) - 1$.

Looking at our graphic matroid M_g, which is rank 3, we can find a subset that is rank 2 and that is rank maximal. Take the subset $\{1, 2\}$ this is not a rank maximal subset because we can add element 3 to the subset and it does not increase the rank of the subset. If we look at the subset $\{1, 2, 3\}$ it is easy to check that this is a rank 2 subset, but adding Element 4 will be the entire matroid which we know is rank 3. Thus the subset $\{1, 2, 3\}$ is rank maximal and has rank 2, so it is a hyperplane.

Hyperplanes are a great tool to help construct matroid duals which we will now introduce.

Chapter 3

Matroid Duals

3.1 Duality in Matroids

Duality is one of the more developed properties of matroids and also one of the most important. We will be talking about matroid representability soon, and duals are extremely useful in helping with the task of trying to identifiy whether matroids are representable or not. In this section the primary source of information is Gordon and McNulty's, Matroids a Geometric Introduction [GM12].

Definition 3.1 (Dual of a Matroid)**.** Given a matroid, M, with ground set E. The dual of matroid, M, denoted M^* is a matroid on the same ground set such that

$$\mathcal{B}(M^*) = \{E - B : B \in \mathcal{B}(M)\}.$$

So, by declaring the complements of the bases of a matroid to be the bases of a new matroid we construct the dual matroid $M*$. A proof that M^* is a matroid can be found in [GM12].

Later in this paper we will be constructing some networks from matroids. The fano and non-fano matroids have been used to create matroidal networks in other works and several results have been proven for these specific matroids. One of the goals of this paper is to construct matroidal networks from the dual matroids of the fano and non-fano matroids, so here it will be useful to take a look at what these matroids look like. We can see a geometric representation of these two matroids in Figure 4.1. First we should look at some of the properties of matroid duals which will allow us to construct duals in an efficient manner.

The first property deals with the rank functions of a matroid and its dual. Since the rank of a matroid is the cardinality of its bases this property is obvious.

Lemma 3.2. Given a matroid, M, and its dual, M^*, on ground set E;

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

Next we have a list of properties, whose proofs will be omitted here, that will make it very easy to construct matroid duals.

Lemma 3.3 (Properties of Matroids and their Duals)**.** Given a matroid, M, and its dual, M^*, the following hold:

1. If B is a basis of M, then $E - B$ is a basis of M^*.
2. If I is independent in M, then $E - I$ is spanning in M^*.
3. If S is spanning in M, then $E - S$ is independent in M^*.
4. If C is a circuit in M, then $E - C$ is a hyperplane in in M^*.
5. If H is a hyperplane in M, then $E - H$ is a circuit in M^*.

In Section 5.1 it will become obvious that we need to identify the bases of the matroids we want to use as well as the circuits. These properties make finding the bases and circuits of dual matroids much less time consuming, though matroids with many elements can still be a very daunting task. There are many other result for matroid duals, but in this paper the previously mentioned results will suffice.

Example 3.1.1. As a starter example we will look at the dual matroid for one of our previous examples. Lets look at the matroid M_v. As a reminder, the ground set is $E_v = \{1, 2, 3, 4\}$, and the indepent sets are $I_v = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$. To construct M_v^* we need to look at the bases of M_v. These are all the rank 2 independent sets of I_v.

$$\mathcal{B}_v = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$$

From our definition the ground set of M_v^* is E_v. Then we can take the complements of the bases of M_v and we will have B_v^* which will the set of bases for M_v^*. I_v^* will be all of

the subsets of the bases. The complements of $\{1,2\},\{1,3\}$, and $\{2,3\}$ are $\{3,4\},\{2,4\}$, and $\{1,4\}$ respectively. Then;

$$\mathcal{B}_v^* = \{\{2,3\},\{3,4\},\{2,4\}\}$$

From here it is not difficult to construct a list of the independent sets for M_v^*. Recall that $r(M_v) = 2$, and note that $r(M_v^*) = 2$. This agrees with Lemma 3.2, $r(M_v)+r(M_v^*) = |E|$ and we can see that $2+2 = 4$ and $|E|$ does equal 4.

3.2 Dual Matroids, Some Examples

In the rest of this section we will do two more examples. We will use these examples to construct the duals of the fano matroid and the non-fano matroid. The information we will need later is the bases and the circuits, and so we will focus on getting those sets. We will discuss the fano and non-fano matroids in further detail in the next section.

Example 3.2.1 (The Fano Matroid and its Dual, F_7^*)**.** The fano matroid, denoted as F_7, has ground set $E_{f_7} = \{1,2,3,4,5,6,7\}$. Figure 4.1 contains a geometric representation of F_7, in this representation, the seven "lines" including the set $\{4,5,6\}$ represent the circuits. $r(F_7) = 3$ and the bases are all of the three element subsets that do not include the seven "lines". We want to obtain the bases and the circuits for the dual of this matroid, so by Lemma 3.3 we will need $\mathcal{B}_{f_7}$ and the hyperplanes. For the hyperplanes, we need all the rank 2 maximal subsets which actually turn out to be the circuits. So,

$$\mathcal{H}_{f_7} = \mathcal{C}_{F_7} = \{\{1,2,4\},\{1,5,7\},\{1,3,6\},\{2,6,7\},\{2,3,5\},\{3,4,7\},\{4,5,6\}\}$$

$\mathcal{B}_{F_7} = \{1,2,3\},\{1,2,5\},\{1,2,6\},\{1,2,7\},\{1,3,4\},\{1,3,5\},\{1,3,7\},\{1,4,5\},\{1,4,6\},$
$\{1,4,7\},\{1,5,6\},\{1,6,7\},\{2,3,4\},\{2,3,6\},\{2,3,7\},\{2,4,5\},\{2,4,6\},\{2,4,7\},\{2,5,6\},$
$\{2,5,7\},\{3,4,5\},\{3,4,6\},\{3,5,6\},\{3,5,7\},\{3,6,7\},\{4,5,7\},\{4,6,7\},\{5,6,7\}\}$

