UNIVERSITY OF CALGARY

Dependence Deduction: A New Perspective in Constructing Matroidal Networks

by

Ming He

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

CALGARY, ALBERTA

SEPTEMBER, 2013

Abstract

Matroidal networks play a fundamental role in proving theoretical results on the limitation of network coding. This can be explained by the underlying connections between network coding and matroid theory. Two existing methods are known in the network coding literature for constructing networks from a matroid. The method due to Dougherty *et al.* [5] has high time complexity but can create relatively simple network structures from a given matroid. The method due to El Rouayheb *et al.* [3] has low time complexity, but results in rather complex network structures.

This thesis studies the design of matroidal networks from uniform and whirl matroids, targeting both low time complexity and minimum network sizes. Our construction is based on the new technique of dependence deduction, which may serve as a promising direction for constructing general matroidal networks. Some of our constructions lead to new networks for understanding network coding in terms of base field requirements.

Acknowledgements

I would like to express my greatest gratitude to the people around me. Without the endless help and support from them, I can never have this thesis completed.

First, I would like to thank the department of computer science for all the guidance and support they have provided. Many thanks to the administration and support staff for their assistance during the past two years. To the Networks Research Group, thanks for the active and friendly atmosphere you have created.

Second, I would like to appreciate Dr. Zongpeng Li, my supervisor for giving me the precious opportunity to study here and research under his supervision. He is always a great tutor for me, leading me when I am seeking the way to do research, encouraging me when I am faced with difficulties and guiding me when I am lost in research. Without his encouragement, patience and dedication, I would never have completed this thesis. Meanwhile, I would like to thank Dr. Randall Dougherty for many helpful discussions during the research.

At last, I would like to thank my lab mates. They offered me great help during my stay here. At the same time, I want to dedicate this thesis to my family. They are always on my side and support me.

I have been fortunate enough to receive so many kinds of help from other people in my life. Thank them all for being around.

Table of Contents

List of Tables

List of Figures and Illustrations

List of Symbols, Abbreviations and Nomenclature

Symbol	Definition
U of C	University of Calgary

Chapter 1

Introduction

1.1 Background

First proposed by Ahlswede *et al.* [1], network coding is a relatively new technique that encourages in-network "mixing" of data flows, departing from the then *de facto* standard of store-and-forward networking [10]-[11]. Fig. 1.1 depicts the well-known butterfly network that is often used to illustrate the idea of network coding. Here every edge has a unit capacity. The source S disseminates two unit-rate information flows x and y to two receivers T_1 and T_2. Other nodes including V_1, V_2, V_3, V_4, which are shown as white circles, are relay nodes. This single-source multicast session aims to make the two receivers receive both source flows x and y simultaneously. Before network coding was proposed, nodes in a network are only allowed to store the information flows and forward them to their output edges. In this case, edge V_3V_4 in the middle of the butterfly network can transmit either x or y, but not x and y simultaneously due to the edge capacity constraint. Consequently, either T_1 or T_2 can receive the messages they want, but not at the same time. In contrast, with network coding, relay nodes in a network can perform not only store-and-forward, but also encoding and decoding. In the case of the butterfly network, the "conflicting" point V_3 can encode the incoming information flows, for example, by taking a a bit-wise exclusive-or (XOR) of x an y, denoted as $x+y$. Then after node V_4's replication and relaying, receiver T_1 can recover y by XORing x and $x+y$, receiver T_2 can recover x by XORing y and $x+y$, at the same time. From this example we can see network coding improves the throughput of the multicast session by resolving the "conflict" at a bottleneck link.

From the butterfly example, we can see the *dependence relation* between the data flows on a node's out-edges and its in-edges generalizes from merely select-and-copy to all possible

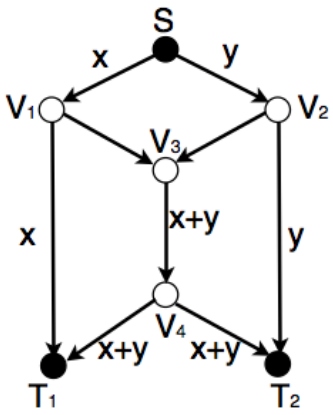


Figure 1.1: The *butterfly* network.

linear and non-linear relations. Linear dependence is shown to suffice in a number of network coding problems, including one-to-many multicast[2][10]. In such network coding problems where linear dependence is known to be sufficient, if the problem is solvable (the desired end-to-end throughput is achievable with a network coding based solution), then all nodes can perform only linear encoding and decoding operations to allow all receivers receive the information they want. Whether linear network coding is sufficient for all network coding problems remained an open problem for a few years, until Dougherty *et al.* [4] designed an example network (Fig. 1.2) that is not solvable if only linear operations is allowed, but is solvable if intermediate nodes can do non-linear encoding, for example bit switching within bit streams. This network has sources n_1, n_2, n_3, n_{11}, n_{12} with messages a, b, c, d, e, respectively. In all networks drawn in the rest of the thesis, a node with a letter above denotes a source node sending the message represented by the letter, a node with a letter below denotes a demand node requesting the message represented by the letter. Letters beside edges denote the packets carried by those edges. A node marked with numeral i will be referred to as n_i, and an edge from n_i to n_j will be referred to as $e_{i,j}$. Receivers n_{37} through n_{46} each demands one of the messages, as indicated below. Dougherty *et al.* designed this example by utilizing the technique of matroidal networks, *i.e.*, constructing a network from a given matroid.

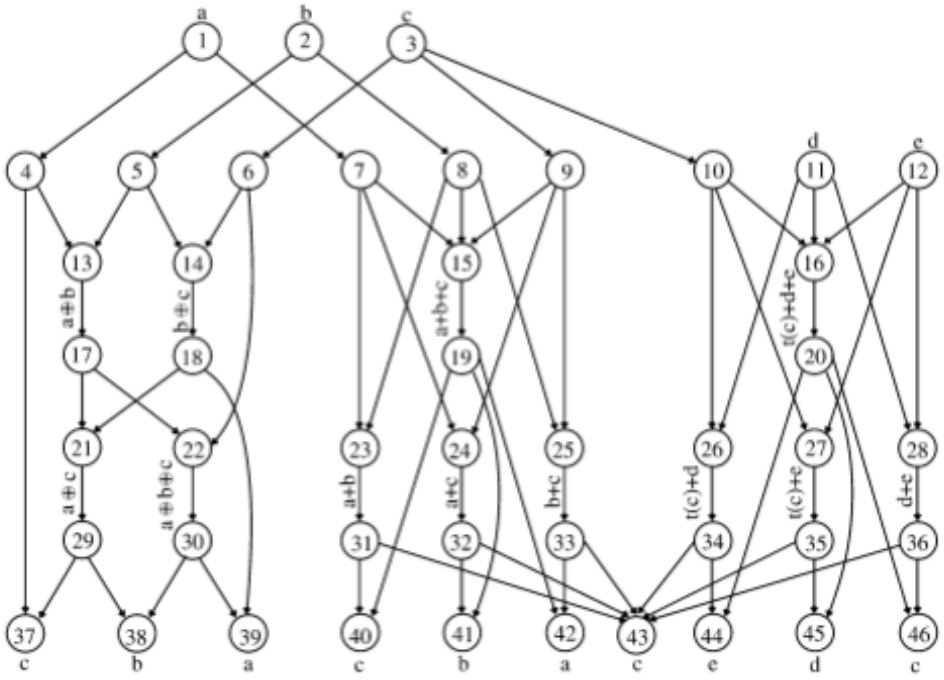


Figure 1.2: A network that requires nonlinear network coding.

The reason behind the construction of matroidal networks lies in the fact that matroid theory is also built upon the fundamental concept of dependence and independence. Founded in 1935 by Whitney [15], matroid theory is a branch of mathematics that generalized the dependence and independence concepts in both linear algebra and graph theory. For example, in graph theory, any set of edges that contains a cycle is a dependent set (see Fig. 1.3(a)), while any subset of a spanning tree is an independent set. Network coding is related to the notion of dependence in a rather obviously way. For a particular network node n, there are four types of relevant data: 1) data from packets received along the in-edges of n; 2) data from messages that originate at n; 3) data from packets sent along out-edges of n; 3) data from messages demanded by n. We require that data of the latter two types be generated by deterministic functions of the first two types. The incoming packets, the originated messages, and any outgoing packet form a dependent set (see Fig. 1.3(b)). Such a connection between network coding and matroid theory suggests the possibility of transforming a matroid into a network with some desired properties.

(a) (b)

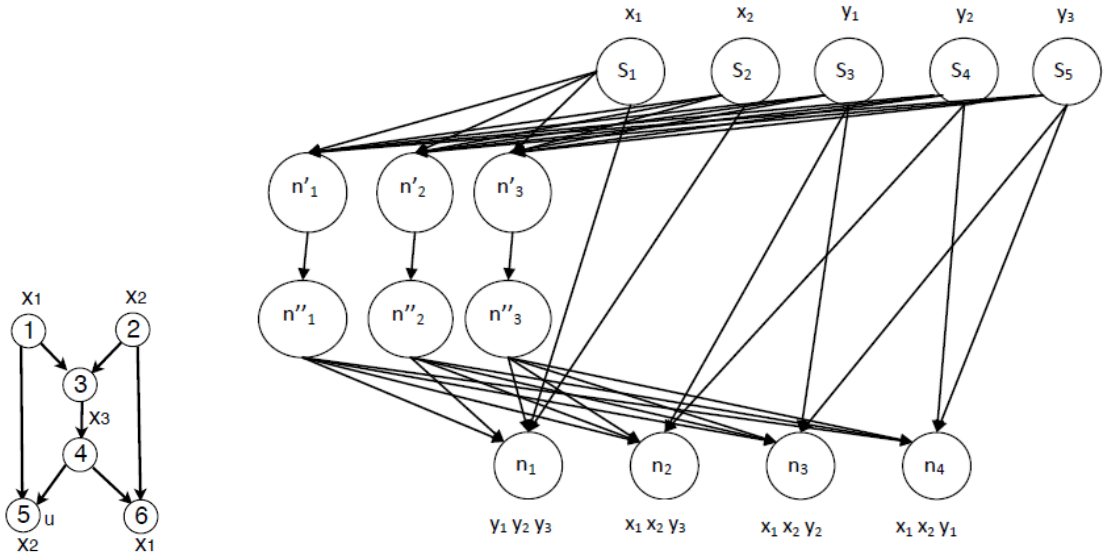
Figure 1.3: Dependent set in a graph (a) and a network (b).

Dougherty *et al.* [5] found that there is a close relationship between matroid linear representability and network scalar-linear solvability. If we can design a procedure to transfer all the dependent relations in a matroid into a network, then the resulting network is scalar-linearly solvable over a finite field $\mathbb{F}$ *if and only if* the matroid is representable over the same field $\mathbb{F}$. As matroid representability is a relatively mature subject of study, relating these two areas will enable us to gain new insight on network coding, specifically the scalar-linear solvability of network coding problems.

Towards this direction, Dougherty *et al.* [5] designed a method to construct a network from a matroid, referred to as *the D-F-Z method* in this thesis. Applying the D-F-Z method, a number of well-known matroids can be transformed into their corresponding networks. Such networks have served as a basis for our understanding of the limitations of network coding, including the insufficiency of linear coding in multi-source network coding [4] (see Fig. 1.2), the non-Shannon information inequalities [5], the unachievability of network coding capacity [20], and the non-reversibility of multiple-unicast networks [6].

Unfortunately, the D-F-Z method suffers from a very high time complexity, despite moderate sizes of its output networks. To mitigate this problem, El Rouayheb *et al.* [3] proposed another method, referred to as *the E-S-G method* in this thesis, using index coding as an intermediate step to construct a network from a matroid. This method has a low time complexity, but results in networks that contain a substantial level of redundancy in nodes and

edges, when compared to the D-F-Z matroidal networks built from the same input matroid. Fig. 1.4 compares the output of the D-F-Z method with that of the E-S-G method, for a simple matroid $U_{2,3}$. Fig. 2.3(a) shows the result from the D-F-Z method while Fig. 1.4(b) is the result from the E-S-G method.



(a) (b)

Figure 1.4: Output network from $U_{2,3}$ matroid by the D-F-Z (a) and E-S-G (b) method, respectively.

1.2 Motivation

We study matroidal network construction that aims at both reducing the time complexity of the D-F-Z method and simplifying the graph structure in the resulting matroidal network. We observe that the D-F-Z method only explicitly transfers a subset of all dependence relations in a matroid into the network during the construction process, while the E-S-G method explicitly transfers all the dependence relations. The high time complexity of the D-F-Z method comes from the complexity to determine the subset of all dependence relations that need to be explicitly transferred. Meantime, as the number of dependence relations transferred during the construction has a direct impact on the size of the resulting network,

the D-F-Z method naturally leads to a very simple network structure.

Another interesting observation is that, in the D-F-Z construction, dependence relations not explicitly transferred can be deduced from the explicitly transferred dependence and independence relations, *by using certain rules*. Using *dependence deduction* we can prove that all dependence relations in a matroid have been indeed transferred to the network created, including both explicitly and implicitly. As a result, if we can determine the proper subset of all dependence relations that need to be explicitly transferred in a more efficient way with the help of the deduction rules, we can reduce the time complexity of the D-F-Z method to a large extent. This concept of dependence deduction serves as an important tool for improving the D-F-Z method.

We first focus on uniform matroids, for which dependence deductions are relatively simple. We design a uniform matroidal network construction procedure that achieves both low time complexity and minimal network sizes. Next we try to apply this technique of dependence deduction on more matroids, including in particular whirl matroids. Again we design a procedure to construct a network from a given whirl matroid. This procedure is also low in time complexity and produces networks of small sizes. Other than the uniform and whirl matroids, we show that the technique can also be applied on a matroid called Q_6 matroid. During the construction of a subset of uniform matroidal networks, we find there exists a subnetwork property between the networks. Finally, we generalize this subnetwork property to a larger set of uniform matroidal networks, specifically matroidal networks from any uniform matroid and its matroid minor.

1.3 Contributions

In matroid theory, uniform matroids have special representability properties. For example, it is known that a uniform $U_{2,n}$ matroid is representable over a finite field $\mathbb{F}_q$ *iff* $q \geq n-1$. Our method creates a $U_{2,n}$ matroidal network that is scalar-linearly solvable over a finite field

$\mathbb{F}_q$ *iff* $q \geq n-1$. A natural question in network coding is what are the smallest networks that require coding over $\mathbb{F}_q$, for each prime power $q \geq 2$. Our two-multicast $U_{2,n}$ matroidal networks beat the currently known combination networks $C_{n,2}$, in that the former contains a smaller number of nodes and a smaller number of edges, while requiring the same finite field $\mathbb{F}_q$ for scalar-linear solvability. A combination network $C_{n,2}$ is a three level multicast network, with source node at the top level, sending two information flows x and y, n relay nodes in the middle, each connected to the source node, $\binom{n}{2}$ receiver nodes at the bottom level, each connected to a different pair of relay nodes. In particular, the $U_{2,4}$ matroidal network (Fig. 1.5(a)) is now the smallest known network that requires $\mathbb{F}_3$, and is simpler than the combination network $C_{4,2}$ (Fig. 1.5(b)) and planar networks [18] due to Xiahou *et al.* [7] that also require $\mathbb{F}_3$.

