ISIT'2013 1569719075

On Uniform Matroidal Networks

Ming He, Zongpeng Li
Department of Computer Science
University of Calgary
{mhe,zongpeng}@ucalgary.ca

Chuan Wu
Department of Computer Science
The University of Hong Kong
cwu@cs.hku.hk

Xunrui Yin
School of Computer Science
Fudan University
09110240030@fudan.edu.cn

***Abstract*—Matroidal networks play a fundamental role in proving theoretical results on the limits of network coding. This can be explained by the underlying connections between network coding and matroid theory, both of which build upon the fundamental concept of *independence*. Two existing methods are known in the network coding literature for constructing networks from a matroid. The method due to Dougherty *et al.* [5] is high in time complexity but can create relatively simple network structures from a given matroid. Another method due to El Rouayheb *et al.* [3] is low in time complexity, but results in rather complex network structures. This work studies the design of matroidal networks from uniform matroids, targetting 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 requirement.**

I. Introduction

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. As a result, 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 linear and non-linear relations. Linear dependence is shown to suffice in a number of network coding problems, including one-to-many multicast [2]. Matroid theory is also built upon the fundamental concept of dependence and independence. Such a connection suggests the possibility of transforming a matroid into a network, with the same set of dependence relations carried over, such that the matroid and the correspondingly network are representable and scalar-linearly solvable, respectively, over the same set of fields.

Matroid representability is a relatively mature subject of study. Once one designs a matroidal network construction procedure that ensures the matroid is representable over a finite field $\mathbb{F}$ *iff* the network is scalar-linearly solvable over the same field $\mathbb{F}$, then requirements on the field size and limitations on linear dependences from matroid representability can be carried over to network coding. For example, using the D-F-Z method due to Dougherty *et al.* [5], 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], the non-Shannon information inequalities [5], and the non-reversibility of multiple-unicast networks [6]. Unfortunately, the D-F-Z method suffers from a high time complexity despite moderate output network sizes. In comparison, the E-S-G method due to El Rouayheb *et al.* [3] has a low time complexity, but results in networks that contain a substantial level of redundancy in nodes and edges, when compared to D-F-Z matroidal networks built from the same input.

This work studies matroidal network construction that aims at both reducing the time complexity of the D-F-Z method and optimizing the graph structure in the resulting matroidal network. We observe that the D-F-Z method essentially transfers only a subset of all dependence relations in a matroid into the network. Other dependence relations are not explicitly transferred, but can be deduced from the explicitly transferred dependence and independence relations. Using *dependence deduction* we can prove that all dependence relations in a matroid have been transferred to the created network, including both explicitly and implicitly. This concept of dependence deduction serves as an important tool for improving the D-F-Z method. This work first focuses on uniform matroids, for which dependence reductions are relatively simple. We design a matroidal network construction procedure that achieves both low time complexity and minimal network sizes.

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. In particular, the $U_{2,4}$ matroidal network is now the smallest known network that requires $\mathbb{F}_3$, and is simpler than the combination network $C_{4,2}$ and planar networks due to Xiahou *et al.* [7] that also require $\mathbb{F}_3$.

Our contribution lies not only in uniform matroidal network construction, but also in the concept of dependence deduction, which is helpful in designing not only uniform matroidal networks but also general matroidal networks. As an example, we apply dependence deduction to transform the $\mathcal{W}^3$ matroid [8], which is representable over a finite field $\mathbb{F}_q$ *iff* $q \geq 3$, into a planar multiple unicast network. We prove that all matroidal

dependences can be deduced in the network, although the deduction 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]. 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.

In the rest of the paper, Sec. II presents preliminaries, Sec. III is on uniform matroidal network construction, Sec. IV generalizes to non-uniform matroids, and Sec. V concludes the paper.

II. Model and Preliminaries

A *network* $\mathcal{N}$ is a finite, directed, acyclic multigraph, assigned with a finite set of messages and packets over an *alphabet* Σ. 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 $|\Sigma| = q$.

The set of *inputs* to a network node *u*, In(*u*), contains packets on its in-edges, together with messages generated locally at *u*. The set of *outputs* of *u*, 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. It is further *scalar-linear* if $k = 1$, and *vector-linear* if $k \geq 2$.

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 $I \in \mathcal{I}$ 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 $c \leftarrow ab$ in $\mathcal{M}$, and in general a circuit C contains $|C|$ dependence restrictions. All bases have the same size, which is the *rank* of $\mathcal{M}$, denoted as $r(\mathcal{S})$.

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. 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 over a field $\mathbb{F}$, then $\mathcal{M}$ is *representable over* $\mathbb{F}$.

Another important class of matroids is the family of *uniform matroids* $U_{r,n}$. 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.