From these sets we can construct the information we need for F_7^* by taking the complements of the bases as the new bases, and taking the complements of the hyperplanes as the circuits. Thus the dual of the fano matroid has these ciruits and bases:

$$\mathcal{C}_{F_7^*} = \{\{3,5,6,7\},\{2,3,4,6\},\{2,4,5,7\},\{1,3,4,5\},\{1,4,6,7\},\{1,2,5,6\},\{1,2,3,7\}\}$$

$\mathcal{B}_{F_7^*} = \{4,5,6,7\},\{3,4,6,7\},\{3,4,5,7\},\{3,4,5,6\},\{2,5,6,7\},\{2,4,6,7\},\{2,4,5,6\},$
$\{2,3,6,7\},\{2,3,5,7\},\{2,3,5,6\},\{2,3,4,7\},\{2,3,4,5\},\{1,5,6,7\},\{1,4,5,7\},\{1,4,5,6\},$
$\{1,3,6,7\},\{1,3,5,7\},\{1,3,5,6\},\{1,3,4,7\},\{1,3,4,6\},\{1,2,6,7\},\{1,2,5,7\},\{1,2,4,7\},$
$\{1,2,4,6\},\{1,2,4,5\},\{1,2,3,6\},\{1,2,3,5\},\{1,2,3,4\}\}$

From here we can construct the independent sets of F_7^* and so we have built the dual of the fano matroid. As a check we can see that $r(F_7^*) = 4$ which is the complement of the rank of F_7.

Example 3.2.2 (The Non-Fano Matroid and its Dual, F_7^{-*})**.** Just as in the above two examples, if we want to construct a matroid dual we need to look at the matroid itself. In example 4.0.3 we look more closely at the non-fano matroid, but here we will just look at the bases and circuits. The non-fano matroid is very similar to the fano matroid, it's difference being that the set $\{4,5,6\}$ is a circuit and hyperplane in the fano matroid, but a basis in the non-fano matroid. So, the circuits and bases for the dual of the non-fano matroid would be:

$$\mathcal{C}_{F_7^{-*}} = \{\{3,5,6,7\},\{2,3,4,6\},\{2,4,5,7\},\{1,3,4,5\},\{1,4,6,7\},\{1,2,5,6\}\}$$

$\mathcal{B}_{F_7^{-*}} = \{4,5,6,7\},\{3,4,6,7\},\{3,4,5,7\},\{3,4,5,6\},\{2,5,6,7\},\{2,4,6,7\},\{2,4,5,6\},$
$\{2,3,6,7\},\{2,3,5,7\},\{2,3,5,6\},\{2,3,4,7\},\{2,3,4,5\},\{1,5,6,7\},\{1,4,5,7\},\{1,4,5,6\},$
$\{1,3,6,7\},\{1,3,5,7\},\{1,3,5,6\},\{1,3,4,7\},\{1,3,4,6\},\{1,2,6,7\},\{1,2,5,7\},\{1,2,4,7\},$
$\{1,2,4,6\},\{1,2,4,5\},\{1,2,3,6\},\{1,2,3,5\},\{1,2,3,4\},\{1,2,3,7\}\}$

Chapter 4

Representability

Whether or not a matroid can be represented with a matrix is an important idea in both matroid theory and when dealing with matroidal networks. In this section we will return to James Oxley's Matroid Theory [Oxl11] for the majority of the definitions, any different sources will be specified.

Definition 4.1. Matroids $M_1 = (E, I)$ and $M_2 = (E', I')$ are isomorphic if there is a bijection $\phi : E \to E'$ such that $X \in I$ if and only if $\phi(X) \in I'$.

Definition 4.2. A matroid M that is isomorphic to the vector matroid of a matrix A over a field $\mathbb{F}$ is representable over $\mathbb{F}$, and A is a representation of M over $\mathbb{F}$.

All matrices can be made into a matroid, and each of those matroids are represented by their matrices. Some interesting examples of representable matroids are the Fano matroid, and the non-Fano matroid. The Fano matroid, depicted in Figure 1.2, is a matroid depiction of the order 2 finite projective plane. The ground set is $E = \{1, 2, 3, 4, 5, 6, 7\}$ and the independent sets are the independent vectors in that projective plane.

$$D = \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}$$

Example 4.0.1 (A Matroid Representation for the Fano Matroid)**.** For this matroid representation we will be taking our matrix entries to be from $\mathbb{Z}_2$. It is easy to see that

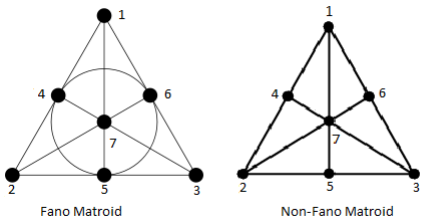

Figure 4.1: Fano and Non-Fano Matroids

$\{1, 2, 3\}$ is a basis for the Fano matroid, called F_7 from here on, so $r(F_7) = 3$. We can assign the first three columns of D to be vectors such that $1 = \{1, 0, 0\}$, $2 = \{0, 1, 0\}$, and $3 = \{0, 0, 1\}$. From here we can look at minimal dependent sets and see that $\{1, 2, 4\}$ is one such set. Then we see that 4 is dependent on 1 and 2 and so $4 = \{1, 1, 0\}$. Then $\{2, 3, 5\}$ are another such dependent set, so $5 = \{0, 1, 1\}$. Next, we have $\{1, 3, 6\}$ with 6 being dependent, so $6 = \{1, 0, 1\}$. Finally, 7 is dependent on 1, 2, and 3, and so $7 = \{1, 1, 1\}$. Next, we can take the matrix we just constructed and verify that our representation preserves the independent sets. For brevity we will look at a one example and leave the rest for the reader.

Since we decided to start with the basis $\{1, 2, 3\}$ as the identity we should check another basis. From Example 3.2.1 we can see that the set $\{2, 5, 7\}$ is also a basis for F_7. Lets look at the sub-matrix composed of these vectors.

$$D_1 = \begin{array}{ccc} 2 & 5 & 7 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{array}$$

Now we can check the determinant of D_1 to find out if it is independent.

$$detD_1 = 0(0) - 0(1) + 1(1) = 1$$

Since the determinant is non-zero we have an independent set. We could use this and other methods from linear algebra to check each of the independent set and we would get the same result. Thus D is a matrix representation for F_7.