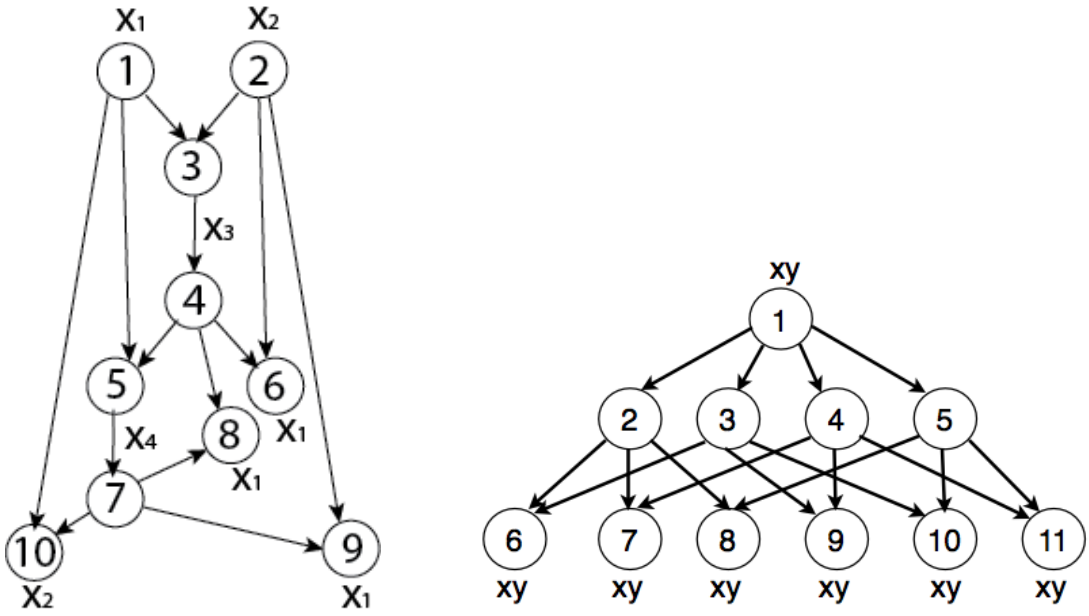


Figure 1.5: The $U_{2,4}$ matroidal network (a) and the $C_{4,2}$ combination network (b).

Whirl matroids [8] have special representability properties as well. All whirl matroids are representable over a finite field $\mathbb{F}_q$ *iff* $q \geq 3$. Our method for whirl matroids $\mathcal{W}^n (n \geq 3)$ transform $\mathcal{W}^3$ into a planar multiple unicast network (see Fig. 1.6(a)). We prove that all

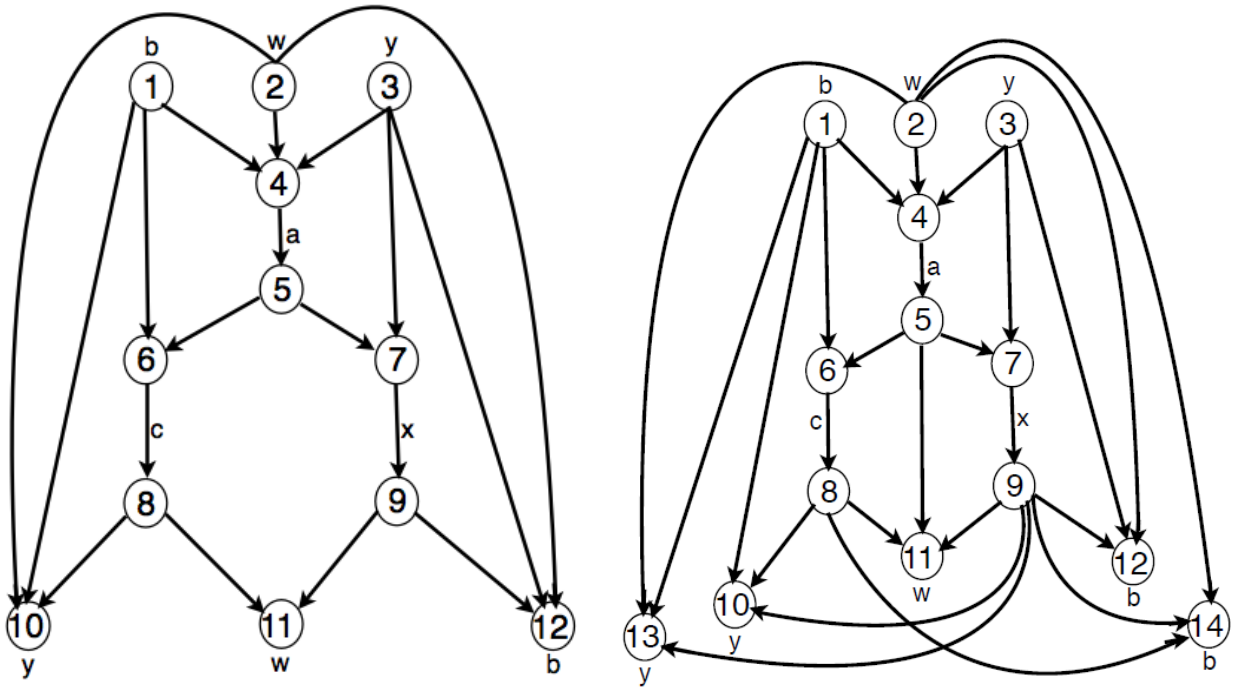
matroidal dependences can be deduced in this network, although the deduction process is more involved than in uniform matroids. The resulting $\mathcal{W}^3$ matroidal network requires a field size of at least 3 to be scalar-linearly solvable. In rather recent literature of network coding, there has been a conjecture, with partial proofs, that multicast network coding problems are always solvable over $\mathbb{F}_3$ in planar networks [7] [19]. While planar *multicast* networks requiring $\mathbb{F}_3$ have been recently designed, our $\mathcal{W}^3$ matroidal network represents the first and only planar *multiple-unicast* network that requires $\mathbb{F}_3$. It further leads to the interesting question whether $\mathbb{F}_3$ is also sufficient for all planar multiple-unicast networks.

Our contribution lies not only in uniform and whirl matroidal network construction, but also in the concept of dependence deduction, which is helpful in designing not only uniform and whirl matroidal networks but also general matroidal networks. As an example, we apply dependence deduction to transform a matroid called Q_6, which is representable over a finite field $\mathbb{F}_q$ *iff* $q \geq 4$. The resulting network (Fig. 1.6(b)) is scalar-linearly solvable over $\mathbb{F}_q$ *iff* $q \geq 4$, and is the second example of an almost-planar network requiring $\mathbb{F}_4$ (the first is $U_{2,5}$). We can further conjecture that $\mathbb{F}_4$ is sufficient for all almost-planar network coding problems.

The technique of dependence deduction also inspires us to take a closer look on the relationship between the matroidal network from a given matroid and its matroid minor. We find that there exists an elegant subnetwork property between the matroidal network from a uniform matroid and any of its minor (Fig. 1.7).

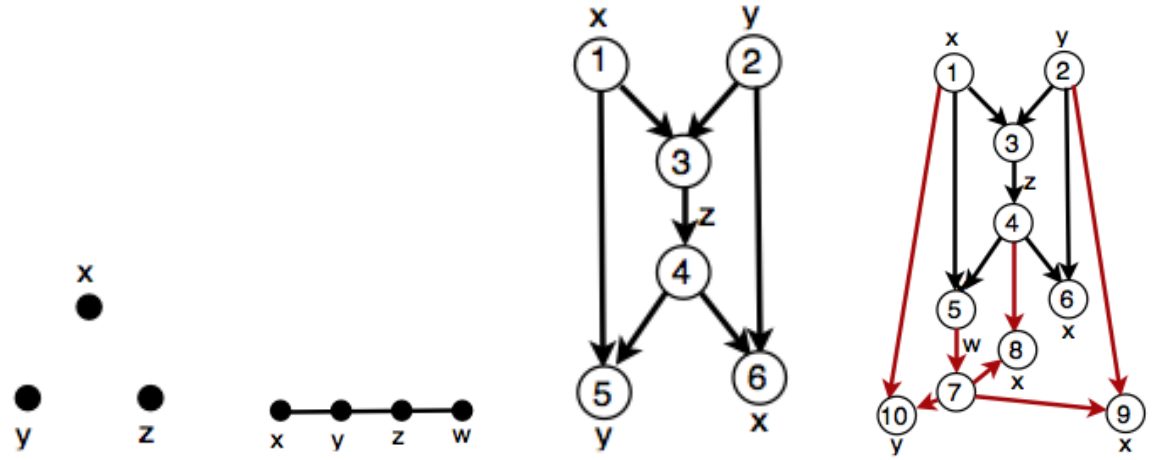
1.4 Structure Overview

In the rest of the thesis, Chapter 2 presents model and preliminaries, Chapter 3 is on related work, Chapter 4 is on uniform matroidal network construction, Chapter 5 is on whirl matroidal network construction, Sec. 6 is about Q_6 matroidal network, Chapter 7 shows the subnetwork property between matroidal networks from a uniform matroid and its minor,



(a) (b)

Figure 1.6: $\mathcal{W}^3$ matroidal network (a) and Q_6 matroidal network (b).



(a) $U_{2,3}$ matroid (b) $U_{2,4}$ matroid (c) $U_{2,3}$ matroidal network (d) $U_{2,4}$ matroidal network

Figure 1.7: $U_{2,3}$ matroid (a) is a minor of $U_{2,4}$ matroid (b) while $U_{2,3}$ matroidal network (c) is a subnetwork of $U_{2,4}$ matroidal network (d).

and Chapter 8 concludes the thesis.

Chapter 2

Model and Preliminaries

2.1 Definition and Notations

2.1.1 Network Basics

A *network* $\mathcal{N}$ is a finite, directed, acyclic multigraph, assigned with a finite set of messages and packets over an *alphabet* Σ. The network is *planar* if its underlying multigraph can be embedded into the 2-dimensional space without any edges crossing except at their endpoints, and *almost-planar* if it's planar after removing a certain edge. Each message originates from a *source node* and is requested by one or more *demand nodes*. Information about the messages is passed from node to node in the form of packets; each edge has capacity for transmitting one packet (per time unit). We assume all messages and packets contain the same number of alphabet symbols, or formally speaking, they are variables with domain Σ^k, where k is a positive integer and $|\Sigma| = q$.

Let us see an example of network coding, known as the *multiple-unicast butterfly* network, as illustrated in Fig. 2.1. The butterfly network was the first example to demonstrate the utility of network coding introduced by Ahlswede *et al.* [1]. It has no routing solution. But with $k = 1$ and any alphabet $\Sigma = \{0, 1, ..., a-1\} (a \geq 2)$, there is a simple coding solution. To see this, let node n_1 emit the message x along its two out-edges. At the same time, let node n_2 emit message y along its two out-edges. Next we will do encoding at node n_3 and emit $z = (x + y) \bmod a$, and n_4 will have no choice but to emit z along its two out-edges. Then, node n_5 will decode y from $y = (z - x) \bmod a$, and node n_6 will decode x from $x = (z - y) \bmod a$.

More generally, the set of *inputs* to a network node u, $\text{In}(u)$, contains packets on its in-

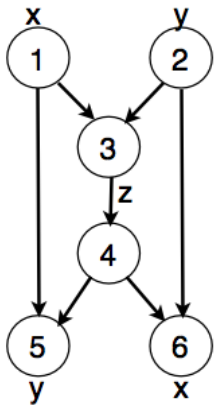


Figure 2.1: The *multiple-unicast butterfly* network. Node n_3 can do encoding and emit $(x + y)$ mod a where a is the size of the alphabet on which network coding is performed.

edges, together with messages generated locally at u. The set of *outputs* of u, $\mathrm{Out}(u)$, includes packets carried on its out-edges, together with messages demanded at u. Each output of a node is a function of its inputs. A *coding solution* for the network is an assignment of such functions, one for each output of each node, such that every demand node can recover its requested messages from its input. The solution is *linear* if Σ is a finite field $\mathbb{F}$ and the functions include only linear operations (Naturally the solution is called *nonlinear* if the functions are not on a finite field, or they are on a finite field but they contain nonlinear operations like square). It is further *scalar-linear* if $k = 1$ (All messages and packets contain just one alphabet symbol), and *vector-linear* if $k \geq 2$. A network is *scalar-linearly solvable* if it has a scalar-linearly solution, *vector-linearly solvable* if it has a vector-linear solution.

Let us see another example, which is not scalar-linearly solvable, but vector-routing solvable (i.e., it has a vector-linear solution with no need to do encoding), which is commonly known as the M-network, as illustrated in Fig. 2.2. This network is due to Koetter and was used by Medard *et al.* [9]. Their solution with $k = 2$ is as follows. Let Σ be any alphabet. Let $a = (a_1, a_2)$, $b = (b_1, b_2)$, $c = (c_1, c_2)$, $d = (d_1, d_2)$ denote the pairs of alphabet symbols for each message. Let the sources emit the packets

$$w_1 = (a_1, b_2), w_2 = (a_2, b_1), w_3 = (c_1, d_2), w_4 = (c_2, d_1)$$

and let node n_4 emit the packets

$$u_1 = (a_2, c_1), u_2 = (a_2, d_2), u_3 = (b_1, c_1), u_4 = (b_1, d_2)$$

. Nodes n_3 and n_5 have only one input so they just copy their input along each outgoing edge. Then nodes n_6, n_7, n_8, n_9 can easily reconstruct the messages they demand.

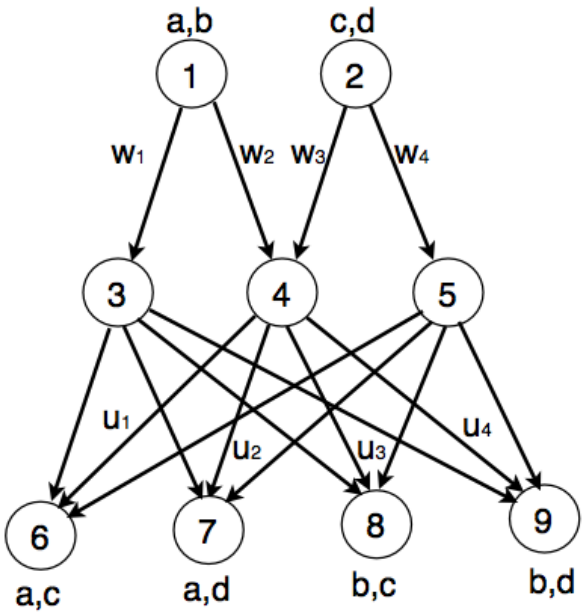


Figure 2.2: The M-network.