Now we can see that the above matrix is a representation for F_7, but notice

two things. First, that we chose to use entries from $\mathbb{Z}_2$ for the matrix, and second, that the construction of the matrix did not rely on the circuit $\{4, 5, 6\}$ (which is the difference between the Fano and non-Fano matroids). Thus, the same representation can be used for both matroids. It turns out that the difference between these two matroids, representation wise, is that the Fano matroid can be represented over fields with characteristic two while the non-Fano matroid can be represented over fields of characteristic not two.

Example 4.0.2. In order to see that these two matroids have the same representation but over fields with different characteristics, we look at the sub-matrix, D', with the column vectors of the circuit $\{4, 5, 6\}$.

$$D' = \begin{array}{ccc} 4 & 5 & 6 \\ \hline 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{array}$$

From D' we can simply check the determinant.

$$detD' = 1(1) - 0(1) + 1(1) = 2$$

In a characteristic 2 field, $2 = 0$ and so these vectors are dependent. In the Fano matroid, $\{4, 5, 6\}$ is dependent. In the non-Fano matroid, these elements form an independent set, and since $detD' = 2$ is non-zero in fields of characteristic not two, these elements are independent. Once again all of the independent sets of the non-fano matroid can be checked using elementary linear algebra techniques to verify that the representation preserves independence.

Another interesting result for matroid representation is this necessary condition.

Theorem 4.3. For matroid $M = (E, I)$ with $X_i \subseteq E$ and $i \in \mathbb{Z}$ where $1 \leq i \leq 4$, a necessary condition for representability is that the rank function must satisfy:

$$\begin{aligned} &r(X_1) + r(X_2) + r(X_1 \cup X_2 \cup X_3) + r(X_1 \cup X_2 \cup X_4) + r(X_3 \cup X_4) \\ &\leq r(X_1 \cup X_2) + r(X_1 \cup X_3) + r(X_4 \cup X_4) + r(X_2 \cup X_3) + r(X_2 \cup X_4) \end{aligned}$$

This theorem is attributed to A. W. Ingleton [Ing69] and a proof can be found in his paper "Representations of Matroids".

Determining whether a matroid is representable can be quite a chore, sometimes it's almost impossible. This theorem gives us a tool to help determine if a matroid is not representable. If for any four subsets this inequality is not satisfied, then there is no matrix representation.

A brief discussion of matroid minors is required to continue the discussion of matroid representation.

Definition 4.4 (Submatroid)**.** Given matroid $M = (E, \mathcal{I})$. $M' = (E', \mathcal{I}')$ is a submatroid of M if $E' \subset E$, and $\mathcal{I}' \subset \mathcal{I}$.

It is good to note that the independent sets in a submatroid specifically must have been independent sets in the original matroid. There are several ways to create submatroids, but two ways are very important. These are deletion and contraction. (In some of the literature, deletion is referred to as restriction.) In Matroids A Geometric Introduction, [GM12] define these two processes nicely, but first we need to define a few more terms.

Definition 4.5 (Isthmus and Loop)**.** Given a Matroid, M, whose ground set is E. For an element $e \in E$, if e is in every basis of M, then e is an isthmus. If e is in no basis of E, then e is a loop.

Definition 4.6 (Deletion)**.** Given a Matroid, M, with ground set E and independent sets $\mathcal{I}$. For an element $e \in E$, where e is not an isthmus, the matroid $M - e$ has the ground set $E - \{e\}$ and it's independent sets are the elements of $\mathcal{I}$ that do not contain e. This is a submatroid created by deletion.

Definition 4.7 (Contraction)**.** Given a Matroid, M, with ground set E and independent sets $\mathcal{I}$. For an element $e \in E$, where e is not a loop, the matroid M/e has the ground set $E - \{e\}$ and it's independent sets are the elements of $\mathcal{I}$ that contained e, where these sets now have e removed.

Lemma 4.8. If e is not an isthmus or a loop, then $M - e$ and M/e are matroids.

Proof. To show that a deletion results in $M - e$ actually being a matroid we need to show that $M - e$ satisfies the three conditions of Definition 2.8. Given matroid $M = (E, \mathcal{I})$ perform a deletion on M by removing element e from E. Resulting in the new set $E - \{e\}$ and $\mathcal{I}'$ where $\mathcal{I}'$ contains all the elements of $\mathcal{I}$ except the elements containing e.

1. Since $\emptyset \in \mathcal{I}$ and $e \notin \emptyset$, then $\emptyset \in \mathcal{I}'$.

2. Let $I \in \mathcal{I}'$ then $e \notin I$. Let $J \subseteq I$, then $e \notin J$, and $J \in \mathcal{I}$. Therefore, $J \in \mathcal{I}'$.

3. Let $I_1, I_2 \subset \mathcal{I}'$, where $|I_1| > |I_2|$. There is an element $x \in I_1 - I_2$ so that $I_2 \cup \{x\} \in \mathcal{I}$. Since $x \in I_1$, $x \neq e$. So $I_2 \cup \{x\}$ does not contain e. Therefore, $I_2 \cup \{x\} \in \mathcal{I}'$.

So $M - e = (E - \{e\}), \mathcal{I}'$ is a matroid.

Next, as we did with $M - e$, we need to show $M - e$ meets the criteria from definition 2.8. Given a matroid , M, perform a contraction on it removing e from E. The resulting sets will be ground set $E - \{e\}$, and independent set $\mathcal{I}'$.

1. Since e is not a loop it is an independent set in the matroid M, so $\{e\} - \{e\} \in \mathcal{I}'$. But $\{e\} - \{e\} = \emptyset$, so the $\emptyset \in \mathcal{I}'$.

2. Let $I \in \mathcal{I}'$, and $J \subseteq I$, so $e \notin J$. But $I + \{e\} \in \mathcal{I}$, and $J + \{e\} \subset I + \{e\}$, so $J + \{e\} \in \mathcal{I}$. Then $J + \{e\} - \{e\} \in \mathcal{I}'$, but $J + \{e\} - \{e\} = J$. Therefore $J \in \mathcal{I}'$.

3. Let I_1 and I_2 be elements of $\mathcal{I}'$ where $|I_1| > |I_2|$. Then $I_1 \cup \{e\}$ and $I_2 \cup \{e\}$ are elements of $\mathcal{I}$ and $|I_1 \cup e| > |I_2 \cup \{e\}|$. From the definition of M we know that there is some element $x \in (I_1 \cup \{e\}) - (I_2 \cup \{e\})$, so that $I_2 \cup \{e, x\}$ is in $\mathcal{I}$. Also note that $x \neq e$ and $x \in I_1 - I_2$. Then by the definition of contraction, $I_2 \cup \{e, x\} - \{e\} = I_2 \cup \{x\}$ is in $\mathcal{I}'$. So Condition 3 is met.

So M/e is a matroid. □

Now that we have a few more definitions at our disposal we can introduce matroid minors. A matroid minor is a submatroid that is created from a matroid through a series of deletions and contractions. There are several propositions and interesting theorems that pertain to matroid minors that the reader is encouraged to study on their own. One thing to note is that the deletions and contractions can be done in any order as long as one is careful not to delete an isthmus or contract a loop.

Why are matroid minors important to matroid representability? Well as has been stated before finding out whether a matroid is representable or not is not always, or even usually, easy. One tool that has been developed is to look for forbidden minors. In very general terms forbidden minors are specific matroids that we know are not representable over specific fields. What we can do is take a matroid that we are interested in

and perform a series of contractions and deletions. If we can find one of the specific forbidden minors, then we know that the matroid we started with is also not representable over the same field.

We can then classify whole matroidal families by the fields they are representable over and the forbidden minors they contain. It is known, up to fields with characteristic four, what the forbidden minors are. For fields with characteristic five there is a list, but it is not known if it is complete. In the 1970's, Gian-Carlo Rota conjectured that for each class of matroid, meaning the group of matroids representable over a specific finite field, there were a finite number of forbidden minors. Geelen, Gerards, and Whittle have announced that they have proven this conjecture. As of the writing of this paper, their proof is forthcoming.

Now we can informally define several matroidal families. The binary matroids, which are the matroids representable over fields with characteristic 2, have the forbidden minor $U_{2,4}$, that is, the uniform matroid with four elements and rank 2. The ternary matroids are the matroids representable over characteristic 3 fields, and the forbidden minors are $U_{2,5}$, $U_{3,5}$, the fano matroid, and the dual of the fano matroid. The quarternary matroids are the matroids representable over fields with characteristic 4 and the list of excluded minors is; $U_{2,6}$, $U_{4,6}$, P_6, the non-fano matroid, the dual of the non-fano matroid, P_8, and a modified P_8 which Oxley denotes as $P_8^{=}$. Finally, there is a class of representable matroids that is representable over all fields, these are the regular matroids. A matroid is regular if it doesn't have the forbidden minors $U_{2,4}$, the fano matroid, and the dual of the fano matroid. The proofs for these forbidden minor classifications can be found in the literature.

Example 4.0.3. Looking at the fano matroid, it obviously contains itself, so it's not represenable over any field except those with characteristic 2. However, since the non-fano matroid, is not representable over fields with characteristic 2 we should be able to find a matroid isomorphic to $U_{2,4}$ by performing a series of deletions and contractions. First lets look at the ground set and independent set of the non-fano matroid. Here we use the normal notation F_7^- to talk about the non-fano matroid.

$$F_7^- = (E, \mathcal{I})$$

$E = \{1, 2, 3, 4, 5, 6, 7\}$

$\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}, \{7\}, \{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{1,6\}, \{1,7\}, \{2,3\},$
$\{2,4\}, \{2,5\}, \{2,6\}, \{2,7\}, \{3,4\}, \{3,5\}, \{3,6\}, \{3,7\}, \{4,5\}, \{4,6\}, \{4,7\}, \{5,6\},$
$\{5,7\}, \{6,7\}, \{1,2,3\}, \{1,2,5\}, \{1,2,6\}\{1,2,7\}, \{1,3,4\}, \{1,3,5\}, \{1,3,7\}, \{1,4,5\},$
$\{1,4,6\}, \{1,4,7\}, \{1,5,6\}, \{1,6,7\}, \{2,3,4\}, \{2,3,6\}, \{2,3,7\}, \{2,4,5\}, \{2,4,6\},$
$\{2,4,7\}, \{2,5,6\}, \{2,5,7\}, \{3,4,5\}, \{3,4,6\}, \{3,5,6\}, \{3,5,7\}, \{3,6,7\}, \{4,5,6\},$
$\{4,5,7\}, \{4,6,7\}, \{5,6,7\}\}$

Now we need to end up with a matroid isomorphic to $U_{2,4}$ where:

$$U_{2,4} = (E', \mathcal{I}')$$

$E' = \{a, b, c, d\}$
$\mathcal{I}' = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a,b\}, \{a,c\}, \{a,d\}, \{b,c\}, \{b,d\}, \{c,d\}\}$

This means we need to delete or contract three elements from F_7^-. You may be able to see that this is not a trivial task even on a relatively small matroid. First we will contract F_7^- by the element 6. This will eliminate an element and will reduce all rank three sets in $\mathcal{I}$ to rank 2.

$$F_7^-/6 = (E - \{6\}, \mathcal{I}_c)$$

$\mathcal{I}_c = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{7\}, \{1,2\}, \{1,4\}, \{1,5\}, \{1,7\}, \{2,3\}, \{2,4\}, \{2,5\}, \{3,4\},$
$\{3,5\}, \{3,7\}, \{4,5\}, \{4,7\}, \{5,7\}\}$

Then we will delete elements 7 and 3.

$$(F_7^-/6) - (3,7) = (E - \{3,6,7\}, \mathcal{I}_d)$$

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

From here it is easy to find a bijective function that takes $(F_7^-/6) - (3,7)$ to $U_{2,4}$. Thus, we can see that the non-fano matroid does indeed have the forbidden minor that prevents it from being representable over characteristic two fields.