2.1.2 Matroid Basics and Definitions

A *matroid* $\mathcal{M}$ is an ordered pair $(\mathcal{S}, \mathcal{I})$, where $\mathcal{S}$ is a finite *ground set* and $\mathcal{I}$ is a set of subsets of $\mathcal{S}$ called *independent sets*, satisfing the following three conditions:

(I1) $\emptyset \in \mathcal{I}$

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

(I3) If $I, J \in \mathcal{I}$ and $|J| < |I|$, then there is an element e of $I \setminus J$ such that $J \cup \{e\} \in \mathcal{I}$.

A subset of $\mathcal{S}$ not in $\mathcal{I}$ is a *dependent set*. A maximal independent set is a *base* of the matroid, and a minimal dependent set is a *circuit*. An independent set is *maximal* if it becomes dependent by including any other element of $\mathcal{S}$. A dependent set is *minimal* if any of its proper subset is independent. All bases have the same size, which is the *rank* of $\mathcal{M}$, denoted as $r(\mathcal{S})$. The set of all bases or the set of all circuits can uniquely define a matroid. Specifically, if we have the set of all bases, or the set of all circuits, we can find all the dependent sets and independent sets of this matroid, and thus $\mathcal{S}$ and $\mathcal{I}$ of $\mathcal{M}$.

In this thesis, any $I \in \mathcal{I}$ is also called an *independence restriction*. In a circuit, each member is *dependent* on other members in the circuit. For example, if $\{a, b, c\}$ is a circuit in $\mathcal{M}$, then a is dependent on b, c (denoted as $a \leftarrow bc$, referred to as a *dependence restriction*). We also have $b \leftarrow ac$ and $c \leftarrow ab$ for circuit $\{a, b, c\}$ in $\mathcal{M}$, and in general a circuit C contains $|C|$ dependence restrictions.

Example 1: Consider a matroid $\mathcal{M}(\mathcal{S}, \mathcal{I})$ with $\mathcal{S} = \{x_1, x_2, x_3\}$ and $\mathcal{I} = \{\emptyset, \{x_1\}, \{x_2\}, \{x_3\}, \{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}\}$. We can easily verify that $\mathcal{I}$ satisfy the three conditions I1-I3. Any member $I \in \mathcal{I}$ is called an independent set or independence restriction. The bases of this matroid $\mathcal{M}$ are the following subsets of $\mathcal{S}$: $\{x_1, x_2\}$, $\{x_1, x_3\}$, $\{x_2, x_3\}$. $\{x_1, x_2, x_3\}$ is the only subset of $\mathcal{S}$ not in $\mathcal{I}$. As a result, it is the only dependent set and circuit of $\mathcal{M}$. $\mathcal{M}$ has three dependence restrictions: $x_1 \leftarrow x_2x_3$, $x_2 \leftarrow x_1x_3$. $x_3 \leftarrow x_1x_2$.

Another equivalent definition of matroid uses the notion of rank function. Now a matroid $\mathcal{M}$ can be defined as a pair $(\mathcal{S}, r)$ where $\mathcal{S}$ is the ground set and $r : 2^{\mathcal{S}} \rightarrow \mathbb{N}^+$ is the rank function. The rank function is a function r from subsets of $\mathcal{S}$ to nonnegative integers satisfying the follow three conditions.

- (R1) If $X \subseteq \mathcal{S}$, then $0 \leq r(X) \leq |X|$.
- (R2) If $X \subseteq Y \subseteq \mathcal{S}$, then $r(X) \leq r(Y)$.
- (R3) If $X, Y \subseteq \mathcal{S}$, then $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$.

We can see the connection between the two definitions as follows: For any $X \subseteq \mathcal{S}$, $r(X)$ is the size of any maximal independent subset of X. It's easy to show using (I3) that all such subsets have the same size. All subsets having $r(X) = |X|$ are independent sets. So we can reconstruct the $\mathcal{I}$ in the first definition from the r in the second definition by letting $\mathcal{I} = \{X \subseteq S : r(X) = |X|\}$. For any basis B, it holds that $r(B) = |B| = r_{\mathcal{M}}$. For each element c of a circuit C, it holds that $r(C \setminus \{c\}) = |C| - 1 = r(C)$. We define $\mathfrak{B}(\mathcal{M})$ to be the set of all bases of the matroid and $\mathfrak{C}(\mathcal{M})$ to be the set of all circuits.

Example 2: We can define the matroid from Example 1 in the notion of the second definition. The ground set is still $\mathcal{S} = \{x_1, x_2, x_3\}$. Function r can be defined as follows:

$$r(\emptyset) = 0, r(\{x_1\}) = 1, r(\{x_2\}) = 1, r(\{x_3\}) = 1,$$

$$r(\{x_1, x_2\}) = 2, r(\{x_1, x_3\}) = 2, r(\{x_2, x_3\}) = 2, r(\{x_1, x_2, x_3\}) = 2.$$

A well-known class of matroids arises from linear algebra. Let A be an $m \times n$ matrix over a field $\mathbb{F}$. Let $\mathcal{S} = \{1, ..., n\}$ and $X \subseteq \mathcal{S}$. If the columns indexed by X are linearly independent over $\mathbb{F}$, then $X \in \mathcal{I}$. The pair $(\mathcal{S}, \mathcal{I})$ forms a *vector matroid* of A, denoted as $\mathcal{M}[A]$. Two matroids $(\mathcal{S}, \mathcal{I})$ and $(\mathcal{S}', \mathcal{I}')$ are *isomorphic* if there is a bijection $f : \mathcal{S} \to \mathcal{S}'$ such that $I \in \mathcal{I}$ if and only if $f(I) \in \mathcal{I}'$. If a matroid $\mathcal{M}$ is isomorphic to the vector matroid associated with some matrix A over a field $\mathbb{F}$, then $\mathcal{M}$ is said to be *representable over* $\mathbb{F}$ and A is said to be a representation of $\mathcal{M}$.

Example 3: Let $A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ with elements from $\mathbb{F}_2$. Then the matroid $\mathcal{M}[A]$ is defined as the pair $(\mathcal{S}, \mathcal{I})$ where the ground set $\mathcal{S} = \{1, 2, 3\}$ and independent sets $\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$. We can say $\mathcal{M}[A]$ is representable over $\mathbb{F}_2$ and A is a representation of $\mathcal{M}[A]$.

There is a more general definition of matroid representation called *multilinear representation* [16] [17]. It can be described in the following two definitions. *Definition 1*: Let $\mathcal{S} = \{y_1, ..., y_m\}$ be a set whose elements are indexed by the integers from 1 to m. For

any collection of m matrices $M_1, ..., M_m \in \mathbb{M}_{\mathbb{F}}(n, k)$ (All matrices of dimension $n \times k$ with elements in field $\mathbb{F}$), and any subset $I = \{y_{i_1}, ..., y_{i_\delta}\} \subseteq \mathcal{S}$, with $i_1 < ... < i_\delta$, define

$$M_I = [M_{i_1}|...|M_{i_\delta}] \in \mathbb{M}_{\mathbb{F}}(n, \delta k)).$$

That is the matrix M_I obtained by concatenating the matrices $M_{i_1}, ..., M_{i_\delta}$ from left to right in the increasing order of the indices $i_1, ..., i_\delta$.

Definition 2: Let $\mathcal{M}(\mathcal{S}, r)$ be a matroid of rank $r_{\mathcal{M}} = k$ with ground set $\mathcal{S} = \{y_1, ..., y_m\}$. The matroid $\mathcal{M}$ is said to have a multi-linear representation of dimension n, or an n-linear representation over a field $\mathbb{F}$, if there exist matrices $M_1, ..., M_m \in \mathbb{M}_{\mathbb{F}}(kn, n)$ such that

$$rank(M_I) = n \times r(I), \forall I \subseteq \mathcal{S}.$$

The definition of representation above corresponds to the case when $n = 1$. Note that there exist matroids that are not representable over any finite field $\mathbb{F}$, but multilinearly reprepresentable over a field $\mathbb{F}$.

Example 4: We can verify that the matroid representation A from Example 3 exactly corresponds to our definition of multilinear representation of dimension 1, by just setting $M_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, M_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, M_3 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.. We can also find a multilinear representation of dimension 2 for the same matroid $\mathcal{M}[A]$ in Example 3. For example, we can set

$$M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, M_2 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}, M_3 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

Matroids of small rank are often depicted geometrically. For example, a matroid of rank 3 can be represented by a figure in which marked points are ground set elements, with any two distinct points giving a size-2 independent set in the matroid. Three points in the figure represent an independent set *iff* they are not collinear. Sometimes the figure will indicate

that certain curved lines are also to be treated as dependent sets, such as the circle in the geometric depiction of the Fano matroid.

2.2 Special Matroids

An important class of matroids is the family of *uniform matroids* $U_{r,n}$ [8]. The ground set of $U_{r,n}$ is the set $\{1, ..., n\}$, and a subset of the ground set is independent *iff* it has size at most r. So the rank of $U_{r,n}$ is r. All subsets of size r are bases, and all subsets of size $r+1$ are circuits.

Example 5: Consider the case of $U_{2,4}$, which has the ground set $\{1, 2, 3, 4\}$. The set of independent sets is $\{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$. The set of circuits is $\{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}\}$.

Another class of matroids is the family of *Whirl matroids* $\mathcal{W}^n$ [8]. The ground set of $\mathcal{W}^n$ is $\{a_1, a_2, ..., a_n, b_1, b_2, ..., b_n\}$. The set of all circuits is the union of the following four sets: $1)\{b_i, b_{i+1}, a_i\}, i = 1, 2, ..., n$; $2)\{b_i,\ b_{i+2},\ a_i,\ a_{i+1}\},\ i = 1, 2, ..., n$; $3)\{b_i,\ b_{i+1}\} \cup \{a_1, a_2, ..., a_n\} \setminus \{a_i\}, i = 1, 2, ..., n$; $4)\{a_1, a_2, ..., a_n, b_i\}, i = 1, 2, ..., n$. $a_i,\ b_i$ will roll back when $i > n (i.e., a_{n+1} = a_1, a_{n+2} = a_2)$. All whirl matroids are representable over a finite field $\mathbb{F}_q$ *iff* $q \geq 3$.

Example 6: Consider the case of $\mathcal{W}^2$ with ground set $\{a_1, a_2, b_1, b_2\}$. The set of circuits include: $1)\{b_1, b_2, a_1\},\ \{b_2, b_1, a_2\}$; $2)\{b_1, a_1, a_2\},\ \{b_2, a_2, a_1\}$; $3)\{b_1, b_2, a_2\},\ \{b_2, b_1, a_1\}$; $4)\{a_1, a_2, b_1\}, \{a_1, a_2, b_2\}$. After deleting duplicates, we can find the set of circuits is $\{\{a_1, a_2, b_1\}, \{a_1, a_2, b_2\}, \{a_1, b_1, b_2\}, \{a_2, b_1, b_2\}\}$.

We can find all matroids we discussed from Example 1 to Example 4 are isomorphic to $U_{2,3}$ (Geometrically depicted in Fig. 2.3(a)), and $\mathcal{W}^2$ is isomorphic to $U_{2,4}$ (Geometrically depicted in Fig. 2.3(b)).

(a) $U_{2,3}$ (b) $U_{2,4}$.

Figure 2.3: Geometric depictions of $U_{2,3}$ and $U_{2,4}$ matroids.

Chapter 3

Related Work

The relationship between network coding and matroid theory was first proposed by Dougherty *et al.* [5]. They first introduced the definition of a matroidal network and showed that the scalar linear solvability of a network coding problem is related to the existence of a representable matroid satisfying certain properties. The D-F-Z method was proposed to construct a network from a matroid such that for certain matroids, the resulting network is scalar-linearly solvable *iff* the network is matroidal over the some field. This method is not general enough to handle all matroids. It also suffers from a very high time complexity due to the indeterminism of the method. The connection between network coding and matroid theory was further developed and strengthened later [3], [12]-[14], especially by El Rouayheb *et al.* [3]. They used index coding to connect the network coding problem with the matroid representability problem, thus arriving at a method (the E-S-G method) to fully handle all matroids. However the resulting network suffers from a very complex graph structure. We now describe the definition of matroidal network, the D-F-Z method and the E-S-G method in the next three sections respectively.

3.1 Matroidal Network Definition

Let $\mathcal{N}$ be a network with message set M and packet set P. Let $\mathcal{M} = (\mathcal{S}, \mathcal{I})$ be a matroid with rank function r. A *network-matroid mapping* from $\mathcal{N}$ to $\mathcal{M}$ is a function $f : M \cup P \to \mathcal{S}$ such that the following conditions are satisfied.

(M1) $f|M$ is one-to-one.

(M2) $f(M) \in \mathcal{I}$.

(M3) $r(f(In(n))) = r(f(In(n) \cup Out(n)))$, for every node n.

Conditions (M1) and (M2) reflect that the messages of the network are independent while (M3) is a reflection of the network dependencies. When such a mapping exists, we say that the network $\mathcal{N}$ is *matroidal over* $\mathcal{M}$ and we also say that $\mathcal{N}$ is a *matroidal* network. However, the matroid witnessing that a particular network is matroidal needs not be unique.

As an example, let us see the fact that the multiple-unicast butterfly network is matroidal over the uniform matroid $U_{2,3}$. As introduced in Sec. 2.2, $U_{2,3}$ has ground set $\{1, 2, 3\}$, and a subset of the ground set is independent if and only if it has size at most 2. To see a network-matroid mapping, let f assign the element 1 to the message x, which originates at node n_1 and also to the two packets emanating from node n_1. Let f assign the element 2 to the message y, and also to the packets emanating from node n_2. The three remaining packets are assigned the element 3. The conditions (M1) and (M2) are easily checked. To see (M3), note that $f(In(n)) = f(In(n) \cup Out(n))$ for nodes $n = n_1, n_2, n_4$. At each of the other nodes, $n = n_3, n_5, n_6$, $f(In(n) \cup Out(n)) = \{1, 2, 3\}$, which has rank 2 while $f(In(n))$ has size two and is therefore independent and therefore also has rank 2. The rank values on the subset of the ground set $\{1, 2, 3\}$ can be easily checked from Example 2 in Sec. 2.1.2. In all the matroidal networks drawn below, matroid ground set elements will be labeled on the network according to f, instead of the actual messages and packets.

It has been proved that a network is scalar-linearly solvable over some finite field *if and only if* the network is matroidal over a representable matroid [5, 12]. So if we want to obtain a network that is not scalar-linearly solvable, we can just construct a network that is matroidal over a nonrepresentable matroid, such as the Vamous matroid.