A result on duality and representability should be added here. From [GM12], with $r = r(M)$, $n = |E|$, and $I_{c\times c}$ being the identity matrix;

Theorem 4.9. The matrix $A = [I_{r\times r}|D]$ represents the matrix M if and only if the matrix $A^* = [-D^T|I_{(n-r)\times(n-r)}]$ represents the dual of matroid M^*.

This means that the duals of representable matroids are also representable. Further it means that they are representable over the same fields as the original matroid.

Chapter 5

Networks from Matroids

5.1 Matroidal Networks

Now that we have some idea of what a matroid is, and we are familiar with the idea of a network, we will talk about matroidal networks. Informally, this is exactly how it sounds. A matroid is chosen and then using a predefined method, a network is constructed from the matroid. During this process the creator of the matroidal network will often have to make some choices, so these networks are not unique. In [DFZ07] matroidal networks are defined as follows:

Definition 5.1 (Matroidal Network)**.** Given a network $\mathcal{N}$ with message set μ, node set ν, edge set ϵ, and given a matroid $M = (S, \mathcal{I})$ with rank function r. Then, $\mathcal{N}$ is a matroidal network associated with M if there exists a function $f : \mu \cup \epsilon \to S$ so that the following conditions hold:

(M1) f is one to one on μ;

(M2) $f(\mu) \in \mathcal{I}$;

(M3) $r(f(In(x))) = r(f(In(x) \cup Out(x)))$, for every $x \in \nu$.

When dealing with matroidal networks there are some interesting results. We mentioned that there is some interest in finding whether or not a network is solvable, and we also talked a great deal about matroid representability. From [DFZ07] we have the following result:

Theorem 5.2. If a network, $\mathcal{N}$, is scalar-linearly solvable over a finite field, then $\mathcal{N}$ is matroidal. Also, $\mathcal{N}$ is associated with a representable matroid.

In [KM10], Kim and Médard prove the other direction.

Theorem 5.3. If a network, $\mathcal{N}$, is associated with a matroid that is representable over a finite field, then $\mathcal{N}$ is scalar-linearly solvable.

These results are nice in that once we have made a matroidal network created from a representable matroid, we know it is scalar-linearly solvable. Also, if we make a network from a matroid whose representability is in question, earlier we mentioned that it is not easy to determine whether matroids are representable, we can attempt to see if the network is scalar-linearly solvable. This could lead us to determining the representability of the matroid.

Now that we know what a matroidal network is we can get into the creation of them. In [DFZ07] the authors lay down a specific method for constructing networks from matroids.

Theorem 5.4 (Method for Construction Networks from Matroids)**.** Let $M = (S, \mathcal{I})$ be a matroid with rank function r. Let $\mathcal{N}$ be the network to be constructed, with μ its message set, ν its node set, and ϵ its edge set.

The construction will simultaneously construct the network $\mathcal{N}$, the function

$$f : \mu \cup \epsilon \to S,$$

and an auxiliary function

$$g : S \to \nu,$$

where for each $x \in S$, either

i. $g(x)$ is a source node with message m and $f(m) = x$; or

ii. $g(x)$ is a node with in-degree 1 and whose in-edge e satisfies $f(e) = x$.

The construction is carried out in four steps, and each step can be completed several ways.

Step 1. Create network source nodes $n_1, n_2, ..., n_{r(S)}$ and corresponding messages $m_1, m_2, ..., m_{r(S)}$. Choose any basis $B = \{b_1, ..., b_{r(S)}\}$ for M and let $f(m_i) = b_i$ and $g(b_i) = n_i$.

Step 2. (to be repeated until no longer possible) Find a circuit $\{x_0, ..., x_j\}$ in M, such that $g(x_1), ..., g(x_j)$ have already been defined, but not $g(x_0)$. Then we add:

1) a new node y and edges $e_1, ...e_j$ such that e_i connects $g(x_i)$ to y. Let $f(e_i) = x_i$.

2) a new node n_0 with a single in-edge e_0 that connects y to n_0. Let $f(e_0) = x_0$ and $g(x_0) = n_0$.

Step 3. (can be repeated arbitrarily many times) If $\{x_0, ..., x_j\}$ is a circuit of M and $g(x_0)$ is a source node with message m_0, then add to the network a receiver node y which demands the message m_0 and in edges $e_1, ..., e_j$ where e_i connects $g(x_i)$ to y. Let $f(e_i) = x_i$.

Step 4. (can be repeated arbitrarily many times) Choose a base $B = \{x_1, ...x_{r(S)}\}$ of M and create a receiver node y that demands all of the network messages and has in-edges $e_1, ...e_{r(S)}$ where e_i connects $g(x_i)$ to y. Let $f(e_i) = x_i$.

This method for created networks from matroids ensures that the resulting network is matroidal, which is consistent with Definition 5.1.

Proof. We need to show that conditions $M(1)$, $(M2)$, and $(M3)$ hold for this construction method. Step 1 and Step 2 clearly uphold conditions $(M1)$ and $(M2)$. To see that condition $M(3)$ is met we look at each type of node that is created. In Step 1, source nodes are created. These source nodes generate a single message and then send the same message out through out-edges; thus $(M3)$ is met. Step 2 creates intermediate nodes that have in-edges and out-edges. These nodes do not generate or demand messages. Also, the messages sent from these node's out-edges are combinations of the messages they receive on the in-edges, so $(M3)$ holds. Finally in Steps 3 and 4, receiver nodes are created. These nodes have no out-edges. Step 3 creates receiver nodes that demand a single message based on a circuit in the matroid. Since circuits are minimal dependent sets the rank of a circuit is the same when you take out just one element. Each Step 3 reciever node recieves a certain number of ground set elements in the form of $f(\epsilon)$ as the in-edges, the rank of that set will not change when you add in one more element that forms a dependent set, so $(M3)$ holds. Then for the receiver nodes created in Step 4 a basis is used to get the in-edges, so $r(f(In(x)))$ will be maximal, so $(M3)$ holds. □

Notice that in Step 3 we don't necessarily include all of the circuts of a matroid. Thus the dependencies of the matroid might not all be represented. At the beginning of the section we mentioned that the creator of the network had to make some choices, namely what basis to use and what circuits to include (in situations where not all of the circuits could be used). Depending on the choices made, the networks will be different.