3.2 The D-F-Z method

3.2.1 Method Description

Let $\mathcal{M} = (\mathcal{S}, \mathcal{I})$ be a matroid with rank function r. Let $\mathcal{N}$ denote the network to be constructed, with message set M, node set N, and packet set P. The construction simultaneously constructs the network $\mathcal{N}$, the function $f : M \cup P \to \mathcal{S}$, and an auxiliary function $g : \mathcal{S} \to N$, where for each $x \in \mathcal{S}$, 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 incoming packet p satisfies $f(p) = x$.

The construction is carried out in four stages; each stage can be completed in many ways. We'll first describe the entire construction and then illustrate the $U_{2,4}$ matroidal network as an example.

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

Step 2) (To be repeated until it's no longer possible.) Find a circuit $\{x_0, ..., x_j\}$ in $\mathcal{M}$, such that $g(x_1), ..., g(x_j)$ have already been defined, but $g(x_0)$ has not yet been defined. Then we'll add the following.

i) a new node y, edges $e_1, ..., e_j$, and corresponding packets $p_1, ..., p_j$, such that e_i connects $g(x_i)$ to y, and we define $f(p_i) = x_i$.

ii) Another new node n_0 with a single in-edge e_0 and corresponding packet p_0, connecting y to n_0, and we let $f(p_0) = x_0$ and $g(x_0) = n_0$.

Step 3) (To be repeated as many times as desired.) If $\{x_0, ..., x_j\}$ is a circuit in $\mathcal{M}$ and $g(x_0)$ is a source node with message m_0, then add to the network a new demand

node y, which demands the message m_0 and which has in-edges $e_1, ..., e_j$ with corresponding packets $p_1, ..., p_j$ where e_i connects $g(x_i)$ to y and where $f(p_i) = x_i$.

Step 4) (To be repeated as many times as desired.) Choose a base $B = \{x_1, ..., x_{r(\mathcal{S})}\}$ of $\mathcal{M}$ and create a demand node y that demands all of the network messages, and such that y has in-edges $e_1, ..., e_{r(\mathcal{S})}$ with corresponding packets $p_1, ..., p_{r(\mathcal{S})}$ where e_i connects $g(x_i)$ to y. Let $f(p_i) = x_i$.

3.2.2 Discussion

For Step 2 and Step 3 of the method above, we can verify that in each repetition, only one dependence restriction of the circuit involved is explicitly enforced in the resulting network. The method also needs to "repeat as many times as desired" for Step 3 and 4. As a result, the number of iterations, and in each iteration which dependence and independence restriction should be used, are undetermined. As the number of dependence and independence can be exponential on the size of the ground set n, this method has an exponential time complexity.

The undeterminism of the set of dependence and independence restrictions that should be explicitly transferred reduces the size of resulting network. However, it also makes the time complexity of the method exponential. If we can find more characteristics of this set, we can reduce the time complexity substantially while keeping the resulting network small in size. In the next chapter, we will introduce the technique of dependence deduction and see how it can be applied to find the characteristics we want.

3.3 The E-S-G method

The E-S-G method reduces the complexity of constructing a network from a matroid to polynomial. This method uses index coding as an intermediate step. Specifically, this method first converts a matroid $\mathcal{M}(\mathcal{S}, r)$ into an index coding problem. Then it converts the

index coding problem into a network coding problem. At the same time, the entire process guarantees the property that the matroid $\mathcal{M}$ has an n-linear representation over $\mathbb{F}_q$ *iff* the network $\mathcal{N}(\mathcal{I}_{\mathcal{M}})$ has an vector linear network code of dimension n over $\mathbb{F}_q$. We will describe the index coding problem, the E-S-G method, and an example in the next three subsections respectively.

3.3.1 The Index Coding Problem

Index coding utilizes the broadcast nature of wireless communication. It includes a single sender node s and a set R of receiver nodes. The sender has a set of information messages that need to be delivered to the receiver nodes. Each receiver needs to obtain a single message and has prior *side information*. The sender can broadcast the encoding of the messages to the receivers through a noiseless channel that can transmit one message per channel use. The objective is to find an optimal encoding scheme, referred to as an *index code*, that satisfies all the receiver nodes with zero-error and with minimum number of transmissions. A simple example is shown as in Fig. 3.1.

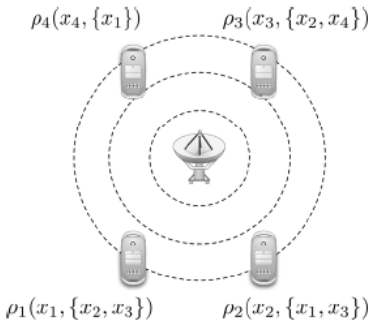


Figure 3.1: An instance of the index coding problem with four messages and four clients. The transmission of two messages $x_1 + x_2 + x_3$ and $x_1 + x_4$ will be enough for the four clients. Each client is labelled with its desired message, and its side information.

Formally, an instance of the index coding problem $\mathcal{I}(X, R)$ includes:

1) A set of k messages $X = \{x_1, ..., x_k\}$,

2) A set of clients or receivers $R = \{(x, H); x \in X, H \subseteq X \setminus \{x\}\}$.

Here, X represents the set of messages available at the sender. Each message x_i belongs to a certain alphabet $\sum^n$, where $|\sum| = q$. A client is represented by a pair (x, H), where $x \in X$ is the message demanded by the client, and $H \subseteq X \setminus \{x\}$ is set of messages available to the client as side information. Note in this mode, each node requests exactly one message. Each message x_i can be divided into n packets, each belonging to the finite q-ary alphabet $\sum$, and we write $x_i = (x_{i1}, ..., x_{in} \in \sum^n)$. We define $\xi = (x_{11}, ..., x_{1n}, ..., x_{k1}, ..., x_{kn}) \in \sum^{nk}$.

Definition 3: An (n, q) index code for $\mathcal{I}(X, R)$ is a function $f : \sum^{nk} \to \sum^c$, for a certain integer c, satisfying that for each client $\rho = (x, H) \in R$, there exists a function $\psi_\rho : \sum^{c+n|H|} \to \sum^n$ such that $\psi_\rho(f(\xi), (x_i)_{x_i \in H}) = x, \forall \xi \in \sum^{nk}$.

3.3.2 E-S-G Method Description

The E-S-G method contains two steps. First we convert a matroid $\mathcal{M}(\mathcal{S}, r)$ into an index code problem. Then we convert the index coding problem into a network coding problem.

Step 1) For a matroid $\mathcal{M}(\mathcal{S}, r)$ of rank k over a ground set $\mathcal{S} = \{y_1, ..., y_m\}$, we define the corresponding index coding problem $\mathcal{I}_\mathcal{M}(Z, R)$ as follows:

1) $Z = \mathcal{S} \cup X$, where $X = \{x_1, ..., x_k\}$;

2) $R = R_1 \cup R_2 \cup R_3$ where

a) $R_1 = \{(x_i, B); B \in \mathfrak{B}(\mathcal{M}), i = 1, ..., k\}$

b) $R_2 = \{(y, C \setminus \{y\}); C \in \mathfrak{C}(\mathcal{M}), y \in C\}$

c) $R_3 = \{(y_i, X); i = 1, ..., m\}$.

Step 2) Let $\mathcal{I}_\mathcal{M}(Z, R)$ be the resulting index coding problem from Step 1. We associate to it the 6-partite network $\mathcal{N}(\mathcal{I}_\mathcal{M})$ constructed as follows:

1) $V \supset V_1 \cup V_2 \cup V_3$, where $V_1 = \{s_1, ..., s_{m+k}\}, V_2 = \{n'_1, ..., n'_m\}$, and $V_3 = \{n''_1, ..., n''_m\}$.

2) Connect each node $s_i, i = 1, ..., k$, to an input edge carrying an information source x_i at its tail node, and each node $s_i, i = k+1, ..., m+k$, to an input edge carrying an information source y_{i-k}.

3) Add edges (s_i, n'_j), for $i = 1, ..., m+k$ and $j = 1, ..., m$.

4) Add edges (n'_j, n''_j), for $j = 1, ..., m$.

5) For each client $\rho = (z, H) \in R$, add a vertex n_ρ to the network, and connect it to an output edge that demands source z. And, for each $z' \in H$, add edge (s', n_ρ), where $s' \in V_1$ is connected to an input edge carrying source z'.

6) For each $\rho \in R$, add edge (n''_j, n_ρ), for $j = 1, ..., m$.

3.3.3 Example

We can apply the E-S-G method on the uniform matroid $U_{2,3}$ and convert it into a network coding problem.

Formally, $\mathcal{M}(\mathcal{S}, r) = U_{2,3}$ has ground set $\mathcal{S} = \{y_1, y_2, y_3\}$. It has rank $k = 2$. The set of all bases $\mathfrak{B}(\mathcal{M}) = \{\{y_1, y_2\}, \{y_1, y_3\}, \{y_2, y_3\}\}$. The set of all circuits $\mathfrak{C}(\mathcal{M}) = \{\{y_1, y_2, y_3\}\}$. So according to Procedure 1, we can derive the corresponding index coding problem $\mathcal{I}_{\mathcal{M}}(Z, R)$ as follows:

1) $Z = \mathcal{S} \cup X$, where $X = \{x_1, x_2\}$

2) $R = R_1 \cup R_2 \cup R_3$ where

   a) $R_1 = \{(x_i, B); B \in \mathfrak{B}(\mathcal{M}), i = 1, 2\}$

   b) $R_2 = \{(y_i, C \setminus \{y_i\}); C \in \mathfrak{C}(\mathcal{M}), i = 1, 2, 3\}$

   c) $R_3 = \{(y_i, X); i = 1, 2, 3\}$.

Given $\mathcal{I}_{\mathcal{M}}(Z, R)$, we next apply Step 2 and obtain the corresponding network $\mathcal{N}(\mathcal{I}_{\mathcal{M}})$, as shown in Fig. 3.2.

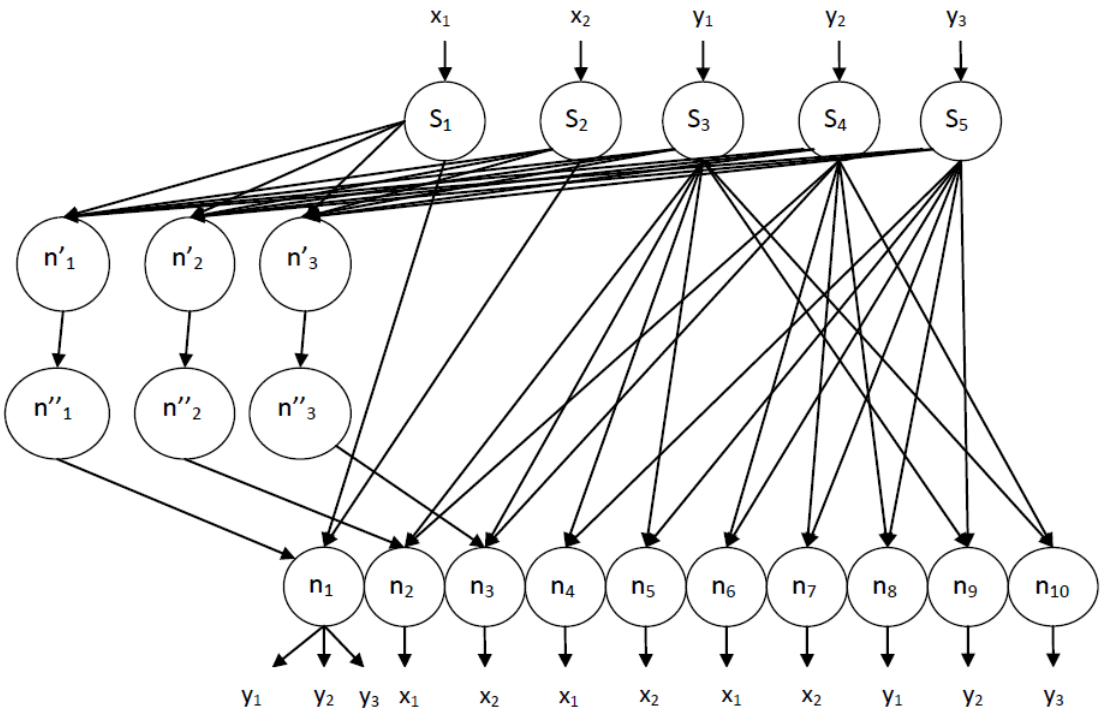


Figure 3.2: Part of the network corresponding to $U_{2,3}$. The edges from n_j'' to all the receivers are not fully shown. We can see that R_1 includes the receivers from n_2 to n_7, R_2 includes the receivers from n_8 to n_{10}, R_3 includes the receiver n_1

We can simplify the structure of an E-S-G matroidal network slightly. More specifically, we can remove some edges and merge some nodes without affecting the network information flow and the resulting code construction. Formally speaking, we can remove all input edges and output edges. Instead we can turn a node connected to an input edge into a source node and a node connected to an output edge into a receiver node. We can also combine some receiver nodes if they have connections to the same set of nodes. Let's take the $U_{2,3}$ matroidal network in Fig. 3.2 as an example. The simplified network is illustrated in Fig. 1.4(b).

Chapter 4

Uniform Matroidal Networks

We now describe the construction of uniform $U_{r,n}$ matroidal networks, describe dependence deduction of $U_{2,n}$ ($U_{r,n}$ when $r = 2$) matroidal networks, and prove that $U_{2,n}$ networks are scalar-linearly solvable over $\mathbb{F}_q$ *iff* $q \geq n - 1$, in the next three sections respectively.

4.1 Network Construction from Uniform Matroids

4.1.1 Method Description

Let $\mathcal{N}$ denote the network to be constructed, with message set M, node set N, and packet set P. The uniform matroid is $U_{r,n}$ $(r \geq 2,\ n \geq r + 1) = \mathcal{M}(\mathcal{S}, \mathcal{I})$, with ground set $\mathcal{S} = \{x_1, x_2, ..., x_n\}$. We simultaneously construct the network $\mathcal{N}$, a function $f : M \cup P \to \mathcal{S}$, and a function $g : \mathcal{S} \to N$, where for each $x \in \mathcal{S}$, either

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

ii) $g(x)$ is a node with in-degree 1, with incoming packet p satisfying $f(p) = x$.

Constructing $U_{r,n}$ Matroidal Networks. The construction consists of 3 steps:

1) Create source nodes $n_1, n_2, ..., n_r$ and corresponding messages $m_1, m_2, ..., m_r$. Choose any base $B = \{b_1, b_2, ..., b_r\}$ in $\mathcal{M}$ and let $f(m_i) = b_i$ and $g(b_i) = n_i$.