5.2 A Dual Fano and a Dual Non-Fano Network

The focus of this paper has been to gain enough knowledge to create some matroidal networks using this method. We have introduced the fano and non-fano matroids. In a subsequent section networks created from these matroids will be seen. However, these networks have been looked at and some very interesting things have been proven about them. Here we will construct some matroids from duals of the fano and non-fano matroids. In examples 3.2.1 and 3.2.2 we have noted the sets of bases and the sets of circuits for these two matroids. From these sets we will use the method in theorem 5.4 to construct the two matroidal networks. Theorem 5.3 says that since these networks are matroidal they should have a scalar linear solution, so we will find one for each of the networks. A note on notation, previously we have talked about the ground sets of both matroids, F_7 and F_7^- as $\{1,2,3,4,5,6,7\}$. From here on we will use the set $\{A,B,C,D,E,F,G\}$ as the ground set so that we can reserve numerals to label our nodes.

Example 5.2.1 (Dual Fano Network)**.** We will start with the dual of the Fano Matroid, and complete each step according to the above method.

Step 1. First, we have to choose a matroid basis. Let $Basis = \{\hat{A},\hat{B},\hat{C},\hat{D}\}$ and network messages A, B, C, and D. We will assign $f(A) = \hat{A}$, $f(B) = \hat{B}$, $f(C) = \hat{C}$, and $f(D) = \hat{D}$. Now we assign the nodes, $g(\hat{A}) = n_1$, $g(\hat{B}) = n_2$, $g(\hat{C}) = n_3$, and $g(\hat{D}) = n_4$. See Figure 5.1.

Figure 5.1: Step 1. Dual Fano Network

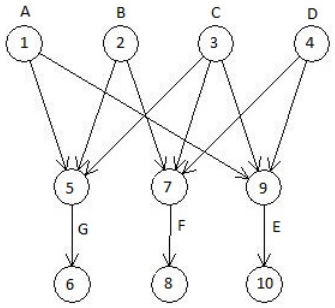

Figure 5.2: Step 2. Dual Fano Network

Step 2. Next we have to represent the other elements of the ground set in the network by adding them one by one using circuits that contain only one new element at a time. Our first circuit will be $\{A, B, C, G\}$ (note that this circuit is one of the things that makes the dual of the fano matroid different from the dual of the non-fano matroid). We will add a new node n_5, and edges $e_{1,5}$, $e_{2,5}$, and $e_{3,5}$. Then we let $f(e_{1,5}) = \hat{A}$, $f(e_{2,5}) = \hat{B}$, and $f(e_{3,5}) = \hat{C}$. Then we another node n_6 with in-edge $e_{5,6}$ and let $f(e_{5,6}) = \hat{G}$, and $g(\hat{G}) = n_6$.

Then we look at circuit $\{B, C, D, F\}$. We add node n_7, and edges $e_{2,7}$, $e_{3,7}$, and $e_{4,7}$. Let $f(e_{2,7}) = \hat{B}$, $f(e_{3,7}) = \hat{C}$, and $f(e_{4,7}) = \hat{D}$. Then add node n_8 with in-edge $e_{7,8}$ and let $f(e_{7,8}) = \hat{F}$ and $g(\hat{F}) = n_8$.

Finally, we use the circuit $\{A, C, D, E\}$. We add node n_9, and edges $e_{1,9}$, $e_{3,9}$, and $e_{4,9}$. Let $f(e_{1,9}) = \hat{A}$, $f(e_{3,9}) = \hat{C}$, and $f(e_{4,9}) = \hat{D}$. Then add node n_{10} with in-edge $e_{9,10}$ and let $f(e_{9,10}) = \hat{E}$ and $g(\hat{E}) = n_{10}$. See Figure 5.2.

Step 3. In this step we will add in the receiver nodes, this step is also based on the circuits of the matroid. We have $g(\hat{A})$ with message A as a source node so using circuit $\{A, B, E, F\}$ we create a reciever node n_{14} that demands message A, with in-edges $e_{2,14}$, $e_{8,14}$, and $e_{10,14}$. Similarly using circuit $\{B, D, E, G\}$ we add receiver node n_{13} that demands message B, with in edges $e_{4,13}$, $e_{6,13}$, and $e_{10,13}$. Next using circuit $\{A, C, D, E\}$ we add receiver node n_{12} demanding message C with in-edges $e_{1,12}$, $e_{4,12}$, and $e_{10,12}$. Finally, using circuit $\{A, D, F, G\}$ we add receiver node n_{11} demanding message D with in-edges $e_{1,11}$, $e_{6,11}$, and $e_{8,11}$. See Figure 5.3.

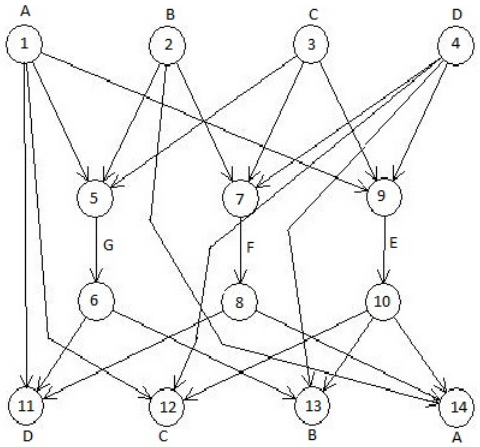

Figure 5.3: Step 3. Dual Fano Network Complete

Here we omit the optional Step 4, and our network made from the dual of the fano matroid is complete.

Example 5.2.2 (Dual Non-Fano Network)**.** Using the same method as before, we will now construct a matroidal network based on the dual of the non-fano matroid.

Step 1. In this step we once again choose a basis. Note that the dual of the non-fano matroid has the set $\{A, B, C, D\}$ as a basis just like the dual of the fano matroid. We will use this same basis for this matroidal network. Thus Step 1, will be identical to Step 1 in the previous example, and figure 5.1 will also be the first visual result.

Step 2. Now we will use circuits from the matroid to convey some of the matroids dependencies. The first circuit we will use is $\{A, C, D, E\}$. We add node n_5, and edges $e_{1,5}$, $e_{3,5}$, and $e_{4,5}$. Let $f(e_{1,5}) = \hat{A}$, $f(e_{3,5}) = \hat{C}$, and $f(e_{4,5}) = \hat{D}$. Then add node n_7 with in-edge $e_{5,7}$ and let $f(e_{5,7}) = \hat{E}$ and $g(\hat{E}) = n_7$.

Then we look at circuit $\{B, C, D, F\}$. We add node n_6, and edges $e_{2,6}$, $e_{3,6}$, and $e_{4,6}$. Let $f(e_{2,6}) = \hat{B}$, $f(e_{3,6}) = \hat{C}$, and $f(e_{4,6}) = \hat{D}$. Then add node n_8 with in-edge $e_{6,8}$ and let $f(e_{6,8}) = \hat{F}$ and $g(\hat{F}) = n_8$.

Finally, we use circuit $\{A, D, F, G\}$. We add node n_9, and edges $e_{1,9}$, $e_{4,9}$, and $e_{8,9}$. Let $f(e_{1,9}) = \hat{A}$, $f(e_{4,9}) = \hat{D}$, and $f(e_{8,9}) = \hat{F}$. Then add node n_{10} with in-edge

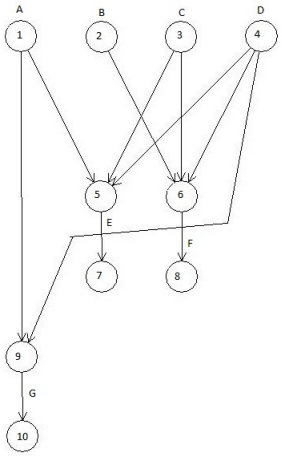

Figure 5.4: Step 2. Dual Non-Fano Network

$e_{9,10}$ and let $f(e_{9,10}) = \hat{G}$ and $g(\hat{G}) = n_{10}$. See Figure 5.4.

Step 3. Once again, we add the receiver nodes using circuits of the matroid. Using circuit $\{A, B, E, F\}$ we add receiver node n_{14} demanding message A with in-edges $e_{2,14}$, $e_{7,14}$, and $e_{8,14}$. Then we use circuit $\{A, C, D, E\}$ and add receiver node n_{13} demanding message D with in-edges $e_{1,13}$, $e_{7,13}$, and $e_{3,13}$. Next we add receiver node n_{12} demanding message C with in-edges $e_{7,12}$, $e_{8,12}$, and $e_{10,12}$. Finally with circuit $\{B, D, E, G\}$ we add receiver node n_{11} demanding message B with in-edges $e_{4,11}$, $e_{7,11}$, and $e_{10,11}$.

Once again we don't use the optional Step 4. See Figure 5.5.

5.3 A Linear Solution

In order for these networks to have a solution, each receiver node has to be able to obtain it's required message using the information that it receives through in-edges attached to it. In "Unachievability of Network Coding Capacity", [DFZ06] the authors prove that a network created from the fano matroid, called the fano network is only scalar linearly solvable over alphabets with even size. They also prove that a network created from the non-fano matroid, is only linearly solvable over fields with odd size. This tells us that some matroidal networks are only solvable over particular fields.

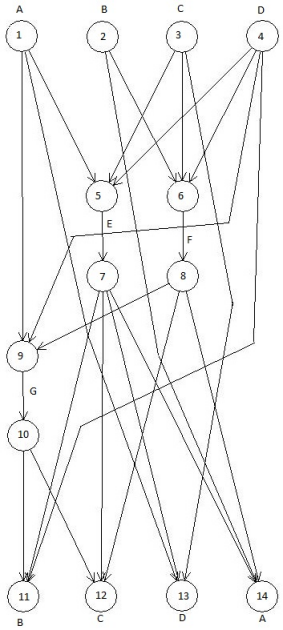

Figure 5.5: Step 3. Dual Non-Fano Network Complete

Example 5.3.1 (A solution for the "Dual Fano Network")**.** When we consider the network that we created in figure 5.3 we can actually find a solution just by examination. Recall from Section 2.1 that if we can find a coding solution that only uses vector addition and multiplication by a constant matrix, then we will have a linear solution. Further recall that if the source dimension and the edge capacity equal 1 then our solution is scalar. Lets take a look at what a simple solution looks like in the Dual Fano network. Looking at node 5 we see that it receives messages A, B, C so let $e_{5,6} = A + B + C = G$. Then node 7 receives messages B, C, D, so let $e_{7,8} = B + C + D = F$. Similarly, node 9 receives A, C, D so let $e_{9,10} = A + C + D = E$. From here we let the decoding messages be as follows:

$$n_{11} : A + G + F,$$

$$n_{12} : A + D + E,$$

$$n_{13} : D + G + E,$$

$$n_{14} : B + F + E.$$

Now if we look at the code in more detail we can see:

$$\begin{aligned}
n_{11} :&A + G + F = A + A + B + C + B + C + D = 2A + 2B + 2C + D,\\
n_{12} :&A + D + E = A + D + A + C + D = 2A + 2D + C,\\
n_{13} :&D + G + E = D + A + B + C + A + C + D = 2D + 2A + 2C + B,\\
n_{14} :&B + F + E = B + B + C + D + A + C + D = 2B + 2C + 2D + A.
\end{aligned}$$

We can see that at each node all of the information that we don't want comes in pairs. When we look at the solution modulo 2, all of the pairs become zeros, and we are left only with the message needed at each node. So for alphabets isomorphic to characteristic 2 fields the coding set is a solution. For other alphabets we do not eliminate the excess information and so our receiver nodes wont have their demands met. This leaves the question of whether there is a coding solution that works over all alphabets. If we let the previously defined edge functions, $f(e_{5,6}), f(e_{7,8})$, and $f(e_{9,10})$ remain the same, but change the decoding functions as follows:

$$\begin{aligned}
n_{11} :&A - G + F = A - (A + B + C) + (B + C + D) = D,\\
n_{12} :&E - A - D = (A + C + D) - A - D = C,\\
n_{13} :&D - E + G = D - (A + C + D) + (A + B + C) = B,\\
n_{14} :&B - F + E = B - (B + C + D) + (A + C + D) = A.
\end{aligned}$$

We can see that this is a coding solution over alphabets of all sizes. As stated above, this isn't always the case, so this is interesting and not something that was entirely expected before this network was created.