2) (Repeat $n - r$ times:) In the ith ($1 \leq i \leq n - r$) iteration, find a dependence restriction $x_0 \leftarrow x_1x_2...x_r$ from a circuit $\{x_0, x_1, x_2, ..., x_r\}$ in $\mathcal{M}$, such that $g(x_1), g(x_2), ..., g(x_r)$ have been defined but $g(x_0)$ has not, and $x_1x_2...x_r$ has not appeared on the right side of the dependence restrictions used in all $1 \leq j \leq i - 1$ iteration(s). Then add the following nodes and edges:

i) a node y, edges $e_1, e_2, ..., e_r$, and corresponding packets $p_1, p_2, ..., p_r$, such that e_i connects $g(x_i)$ to y, and we define $f(p_i) = x_i$.

ii) a node n_0 with a single in-edge e_0 and corresponding packet p_0, connecting y to n_0, and we let $f(p_0) = x_0$ and $g(x_0) = n_0$.

3) (Repeat $\binom{n}{r} - (n-r)$ times:) In the ith iteration, find a dependence restriction $x_0 \leftarrow x_1 x_2 ... x_r$ from a circuit $\{x_0, x_1, x_2, ..., x_r\}$ in $\mathcal{M}$, such that $g(x_0)$ is a source node with message m_0, and $x_1 x_2, ..., x_r$ has not appeared on the right side of the dependence restrictions used in all $1 \leq j \leq i-1$ iteration(s) and Step 2. Add a demand node y that requests message m_0, with in-edges $e_1, e_2, ..., e_r$ and corresponding packets $p_1, p_2, ..., p_r$, where e_i connects $g(x_i)$ to y and $f(p_i) = x_i$.

4.1.2 The $U_{2,4}$ Example

We next use $U_{2,4}$ as an example to illustrate the construction process.

Example: Constructing The $U_{2,4}$ Matroidal Network. Consider $U_{2,4} = \mathcal{M}(\mathcal{S}, \mathcal{I})$, with ground set $\mathcal{S} = \{x_1, x_2, x_3, x_4\}$. All size-2 subsets of $\mathcal{S}$ are bases; all size-3 subsets are circuits.

1) Create source nodes n_1, n_2 with messages m_1, m_2. Choose base $B = \{x_1, x_2\}$, let $f(m_i) = x_i, g(x_i) = n_i, i = 1, 2$ (Fig. 4.1). Ground set elements are labelled according to function f.

Figure 4.1: Partial $U_{2,4}$ network after Step 1.

2) Choose dependence restriction $x_3 \leftarrow x_1x_2$ from circuit $\{x_1, x_2, x_3\}$ in $U_{2,4}$. For Step 2(i), add a node n_3, edges $e_{1,3}$ from n_1 to n_3 and $e_{2,3}$ from n_2 to n_3, and corresponding packets $p_{1,3}$ and $p_{2,3}$. Let $f(p_{1,3}) = x_1, f(p_{2,3}) = x_2$. For Step 2(ii), add a node n_4 with a single in-edge $e_{3,4}$ and packet $p_{3,4}$, connecting n_3 to n_4, and let $f(p_{3,4}) = x_3$ and $g(x_3) = n_4$. Repeat the above procedure for $x_4 \leftarrow x_1x_3$ (Fig. 4.2).

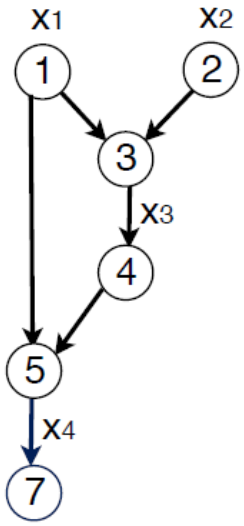


Figure 4.2: Partial $U_{2,4}$ network after Step 2.

3) Choose $x_1 \leftarrow x_2x_3$ from the circuit $\{x_1, x_2, x_3\}$ in $U_{2,4}$, because $g(x_1) = n_1$ is a source node with message m_1, and x_2x_3 has not appeared in previously used dependence restrictions ($x_3 \leftarrow x_1x_2, x_4 \leftarrow x_1x_3$). Add a demand node n_6, which demands message m_1 and has in-edges $e_{2,6}, e_{4,6}$ with corresponding packets $p_{2,6}, p_{4,6}$. $e_{2,6}$ connects $g(x_2)$ to n_6. $e_{4,6}$ connects $g(x_3)$ to n_6. Set $f(p_{2,6}) = x_2$ and $f(p_{4,6}) = x_3$. Repeat the above procedure for another 3 times when choosing $x_2 \leftarrow x_1x_4$, $x_1 \leftarrow x_2x_4$, $x_1 \leftarrow x_3x_4$. The resulting network is shown in Fig. 4.3.

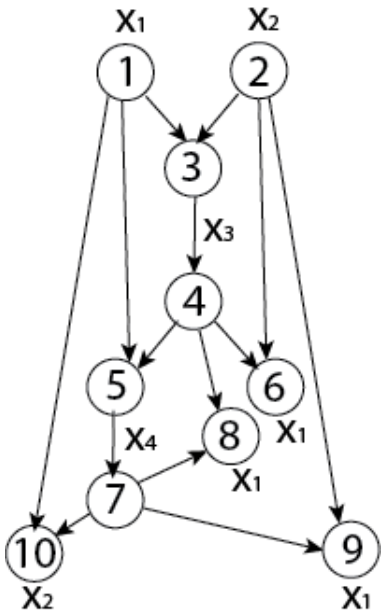


Figure 4.3: Complete $U_{2,4}$ network after Step 3. Smallest known network requiring $\mathbb{F}_3$.

4.1.3 Discussions

We can prove that the smallest field size for the $U_{2,4}$ matroidal network to have a scalar-linear solution is 3. As $U_{2,4}$ is only representable over $\mathbb{F}_q$ when $q \geq 3$, the $U_{2,4}$ matroidal network we constructed is "correct" in the sense that it satisfies the condition that the output network is scalar-linearly solvable over a field $\mathbb{F}_q$ *iff* the matroid is representable over $\mathbb{F}_q$. In fact, we can prove the above construction has used a just right number of dependence restrictions, and hence the network can not be simpler to be still correct — any smaller number of dependence restrictions will result in a network solvable over $\mathbb{F}_2$. If we use more dependence restrictions by repeating Step 3 more than the specified number of times, the resulting network is still scalar-linearly solvable over $\mathbb{F}_3$, but is unnecessarily complex.

How can the 6 dependence restrictions used ($x_3 \leftarrow x_1x_2$, $x_4 \leftarrow x_1x_3$, $x_2 \leftarrow x_1x_4$, $x_1 \leftarrow x_2x_3$, $x_1 \leftarrow x_2x_4$, $x_1 \leftarrow x_3x_4$) be sufficient to derive the necessity of $\mathbb{F}_3$ in the $U_{2,4}$ matroidal network? As a matroid can be uniquely defined by its set of circuits (dependence restrictions in network construction), in order to make sure that a matroid is representable over a finite field $\mathbb{F}$ *iff* the corresponding network is scalar-linearly solvable over $\mathbb{F}$, the net-

work should reflect all the dependence restrictions from the matroid. Hence the network construction should enforce all the dependence restrictions of the matroid. In constructing the $U_{2,4}$ matroidal network, only 6 out of 12 dependence restrictions are explicitly enforced in the network. We prove in Sec. 4.2 that the other 6 are indeed enforced in the network implicitly. The right side of the 6 explicitly enforced dependence restrictions are all different from each other, and actually form the set of all bases — that is why Step 3 is repeated $\binom{n}{r} - (n-r)$ times.

For general r and n, the representability of $U_{r,n}$ has not been determined [8]. We therefore focus on $U_{2,n}(n \geq 3)$ that is known to be representable over $\mathbb{F}_q$ *iff* $q \geq n-1$. Sec. 4.2 proves that for $U_{2,n}$, this set of $\binom{n}{2}$ dependence restrictions with the right sides forming the set of bases can indeed deduce all the $3 \times \binom{n}{3}$ dependence restrictions, and it is the minimum set of dependence restrictions with this property, thus resulting the smallest network size possible.

4.2 Dependence Deduction of $U_{2,n}$ Matroidal Networks

We first explain how to deduce dependence restrictions from explicitly enforced dependence and independence restrictions. The following two rules are proved to be correct and can be used for guiding such deduction. All x_i's are ground set elements.

(R1) If $x_1 \leftarrow x_2 ... x_n$, and $\{x_1, x_2, ..., x_{n-1}\}$ is an independence restriction, then $x_n \leftarrow x_1 x_2 ... x_{n-1}$.

(R2) If $x_1 \leftarrow x_2 x_3 ... x_n$ and $x_n \leftarrow x_{n+1} x_{n+2} ... x_{n+m}$, then $x_1 \leftarrow x_2 x_3 ... x_{n-1} x_{n+1} ... x_{n+m}$. Duplicate x_is on the right side can be eliminated. If there is already $x_i \leftarrow x_j x_k, i, j, k \in \{2, 3, ..., n-1, n+1, ..., n+m\}$, we can also eliminate the x_i on the right side.

Let $S = \{x_1, x_2, ..., x_n\}(n \geq 3)$ be the ground set of $U_{2,n}$. The construction in Sec. 4.1.1 may lead to non-unique matroidal networks for $U_{2,n}$, but they all have the same size, since

the same number of dependence restrictions are used in their constructions. A particular process for $U_{2,n}$ matroidal network construction works as follow.

1) Create source nodes n_1, n_2 with messages m_1, m_2 according to the base $B = \{x_1, x_2\}$.

2) Create intermediate nodes by apply the following $n-2$ dependence restrictions, for all $3 \leq k \leq n, x_k \leftarrow x_1 x_{k-1}$, sequentially from $k = 3$ to $k = n$.

3) Create demand nodes to demand m_2 based on $x_2 \leftarrow x_1 x_n$, and m_1 based on the dependence restrictions, for all $2 \leq i \leq n-1, i+1 \leq j \leq n, x_1 \leftarrow x_i x_j$.

Theorem 1. In the $U_{2,n}(n \geq 3)$ matroidal network from the above construction, we can deduce all the dependence restrictions of $U_{2,n}$.

Proof. : We have ground set $S = \{x_1, x_2, ..., x_n\}$, independence restriction $\{x_1, x_2\}$, and dependence restrictions: (1) for all $3 \leq k \leq n, x_k \leftarrow x_1 x_{k-1}$, (2) $x_2 \leftarrow x_1 x_n$, (3) for all $2 \leq i \leq n-1, i+1 \leq j \leq n, x_1 \leftarrow x_i x_j$. We want to prove, for all size-3 subsets $\{x_i, x_j, x_k\}$ of S, $x_i \leftarrow x_j x_k, x_j \leftarrow x_i x_k, x_k \leftarrow x_i x_j$. First, we can apply R2 on (2) and (1) sequentially (replace the x_n in (2) with the right side of $x_n \leftarrow x_1 x_{n-1}$, then replace x_{n-1} with the right side of $x_{n-1} \leftarrow x_1 x_{n-2}$), we can obtain for all $2 \leq i \leq n, x_2 \leftarrow x_1 x_i$. Similarly, applying R2 on (3) and (1), we have for all $3 \leq j \leq n, x_j \leftarrow x_{j-1} x_k, k \in \{1, 2, ..., n\} \setminus \{j-1\}$. Replacing all the x_1s of $x_2 \leftarrow x_1 x_i$ with the right side of (3), we obtain all the dependence restrictions $x_2 \leftarrow x_i x_j$. Then recursively, replacing all the x_2s of $x_3 \leftarrow x_2 x_i$ with the right side of $x_2 \leftarrow x_i x_j$ we get all the dependence restrictions $x_3 \leftarrow x_i x_j$. Conduct the recursion until all dependence restrictions $x_n \leftarrow x_i x_j$ are obtained. Then after deleting duplicate x_is and selecting dependence restrictions of the form $x_i \leftarrow x_j x_k$ with distinct i, j and k, we can conclude that for all size-3 subsets of S, each member is dependent on the other two. □

Theorem 2. The set of dependence restrictions used during the $U_{2,n}(n \geq 3)$ matroidal network construction is minimum, for deducing complete $U_{2,n}$ dependence restrictions.

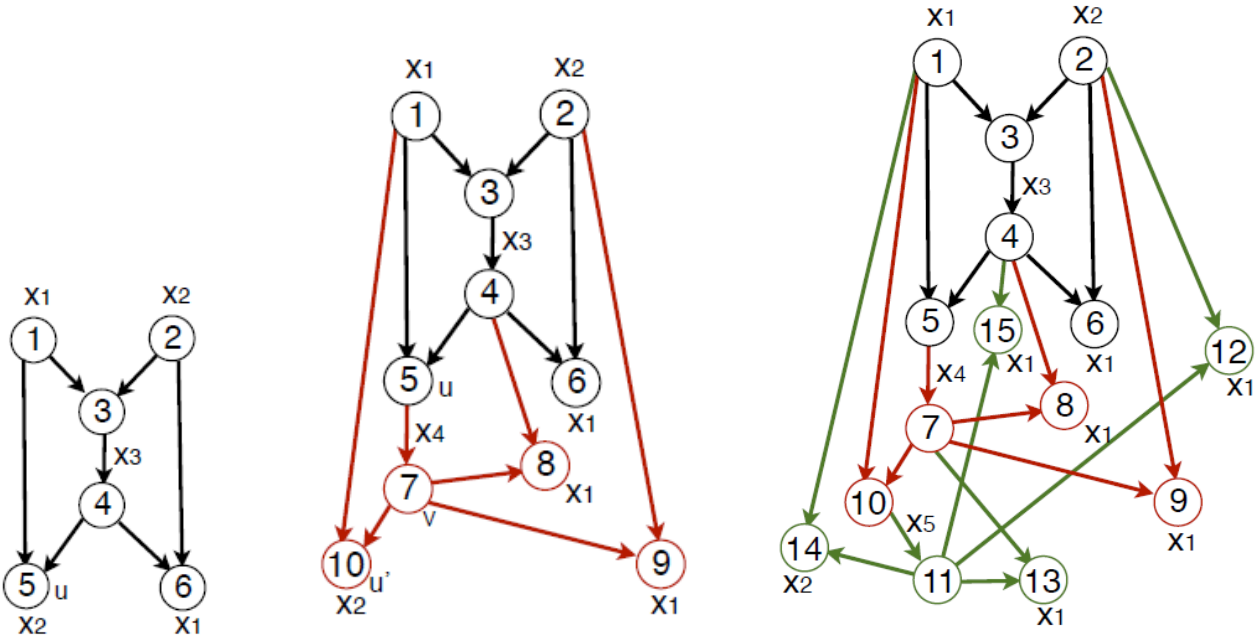
Proof. In constructing the $U_{2,n}$ network, we used $\binom{n}{2}$ dependence restrictions. Their right sides form the set of all bases. In total we wish to deduce $3 \times \binom{n}{3}$ dependence restrictions, which can be grouped into $\binom{n}{2}$ sets based on their right side. If any single dependence restriction $x_i \leftarrow x_j x_k$ is missed, we will not be able to deduce the dependence restriction set that has the right side as $x_j x_k$, because the rule set available can not enable us to deduce any dependence restriction with a size-2 right side different from the input dependence restrictions in this case. Therefore, the set of dependence restrictions we have applied is the minimum set to deduce all the dependence restrictions. □

4.3 Scalar-linear Solvability of $U_{2,n}$ Matroidal Networks

Theorem 3. The $U_{2,n}(n \geq 3)$ matroidal network from the construction in Section 4.2 is scalar-linearly solvable over a finite field $\mathbb{F}_q$ iff $q \geq n-1$.