Example 5.3.2 (A solution for the "Dual Non-Fano Network")**.** Now that we have seen what a coding solution can look like, finding one for our dual non-fano matroidal network won't be to much of a problem. We can start by defining some of our edge functions as follows:

$$\begin{aligned}
e_{5,7} =&A + C + D = E,\\
e_{6,8} =&B + C + D = F,\\
e_{9,10} =&A + D + F = G.
\end{aligned}$$

From here we can then define our decode functions at our receiver nodes:

$$
\begin{aligned}
n_{11} =& G - E - D = A + D + B + C + D - (A + C + D) - D = B, \\
n_{12} =& F - G + E = B + C + D - (A + D + B + C + D) + (A + C + D) = C, \\
n_{13} =& E - A - C = (A + C + D) - A - C = D, \\
n_{14} =& E - F + B = (A + C + D) - (B + C + D) + B = A
\end{aligned}
$$

Using this code each of the receiver nodes do obtain the messages that they require, and so this is a solution over all fields.

Chapter 6

Conclusion and Further Questions

When beginning the research on matroidal networks there were several topics that one naturally has to gain at least a partial understanding. This paper only just brushes the surface of the two namesake areas, network theory and matroid theory, but during the research many deeper questions began to manifest. One of these questions became more of a focus then the others. In prior works, see [DFZ07] and [DFZ06], two matroidal networks have been studied in some detail. These networks are known as the fano network and the non-fano network, and as previously stated were of prime influence on the creation of the two networks in examples 5.2.1 and 5.2.2. In [DFZ06] the authors prove that the fano network only has a scalar linear solution over alphabets with size power 2, and the non-fano network only has scalar linear solutions over alphabets with odd size. These proofs are certainly not trivial and required the authors to identify a property universal to every scalar linear solution for both of the networks. They then used the property to prove the above. The interesting thing about this is that the fano matroid is only representable over fields with two elements, and the non-fano matroid is representable, but not over fields with two elements. The networks and the matroids they come from have some surprising similarities, right?

This makes one wonder whether all matroidal networks' solutions, made from representable matroids, share a similar relationship with their matroids representation restrictions. In this paper we built two matroidal networks and then talked about some of the solutions to these networks. One thing to note with both examples was that there is a solution that works over all fields. It would appear that a matroids representation

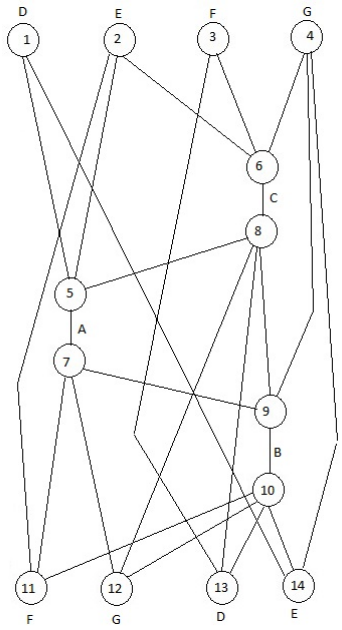

Figure 6.1: Another Network Created from the Dual of the Fano Matroid

restrictions do not guarantee a restriction for what fields a network has scalar linear solutions. This only leads to more questions.

During the process of constructing a matroidal network, there are several choices that have to be made, i.e. what basis to use, what circuits to include. These choices allow for different networks to be created from the same matroid. Figure 6.1 shows a second network created from the dual of the fano network using the method set out in section 5. This network uses a different basis in the first step and so becomes a completely different network, with different solutions. Which leads to the next question. Is there a constructable matroidal network for every representable matroid that shares the affore mentioned similarity between the matroids representation restrictions and the matroidal networks alphabet size?

This question is by no means an easy one. The current method to prove that a matroidal network only has scalar linear solutions over certain fields requires use of the property mentioned earlier. This property is tailored to the networks being used in the proof, and so the property is not general to all matroidal networks. Finding an answer to this question would perhaps require a new method for constructing matroidal networks that restricts the construction to networks with the property required.

Matroidal Networks are a relatively new area of study with many questions still unanswered. In this paper we have discussed the basics of both matroids and networks. We then constructed two matroidal networks from the duals of some matroids that stand out in the field. Finally we discussed a linear solution for each of the created networks. We are now armed with a better understanding of matroidal networks and in the future we can proceed to find the answers to some of those pressing questions.

Bibliography

[ACLY00] R. Ahlswede, N. Cai, S.Y.R. Li, and R.W. Yeung. Network information flow. *IEEE Transactions on Information Theory*, 46:1204–1216, 2000.

[DFZ06] R. Dougherty, C. Freiling, and K. Zeger. Unachievability of network coding capacity. *IEEE Transactions on Information Theory*, 52:2365–2372, 2006.

[DFZ07] R. Dougherty, C. Freiling, and K. Zeger. Networks, matroids, and non-shannon information inequalities. *IEEE Transactions on Information Theory*, 53:1949–1969, 2007.

[GM12] Gary Gordon and Jennifer McNulty. *Matroids A Geometric Introduction.* Cambridge Iniversity Press, Cambridge, UK, 2012.

[Ing69] A.W. Ingleton. Representations of matroids. In *Proc. of the Conference on Combinatorial Mathematics and its Applications.* Oxford, 1969.

[KM10] A. Kim and M. Médard. *Scalar-linear Solvability of Matroidal Networks Associated with Representable Matroids.* Massachusetts Institute of Technology, Cambridge, MA, 2010.

[Oxl11] James Oxley. *Matroid Theory.* Oxford University Press, 2011.