Proof. The construction process applies overlapping dependence restrictions for $U_{2,n}$ and $U_{2,n+1}$ matroidal networks. Consequently, as shown in Fig. 4.4, a $U_{2,n}$ matroidal network is a subnetwork of a $U_{2,n+1}$ matroidal network. One can extend the $U_{2,n}$ into the $U_{2,n+1}$ network by replacing node u that demands m_2 in $U_{2,n}$ with a relay node, adding an out-edge from the relay and a new node v at the head of this out-edge. Packet p on the out-edge should be mapped to x_{n+1}. Set $f(p) = x_{n+1}$, and $g(x_{n+1}) = v$. Then we can add demand nodes connecting to the head node and each node corresponding to the other ground set elements according to $g : \mathcal{S} \to N$. One demand node that is connected to the nodes $g(x_1)$ and $g(x_{n+1})$ should demand m_2. All the other demand nodes connected to $g(x_{n+1})$ and $g(x_i)$, for all $2 \leq i \leq n$ should demand m_1.

The theorem can then be proved by induction on n. When $n = 3$, the $U_{2,3}$ matroidal



(a) (b) (c)

Figure 4.4: $U_{2,3}$, $U_{2,4}$ and $U_{2,5}$ matroidal networks, each contained in its subsequent network as a subnetwork.

network is the well-known butterfly network (Fig. 4.4(a)), solvable over $\mathbb{F}_2$. Assume the theorem is true when $n = k$, *i.e.*, the minimum field size required for the $U_{2,k}$ matroidal network is at least $k-1$. The $U_{2,k+1}$ matroidal network is an extension of $U_{2,k}$, and requires a field size at least $k-1$, since otherwise the $U_{2,k}$ sub-network it contains would not be scalar-linearly solvable.

If the field size is at most $k-1$, u in the $U_{2,k+1}$ matroidal network will be able to recover both m_1 and m_2 from its two in-edges. It can send combinations of m_1 and m_2 to its out-edge, among $m_1, m_2, m_1+m_2, m_1+2m_2, ..., m_1+(k-2)m_2$. Thus there are only these k possible choices for the packets on the out-edges of v. However, there are also k demand nodes connecting to v. The other node with which the demand node connects is $g(x_i)(1 \leq i \leq n)$. Any one of the k choices for the out-going packet of v is dependent with one of the packets sent by $g(x_i)$. If the field size is at least k instead, one more choice $m_1+(k-1)m_2$ becomes available for p. It is independent from all the packets sent by $g(x_i)$, and will enable all the

demand nodes to recover the message they desire. □

Inspired by the subnetwork property between $U_{2,n}$ matroidal networks above, we can make a simple graph-theoretical comparison between matroidal networks created by our method and the E-S-G method, as shown in Table 4.1. It also turns out our $U_{2,n}$ matroidal network is one node and two edges smaller than the $C_{n,2}$ combination network. Both networks require a finite field size of at least $n-1$ to be scalar-linearly solvable.

$U_{2,n}$ matroid	our method		The E-S-G method	
	node #	edge #	node #	edge #
$U_{2,3}$	6	7	15	38
$U_{2,4}$	10	14	21	70
$U_{2,5}$	15	23	28	117
$U_{2,n}$	$\frac{n(n+1)}{2}$	n^2-2	$\frac{(n+2)(n+3)}{2}$	$\frac{n^3+3n^2+6n+4}{2}$

Table 4.1: Number of nodes and number of edges in our uniform matroidal networks and in simplified E-S-G matroidal networks.

The case of $U_{2,n}$ matroidal networks illustrates that the application of dependence deduction reduces the complexity of transferring dependence relations from a matroid to a network, and minimizes the size of the resulting matroidal network. For a uniform matroidal network constructed from our method, or a more general matroidal network constructed from the optimized D-F-Z method, if we can deduce all the dependence restrictions, the network should be scalar-linearly solvable over the finite field on which the matroid is representable. We proved this to be true for $U_{2,n}$ matroidal networks, and conjecture that it is true for *general* $U_{r,n}$ matroidal networks, whose proof may be derived after general uniform matroid representability is settled. We next proceed to whirl matroidal networks.

Chapter 5

Whirl Matroidal Networks

We now describe the construction of whirl $\mathcal{W}^n (n \geq 3)$ matroidal networks, describe dependence deduction of the $\mathcal{W}^3$ ($\mathcal{W}^n$ when $n = 3$) matroidal network, and discuss the scalar-linear solvability of $\mathcal{W}^3$ matroidal network in the next three sections respectively.

5.1 Network Construction from Whirl Matroids

5.1.1 Method Description

The method to construct whirl matroidal networks is nearly the same as the method for uniform matroidal networks that is described in Sec. 4.1.1, except for the base and circuits used in the construction, and the number of repetition times for Step 2 and Step 3. The method can be briefly described as follows. We denote the whirl matroid as $\mathcal{W}^n$ $(n \geq 3)$ $= \mathcal{M}(\mathcal{S}, \mathcal{I})$, with ground set $\mathcal{S} = \{a_1, a_2, ..., a_n, b_1, b_2, ..., b_n\}$.

Constructing $\mathcal{W}^n$ Matroidal Networks. The construction consists of 3 steps:

1) Create source nodes according to the base $B = \{a_1, a_2, ..., a_n\}$ in $\mathcal{M}$.

2) Create intermediate nodes by applying the following n dependence restrictions sequentially: $b_1 \leftarrow a_1 a_2 ... a_n, b_2 \leftarrow b_1 a_1, b_3 \leftarrow b_2 a_2, ..., b_{n-1} \leftarrow b_{n-2} a_{n-2}, b_n \leftarrow b_1 a_n$.

3) Create demand nodes according to the following n dependence restrictions: $a_{n-1} \leftarrow b_n b_{n-1}, a_i \leftarrow \{a_1, a_2, ..., a_n\} \setminus \{a_i\} \cup \{b_{n+1-i}\}$, for i from 1 to $n-2$, $a_n \leftarrow \{a_1, a_2, ..., a_n\} \setminus \{a_n\} \cup \{b_2\}$.

5.1.2 $\mathcal{W}^3$ Example

We next use $\mathcal{W}^3$ as an example to illustrate the construction process.

Example: Constructing The $\mathcal{W}^3$ Matroidal Network. Consider $\mathcal{W}^3 = \mathcal{M}(\mathcal{S}, \mathcal{I})$, with ground set $\mathcal{S} = \{a_1, a_2, a_3, b_1, b_2, b_3\}$. $\mathcal{W}^3$ can be depicted geometrically as in Fig. 5.1. The set of circuits include $\{b_1, a_1, b_2\}$, $\{b_2, a_2, b_3\}$, $\{b_3, a_3, b_1\}$, $\{b_1, b_3, a_1, a_2\}$, $\{b_2, b_1, a_2, a_3\}$, $\{b_3, b_2, a_1, a_3\}$, $\{a_1, a_2, a_3, b_1\}$, $\{a_1, a_2, a_3, b_2\}$, $\{a_1, a_2, a_3, b_3\}$.

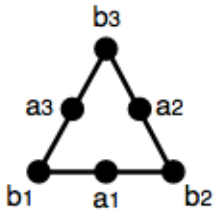


Figure 5.1: Geometric depiction of the $\mathcal{W}^3$ Matroid.

1) Create source nodes n_1, n_2, n_3 with messages m_1, m_2, m_3. Choose base $B = \{a_1, a_2, a_3\}$, let $f(m_i) = a_i, g(a_i) = n_i, i = 1, 2, 3$ (Fig. 5.2). Ground set elements are labelled according to function f.

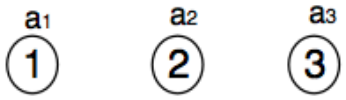


Figure 5.2: Partial $\mathcal{W}^3$ network after Step 1.

2) Choose dependence restriction $b_1 \leftarrow a_1 a_2 a_3$ from circuit $\{a_1, a_2, a_3, b_1\}$ in $\mathcal{W}^3$. First, we add a node n_4, edges $e_{1,4}$ from n_1 to n_4, $e_{2,4}$ from n_2 to n_4 and $e_{3,4}$ from n_3 to n_4, and corresponding packets $p_{1,4}$, $p_{2,4}$ and $p_{3,4}$. Let $f(p_{1,4}) = a_1, f(p_{2,4}) = a_2, f(p_{3,4}) = a_3$. Second, we add a node n_5 with a single in-edge $e_{4,5}$ and packet $p_{4,5}$, connecting n_4 to n_5, and let $f(p_{4,5}) = b_1$ and $g(b_1) = n_5$. Repeat the above procedure for $b_2 \leftarrow b_1 a_1$, $b_3 \leftarrow b_1 a_3$ (Fig. 5.3).

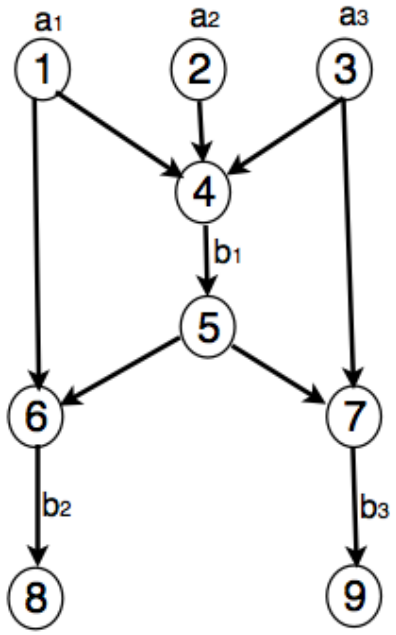


Figure 5.3: Partial $\mathcal{W}^3$ network after Step 2.

3) Choose $a_2 \leftarrow b_2 b_3$ from the circuit $\{b_2, a_2, b_3\}$ in $\mathcal{W}^3$. As $g(a_2) = n_2$ is a source node with message m_2, we add a demand node n_{11}, which demands message m_2 and has in-edges $e_{7,11}, e_{9,11}$ with corresponding packets $p_{7,11}, p_{9,11}$. $e_{7,11}$ connects $g(b_2)$ to n_{11}. $e_{9,11}$ connects $g(b_3)$ to n_{11}. Set $f(p_{7,11}) = b_2$ and $f(p_{9,11}) = b_3$. Repeat the above procedure for $a_1 \leftarrow a_2 a_3 b_3, a_3 \leftarrow a_1 a_2 b_2$. The resulting network is shown in Fig. 5.4.

5.2 Dependence Deduction of $\mathcal{W}^3$ matroidal Network

For a whirl matroidal network, deducing all the dependence restrictions may be harder than the case of uniform matroidal networks. There exist whirl matroidal network where just using the dependence restrictions applied during the construction is insufficient to deduce *all* the dependence restrictions. In this scenario, one may deduce a number of independence restrictions first, from existing dependence and independence restrictions of the network. We next show this fact from the $\mathcal{W}^3$ matroidal network (Fig. 5.4).

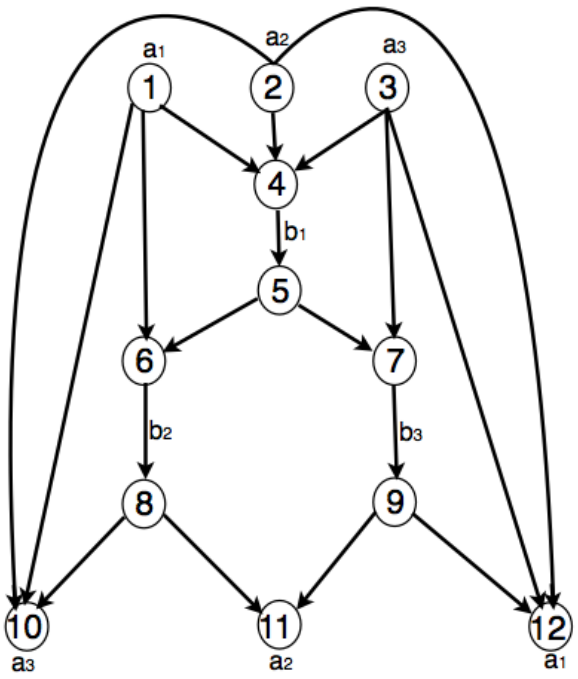


Figure 5.4: Complete $\mathcal{W}^3$ network after Step 3. Smallest known planar multiple unicast network requiring $\mathbb{F}_3$.

Theorem 4. In the $\mathcal{W}^3$ matroidal network, we can deduce all the dependence restrictions of $\mathcal{W}^3$.

Proof. During the construction of $\mathcal{W}^3$ matroidal network, we use the base $\{a_1, a_2, a_3\}$ and the dependence restrictions $b_1 \leftarrow a_1a_2a_3$, $b_2 \leftarrow b_1a_1$, $b_3 \leftarrow b_1a_3$, $a_2 \leftarrow b_2b_3$, $a_1 \leftarrow a_2a_3b_3$, $a_3 \leftarrow a_1a_2b_2$. Applying the rules directly on these 6 dependence restrictions can not deduce all 33 (3 size-3 and 6 size-4 circuits) dependence restrictions. We first deduce a number of independence restrictions from the network.

In order to apply R1 on size-3 dependence restrictions, we need size-2 independence restriction first. From the network, we can deduce that for the three size-3 circuits, $\{b_1, a_1, b_2\}$, $\{b_2, a_2, b_3\}$, $\{b_3, a_3, b_1\}$, any size-2 subset of each circuit is an independence restriction. For example, $\{a_1, b_1\}$ should be an independence restriction since if b_1 is dependent on a_1, then b_1 must be a constant multiple of a_1. Then b_2 can not contain any information about message a_3, and receiver n_{10} can not recover a_3. Not all the independence restrictions are so easy

to deduce though, for example, $\{b_1, b_2\}$. If b_1 is the same as b_2, then b_3 should be a linear combination of b_2 and a_3. Then receiver n_{11} can only decode b_2 or a_3. As b_2 can not be a_2, n_{11} can't decode a_2. Given these independence restrictions and 6 dependence restrictions, by applying the rules, we can finally deduce all the 33 dependence relations. □

From the above, we can observe that for whirl matroidal networks, we may have to deduce a number of independence restrictions first before applying rules directly on the dependence restrictions we have. This is proved to be true for other non-uniform matroidal networks as well, including the Fano and non-Fano matroidal networks [4].

5.3 Scalar-linear Solvability of the $\mathcal{W}^3$ Matroidal Network

We can prove the $\mathcal{W}^3$ matroidal network has no $\mathbb{F}_2$ scalar linear solution simply by enumeration. To satisfy the demands of all receivers, we can infer that b_1 has no choice but being $a_1 + a_2 + a_3$. Then as for b_2, it can be a_1, $a_1 + b_1 = a_2 + a_3$ under $\mathbb{F}_2$, or $b_1 = a_1 + a_2 + a_3$. The same goes for b_3: it can be a_3, $a_3 + b_1 = a_1 + a_2$ under $\mathbb{F}_2$, or $b_1 = a_1 + a_2 + a_3$. We can verify that no combinations of b_1, b_2, b_3 can satisfy the demands of all three receivers simultaneously. We conclude that there's no scalar linear solution over $\mathbb{F}_2$ for this $\mathcal{W}^3$ matroidal network.

However, it does have a vector linear solution over $\mathbb{F}_2$ for the dimension of 2. The coefficients of this solution are as illustrated in Fig. 5.5. One possible assignment could be as follows. $M_1 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $M_2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $M_3 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $M_4 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, $M_5 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $M_6 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $M_7 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $M_8 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, $M_9 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, $M_{10} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $M_{11} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $M_{12} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $M_{13} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, $M_{14} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $M_{15} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. We can verify this coefficient

assignment is valid as follows. Remember $1 + 1 = 0$ over $\mathbb{F}_2$.

$$
\begin{aligned}
e_{4,5} &= M_1 a_1 + M_2 a_2 + M_3 a_3 \\
&= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_{11} \\ a_{12} \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_{21} \\ a_{22} \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_{31} \\ a_{32} \end{bmatrix} = \begin{bmatrix} a_{11} + a_{12} + a_{21} + a_{22} + a_{31} + a_{32} \\ a_{11} + a_{21} + a_{31} \end{bmatrix}
\end{aligned}
$$

$$
\begin{aligned}
e_{6,8} &= M_4 a_1 + M_5 e_{4,5} \\
&= \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a_{11} \\ a_{12} \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_{11} + a_{12} + a_{21} + a_{22} + a_{31} + a_{32} \\ a_{11} + a_{21} + a_{31} \end{bmatrix} = \begin{bmatrix} a_{11} + a_{21} + a_{22} + a_{31} + a_{32} \\ a_{12} + a_{21} + a_{31} \end{bmatrix}
\end{aligned}
$$

$$
\begin{aligned}
e_{7,9} &= M_7 a_3 + M_6 e_{4,5} \\
&= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_{31} \\ a_{32} \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_{11} + a_{12} + a_{21} + a_{22} + a_{31} + a_{32} \\ a_{11} + a_{21} + a_{31} \end{bmatrix} = \begin{bmatrix} a_{11} + a_{12} + a_{21} + a_{22} + a_{32} \\ a_{11} + a_{21} + a_{31} + a_{32} \end{bmatrix}
\end{aligned}
$$

$$
\begin{aligned}
n_{10} : \begin{bmatrix} a_{31} \\ a_{32} \end{bmatrix} &= M_8 e_{6,8} + M_9 a_1 + M_{10} a_2 \\
&= \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a_{11} + a_{21} + a_{22} + a_{31} + a_{32} \\ a_{12} + a_{21} + a_{31} \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a_{11} \\ a_{12} \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_{21} \\ a_{22} \end{bmatrix}
\end{aligned}
$$

$$
\begin{aligned}
n_{11} : \begin{bmatrix} a_{21} \\ a_{22} \end{bmatrix} &= M_{11} e_{6,8} + M_{12} e_{7,9} \\
&= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_{11} + a_{21} + a_{22} + a_{31} + a_{32} \\ a_{12} + a_{21} + a_{31} \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_{11} + a_{12} + a_{21} + a_{22} + a_{32} \\ a_{11} + a_{21} + a_{31} + a_{32} \end{bmatrix}
\end{aligned}
$$

$$
\begin{aligned}
n_{12} : \begin{bmatrix} a_{11} \\ a_{12} \end{bmatrix} &= M_{13} e_{7,9} + M_{14} a_3 + M_{15} a_2 \\
&= \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a_{11} + a_{12} + a_{21} + a_{22} + a_{32} \\ a_{11} + a_{21} + a_{31} + a_{32} \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_{31} \\ a_{32} \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_{21} \\ a_{22} \end{bmatrix}
\end{aligned}
$$

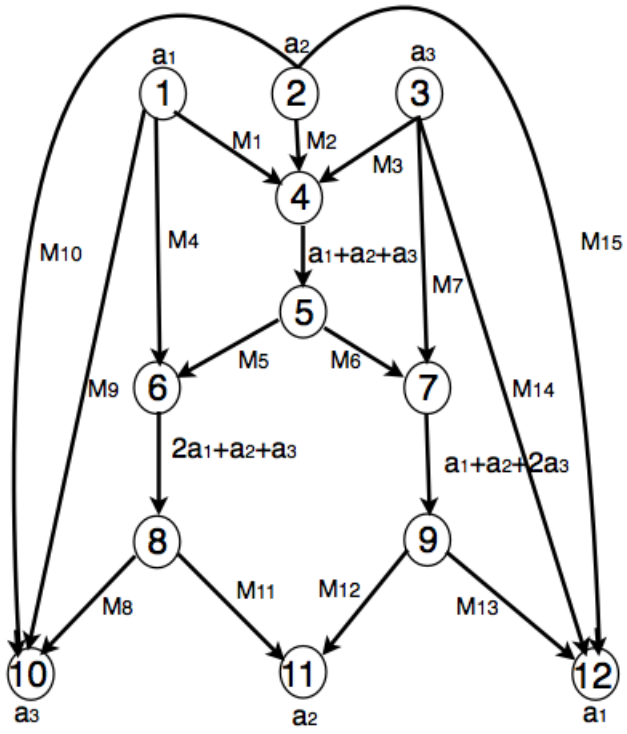


Figure 5.5: The $\mathcal{W}^3$ matroidal network has no scalar-linear solution over $\mathbb{F}_2$, but it has a vector linear solution over $\mathbb{F}_2$.

We can easily see this network has a scalar linear solution over all finite fields with size greater than or equal to 3. The code construction according to $\mathbb{F}_3$ is shown in Fig. 5.5. More specifically, b_1 could be $a_1 + a_2 + a_3$, b_2 could be $2a_1 + a_2 + a_3$, b_3 could be $a_1 + a_2 + 2a_3$. We can verify that this is indeed a valid solution.

Recent literature in network coding studied the necessary field size in planar networks. Xiahou *et al.* [7] first constructed a planar multicast network that requires $\mathbb{F}_3$. It is further conjectured and partially proved that $\mathbb{F}_3$ is sufficient for all multicast networks that are planar. Interestingly, all known multiple-unicast networks that are planar either do not require network coding or can be solved over $\mathbb{F}_2$. The $\mathcal{W}^3$ matroidal network is the first planar multiple-unicast network that is solvable over $\mathbb{F}_3$ but not $\mathbb{F}_2$.

We can further conjecture all $\mathcal{W}^n (n \geq 3)$ matroidal networks are scalar-linearly solvable over $\mathbb{F}_q$ *iff* $q \geq 3$. The conjecture can be probably proved by simple enumeration. Given $\mathbb{F}_2$, we can calculate all possible values of b_1 through b_n. For all possible combinations of

b_1 through b_n, we try to prove that no combination will enable all demand nodes to decode the information they want. However, given $\mathbb{F}_3$, if we can design the encoding and decoding scheme, then the claim is proved.

Chapter 6

More Matroidal Network Example

By applying the technique of dependence deduction on the Q_6 matroid [8], we construct an almost-planar matroidal network requiring $\mathbb{F}_4$. The Q_6 matroid has a graphic depiction as shown in Fig. 6.1. It has rank 3 and two circuits of size 3. The corresponding network is shown in Fig. 6.2. As Q_6 is representable over a finite field $\mathbb{F}$ if and only if $|\mathbb{F}| \geq 4$, we can prove the network constructed is scalar linearly solvable over a finite field if and only if the size of the field is greater then or equal to 4.

Consider $Q_6 = \mathcal{M}(\mathcal{S}, \mathcal{I})$, with ground set $\mathcal{S} = \{a, b, c, w, x, y\}$. The geometric depiction in Fig. 6.1 implies that the set of circuits includes $\{a, b, c\}$, $\{a, x, y\}$, $\{c, w, x, y\}$, $\{c, w, x, b\}$, $\{c, w, x, a\}$, $\{c, w, y, b\}$, $\{x, w, y, b\}$, $\{a, b, w, y\}$, $\{a, b, x, w\}$, $\{b, c, x, y\}$, $\{c, w, a, y\}$. The construction process can be as follows.

1) Create source nodes with messages according to the base $B = \{b, w, y\}$.

2) Create intermediate nodes by apply the following 3 dependence restrictions: $a \leftarrow bwy$, $c \leftarrow ab$, $x \leftarrow ay$.

3) Create demand nodes to demand w based on $w \leftarrow acx$, and y based on $y \leftarrow wbx$, $y \leftarrow bcx$, and b based on $b \leftarrow wxy$, $b \leftarrow cwx$.

As the $U_{2,5}$ matroidal network (Fig. 4.4(c)) is also almost-planar and requires a finite field of $\mathbb{F}_4$ to be scalar-linearly solvable, we can further conjecture that $\mathbb{F}_4$ may be sufficient for all almost-planar network coding problems.

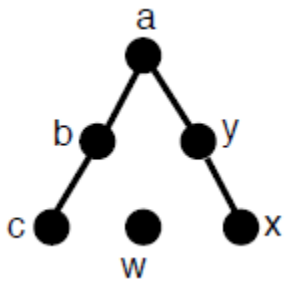


Figure 6.1: Geometric depiction of the Q_6 matroid.

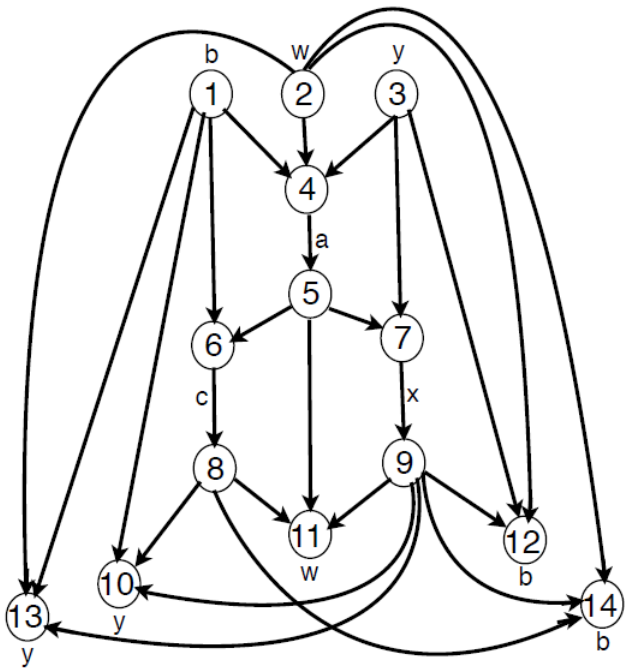


Figure 6.2: The Q_6 matroidal network.

Chapter 7

Connection Between Matroidal Networks from A Uniform Matroid and Its Minor

Inspired by the subnetwork property between $U_{2,n}$ matroidal networks as introduced in Sec. 4.3, in this chapter we explore if this property can be generalized to more uniform matroidal networks. We find that this property does exist between matroidal networks from a uniform matroid and any of its matroid minor. First we will describe the definition of matroid minor. Then we will focus on the property of uniform matroid minor. Finally, we will present the subnetwork property between matroidal networks of a uniform matroid and its minor.

7.1 Matroid Minor Definition

If M is a matroid with ground set E, and $S \subseteq E$, the **restriction** of M to S, denoted as $M|S$, is the matroid on the set S whose independent sets are the independent sets of M that are contained in S. Its circuits are the circuits of M that are contained in S and its rank function is that of M restricted to subsets of S.

The dual operation of restriction is **contraction**. Let $T \subseteq E$, the contraction of M by T, denoted as M/T, is the matroid on the underlying set $E - T$ whose rank function is $r'(A) = r(A \cup T) - r(T)$ for $A \subseteq E - T$.

A matroid N that is obtained from M by a sequence of restriction and contraction operations is called a minor of M. We say M **contains** N **as a minor**.

Example 7: Recall $\mathcal{W}^3$ is defined on the ground set $\{a_1, a_2, a_3, b_1, b_2, b_3\}$. The set of circuits includes $\{b_1, a_1, b_2\}$, $\{b_2, a_2, b_3\}$, $\{b_3, a_3, b_1\}$, $\{b_1, b_3, a_1, a_2\}$, $\{b_2, b_1, a_2, a_3\}$, $\{b_3, b_2, a_1, a_3\}$, $\{a_1, a_2, a_3, b_1\}$, $\{a_1, a_2, a_3, b_2\}$, $\{a_1, a_2, a_3, b_3\}$. Set $T_1 = \{b_1, b_2, a_2, a_3\}$, then according to the

definition of restriction, $\mathcal{W}^3|T_1$ has ground set $\{b_1, b_2, a_2, a_3\}$. The set of independent sets is $\{\emptyset, \{b_1\}, \{b_2\}, \{a_2\}, \{a_3\}, \{b_1, b_2\}, \{b_1, a_2\}, \{b_1, a_3\}, \{b_2, a_2\}, \{b_2, a_3\}, \{a_2, a_3\}, \{b_1, b_2, a_2\}, \{b_1, b_2, a_3\}, \{b_1, a_2, a_3\}, \{b_2, a_2, a_3\}\}$. We can easily see $\mathcal{W}^3|T_1$ is isomorphic to $U_{3,4}$.

Example 8: Recall $U_{5,6}$ is defined on the ground set $E = \{x_1, x_2, x_3, x_4, x_5, x_6\}$. Any size-5 subset of the ground set is a base and any size-6 subset of the ground set is a circuit. Set $T_2 = \{x_1, x_2, x_3\}$, then according to the definition of contraction, $U_{5,6}/T_2$ has ground set $E - T_2 = \{x_4, x_5, x_6\}$. We can use the rank definition of a matroid to define $U_{5,6}/T_2$ as follows.

$$r'(\emptyset) = r(T_2) - r(T_2) = 0,$$

$$r'(\{x_4\}) = r(x_1, x_2, x_3, x_4) - r(x_1, x_2, x_3) = 4 - 3 = 1,$$

$$r'(\{x_5\}) = r(x_1, x_2, x_3, x_5) - r(x_1, x_2, x_3) = 4 - 3 = 1,$$

$$r'(\{x_6\}) = r(x_1, x_2, x_3, x_6) - r(x_1, x_2, x_3) = 4 - 3 = 1,$$

$$r'(\{x_4, x_5\}) = r(x_1, x_2, x_3, x_4, x_5) - r(x_1, x_2, x_3) = 5 - 3 = 2,$$

$$r'(\{x_4, x_6\}) = r(x_1, x_2, x_3, x_4, x_6) - r(x_1, x_2, x_3) = 5 - 3 = 2,$$

$$r'(\{x_5, x_6\}) = r(x_1, x_2, x_3, x_5, x_6) - r(x_1, x_2, x_3) = 5 - 3 = 2,$$

$$r'(\{x_4, x_5, x_6\}) = r(x_1, x_2, x_3, x_4, x_5, x_6) - r(x_1, x_2, x_3) = 5 - 3 = 2.$$

We can check that $U_{5,6}/T_2$ is isomorphic to $U_{2,3}$.

7.2 Uniform matroid minors

For a uniform matroid $U_{r,n}$ defined on the ground set $E = \{x_1, x_2, ..., x_n\}$, suppose $S = \{x_1, x_2, ..., x_k\}(r \leq k \leq n)$, then $U_{r,n}|S = U_{r,k}$. Suppose $T = \{x_1, x_2, ..., x_m\}(0 \leq m \leq r)$, then $U_{r,n}/T = U_{r-m,n-m}$.

To illustrate the distribution of $U_{r,n}$ minors, we can draw all $U_{r',n'}(r' \leq r, n' \leq n)$ in a table as follows. We can find that not all $U_{r',n'}$ with $r' \leq r, n' \leq n$ is a minor of $U_{r,n}$. Only

the $U_{r',n'}$s on the right side of the line are minors of $U_{r,n}$. As a result, $U_{r,n}$ has a total of $(n-r+1)\times r$ minors.

$$\begin{array}{cccc|cccc}
 & & & & U_{r,n} & U_{r,n-1} & \cdots & U_{r,r} \\
 & & & U_{r-1,n} & U_{r-1,n-1} & U_{r-1,n-2} & \cdots & U_{r-1,r-1} \\
 & & U_{r-2,n} & U_{r-2,n-1} & U_{r-2,n-2} & U_{r-2,n-3} & \cdots & U_{r-2,r-2} \\
 & \iddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
U_{1,n} & \cdots & U_{1,n-r+3} & U_{1,n-r+2} & U_{1,n-r+1} & U_{1,n-r} & \cdots & U_{1,1}
\end{array}$$

7.3 Matroidal Networks from A Uniform Matroid and Its Minor

Theorem 5: For a uniform matroid $U_{r,n}$ with ground set $E = \{x_1, x_2, ..., x_n\}$, let $S = \{x_1, x_2, ..., x_k\}(r \leq k \leq n), T = \{x_1, x_2, ..., x_m\}(0 \leq m \leq r)$, then any $U_{r,n}|S$ or $U_{r,n}/T$ matroidal network is a subnetwork of the $U_{r,n}$ matroidal network.

Proof. As introduced in Sec. 4.3, we can see that the $U_{r,k}$ matroidal network is a subnetwork of the $U_{r,n}$ matroidal network when $r \leq k \leq n$. So the $U_{r,n}|S$ matroidal network is always a subnetwork of the $U_{r,n}$ matroidal network.

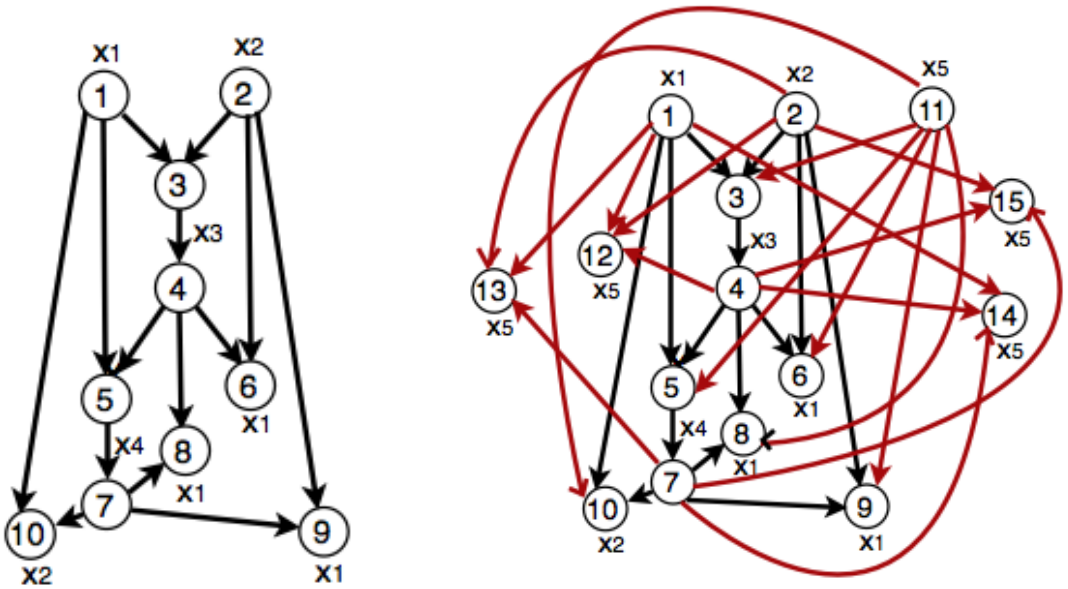
As for the case of $U_{r,n}/T$, we just need to show that the $U_{r-m,n-m}$ matroidal network is always a subnetwork of the $U_{r,n}$ matroidal network for $0 \leq m \leq r$. Given the transitivity of the subnetwork property (i.e., if g_1 is a subnetwork of g_2 and g_2 is a subnetwork of g_3, then g_1 is a subnetwork of g_3.), we can reduce the case to prove $U_{r,n}$ matroidal network is always a subnetwork of $U_{r+1,n+1}$ matroidal network.

Using the method we developed for constructing uniform matroidal networks (Sec. 4.1.1), we can construct $U_{r,n}$ matroidal network as follows. In Step 1, we use the base $\{x_1, x_2, ..., x_r\}$. In Step 2 and Step 3, we use the $\binom{n}{r}$ dependence restrictions with the right side forming the set of all bases. Then to construct $U_{r+1,n+1}$, we proceed as follows: in Step 1, we use the base $\{x_1, x_2, ..., x_r, x_{r+1}\}$, in Step 2 and 3, we add x_{n+1} to the right side of the $\binom{n}{r}$ dependence restrictions to create a new set of $\binom{n}{r}$ dependence restrictions. At the same time, we create

another $\binom{n}{r+1}$ dependence restrictions, with the left side being x_{n+1} and right side being all possible $r+1$ element combinations of $\{x_1, x_2, ..., x_n\}$. As $\binom{n}{r} + \binom{n}{r+1} = \binom{n+1}{r+1}$, we can see the $\binom{n+1}{r+1}$ dependence restrictions used in $U_{r+1,n+1}$ matroidal network construction satisfy the property that the right side of all dependence restrictions form the set of all bases. So the network created is the correct $U_{r+1,n+1}$ matroidal network.

As a result, we can create the $U_{r+1,n+1}$ matroidal network from the $U_{r,n}$ matroidal network by just adding more nodes and edges in each step. So we can conclude that the $U_{r,n}$ matroidal network is a subnetwork of the $U_{r+1,n+1}$ matroidal network. □

Example 9: We can show that the $U_{2,4}$ matroidal network is a subnetwork of the $U_{3,5}$ matroidal network. Their construction processes are as follows. For $U_{2,4}$ with ground set $\{x_1, x_2, x_3, x_4\}$, in Step 1, we choose base $\{x_1, x_2\}$, in Step 2, we choose dependence restrictions $x_3 \leftarrow x_1x_2, x_4 \leftarrow x_1x_3$, in Step 3, we choose dependence restrictions $x_2 \leftarrow x_1x_4, x_1 \leftarrow x_2x_3, x_1 \leftarrow x_2x_4, x_1 \leftarrow x_3x_4$. For $U_{3,5}$ with ground set $\{x_1, x_2, x_3, x_4, x_5\}$, in Step 1, we choose base $\{x_1, x_2, x_5\}$, in Step 2, we choose dependence restrictions $x_3 \leftarrow x_1x_2x_5, x_4 \leftarrow x_1x_3x_5$, in Step 3, we choose dependence restrictions $x_2 \leftarrow x_1x_4x_5, x_1 \leftarrow x_2x_3x_5, x_1 \leftarrow x_2x_4x_5, x_1 \leftarrow x_3x_4x_5, x_5 \leftarrow x_1x_2x_3, x_5 \leftarrow x_1x_2x_4, x_5 \leftarrow x_1x_3x_4, x_5 \leftarrow x_2x_3x_4$. According to the method, we can see that the $U_{2,4}$ matroidal network (Fig. 7.1(a)) is a subnetwork of the $U_{3,5}$ matroidal network (Fig. 7.1(b)).



(a) $U_{2,4}$ matroidal network

(b) $U_{3,5}$ matroidal network

Figure 7.1: The $U_{2,4}$ matroidal network is a subnetwork of the $U_{3,5}$ matroidal network.

Chapter 8

Conclusion

In this thesis, we proposed the concept of dependence deduction, which helps us create matroidal networks of small size in polynomial time complexity. Applying this technique on specific matroids, including uniform matrons and whirl matroids, we derive matroidal networks that advance our understandings on the power and limitations of network coding. Our results can be summarized as follows.

1. The $U_{2,n}$ matroidal network we constructed advances the state-of-art in designing smallest network that require network coding over a field $\mathbb{F}_q$, for all prime power $q \geq n-1$. It is encouraging that the $U_{2,n}$ matroidal network is simpler than $C_{n,2}$ combination network, and by far the corresponding E-S-G matroidal network. $U_{2,4}$ is now the smallest network requiring $\mathbb{F}_3$.

2. The $\mathcal{W}^3$ matroidal network is the first planar multiple-unicast network requiring $\mathbb{F}_3$.

3. The Q_6 matroidal network is another example of an almost-planar network requiring $\mathbb{F}_4$.

4. There exists a subnetwork property between matroidal networks from a uniform matroid and that from its matroid minor.

There are a number of open problems for future research.

1. Is $U_{2,n}$ matroidal network the smallest network that requires a field size of $n-1$ to be scalar-linearly solvable?

2. Is $\mathbb{F}_3$ sufficient for all planar multiple-unicast network coding problems?

3. Is $\mathbb{F}_4$ sufficient for all almost-planar network coding problems?

4. Can the subnetwork property be generalized to all matroids? Specifically, is there a subnetwork property between matroidal networks from a general matroid and its matroid minors?

Bibliography

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow", *IEEE Trans. on Inf. Theory*, vol. 46, no. 4, pp. 1204-1216, Jul. 2000.

[2] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding", *IEEE Trans. on Inf. Theory*, vol. 49, no. 2, pp. 371-381, Feb. 2003.

[3] S. El Rouayheb, A. Sprintson, and C. Georghiades, "On the index coding problem and its relation to network coding and matroid theory," *IEEE Trans. on Inf. Theory*, vol. 56, no. 7, pp. 3187-3195, Jul. 2010.

[4] R. Dougherty, C. Freiling, and K. Zeger, "Insufficiency of linear coding in network information flow," *IEEE Trans. on Inf. Theory*, vol. 51, no. 8, pp. 2745-2759, Aug. 2005.

[5] R. Dougherty, C. Freiling, and K. Zeger, "Networks, matroids, and non-Shannon information inequalities," *IEEE Trans. on Inf. Theory*, vol. 53, no. 6, pp. 1949-1969, Jun. 2007.

[6] R. Dougherty, C. Freiling, and K. Zeger, "Nonreversibility and equivalent constructions of multiple-unicast networks," *IEEE Trans. on Inf. Theory*, vol. 52, no. 11, pp. 5067-5077, Nov. 2006.

[7] T. Xiahou, Z. Li, and C. Wu, "Information Multicast in (Pseudo-)Planar Networks: Efficient Network Coding over Small Finite Fields," in *Proc. IEEE Int. Symp. Network Coding*, Calgary, AB, Canada, June 2013.

[8] J. G. Oxley, *M*atroid Theory, second edition. New York: Oxford Univ. Press, 2011.

[9] M. Medard, M. Effros, T. Ho, and D. Karger,"On coding for non-multicast networks," in *Proc. 41st Annu. Allerton Conf. Commun. Control Comput.*, Monticello, IL, pp. 21-29, Oct. 2003.

[10] R. Koetter, and M. Medard,"An Algebraic Approach to Network Coding," in *IEEE Trans. on Networking*, vol. 11, no. 5, pp. 782-795, Oct. 2003.

[11] S. Jaggi, P. Sanders, P.A. Chou, M. Effros, S. Egner, K. Jain, and L.M.G.M. Tolhuizen,"Polynomial time algorithms for multicast network code construction," in *IEEE Trans. on Inf. Theory*, vol. 51, no. 6, Jun. 2005, pp. 1973-1982.

[12] A. Kim, and M. Medard, "Scalar-linear Solvability of Matroidal Networks Associated with Representable Matroids," Available on Arxiv:1004.0727v1 [cs.IT], April, 2010.

[13] R. Dougherty, C. Freiling, and K. Zeger, "Linear Network Codes and Systems of Polynomial Equations," *IEEE Trans. on Inf. Theory*, vol. 54, no. 5, pp. 2303-2316, May 2008.

[14] Q. Sun, S. T. Ho, and S.-Y.R. Li, "On Network Matroids and Linear Network Codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 1833-1837.

[15] H. Whitney, "On the abstract properties of linear dependence," in *Amer. J. Math.*, vol. 57, pp. 509-533, 1935.

[16] J. Simonis, and A. Ashikhmin, "Almost affine codes," in *Desings, Codes Cryptogr.*, vol. 14, pp. 179-797, 1998.

[17] F. Matus, "Matroid representations by partitions," in *Discrete Math.*, vol. 203, pp. 169-194, 1999.

[18] R. Diestel, "Graph Theory, Electronic," in *Graduate Texts in Mathematics*, vol. 173, 2000.

[19] X. Yin, Y. Yang, X. Wang, X. Yang, and Z. Li, "A Graph Minor Perspective to Network Coding: Connecting Algebraic Coding with Network Topologies," in *Proc. of IEEE INFOCOM*, 2013.

[20] R. Dougherty, C. Freiling, and K. Zeger, "Unachievability of Network Coding Capacity," in *IEEE Trans. on Inf. Theory*, vol. 52, no. 6, June 2006, pp. 2365-2372.