III. 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 subsections respectively.

A. Network Construction from Uniform Matroids

Let $\mathcal{N}$ denote the network to be constructed, with message set M, node set N, and packet set P. The uniform matroid $U_{r,n}$ $(n \geq r + 1) = \mathcal{M}(\mathcal{S}, \mathcal{I})$, 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 $x_0 \leftarrow x_1 x_2 ... x_r$ 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 $x_1 x_2 ... x_r$ has not appeared on the right side of the dependence restrictions used in all $1 \leq j \leq i - 1$ iteration(s). 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 $f(p_i) = x_i$.

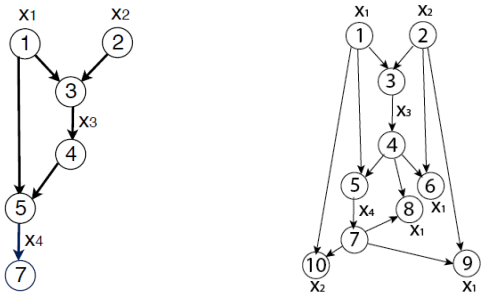
We next use $U_{2,4}$ as an example to illustrate the construction process.

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. 1). Ground set elements are labelled according to function f.

Fig. 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. 2(a)).
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. The resulting network is shown in Fig. 2(b).



(a) After Step 2. (b) After Step 3.

Fig. 2. $U_{2,4}$ matroidal network, smallest known network requiring $\mathbb{F}_3$.

Discussion. 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 network 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. III-B 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. III-B 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.

B. 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 right and can be used for guiding such deduction. All x_is 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 $x_n \leftarrow x_1x_2...x_{n-1}$.
(R2) If $x_1 \leftarrow x_2x_3...x_n$ and $x_n \leftarrow x_{n+1}x_{n+2}...x_{n+m}$, then $x_1 \leftarrow x_2x_3...x_{n-1}x_{n+1}...x_{n+m}$. Duplicate x_is on the right side can be eliminated. If there is already $x_i \leftarrow x_jx_k, i, j, k \in \{2, 3, ..., n-1, n+1, ..., n+m\}$, 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. III-A 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. In Step 1, we create source nodes n_1, n_2 with messages m_1, m_2. Then we choose base $B = \{x_1, x_2\}$ and let $f(m_i) = x_i, g(x_i) = n_i (i = 1, 2)$.

In Step 2, 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 $k=n$. At last in Step 3, we add 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 $3 \times \binom{n}{2}$ 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. □

C. 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 III-B 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. 3, a $U_{2,n}$ matroidal network is a subgraph 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.

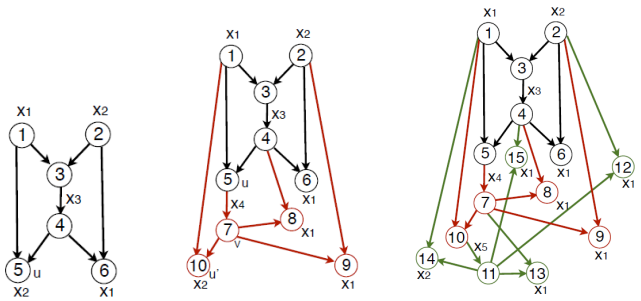


Fig. 3. $U_{2,3}$, $U_{2,4}$ and $U_{2,5}$ matroidal networks, each contained in its subsequent network as a subgraph.

The theorem can then be proved by induction on n. When $n=3$, the $U_{2,3}$ matroidal network is the well-known butterfly network (Fig. 3(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. □

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 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 non-uniform matroidal networks.

IV. Dependence Deduction Beyond Uniform Matroidal Networks

For a general matroidal network, deducing all the dependence restrictions may be harder than the case of uniform matroidal networks. There exist matroidal networks 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 study such a matroidal network (Fig. 4) resulting from the D-F-Z method applied on the $\mathcal{W}^3$ matroid [8], which is representable over a finite field $\mathbb{F}_q$ *iff* $q \geq 3$. The network can be proved to be scalar-linearly solvable over a finite field $\mathbb{F}_q$ *iff* $q \geq 3$. Next we show that all the dependence restrictions can be deduced from this $\mathcal{W}^3$ matroidal network.

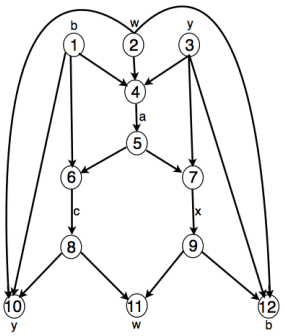


Fig. 4. The $\mathcal{W}^3$ matroidal network, the first planar multiple-unicast network requiring $\mathbb{F}_3$.

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

Proof. Let $\{a, b, c, w, x, y\}$ be the ground set of $\mathcal{W}^3$. By definition of $\mathcal{W}^3$, the circuits are $\{a, b, c\}$, $\{a, x, y\}$, $\{c, w, x\}$, $\{a, b, w, y\}$, $\{b, c, w, y\}$, $\{b, x, w, y\}$, $\{a, c, w, y\}$, $\{b, c, x, y\}$, $\{a, b, w, x\}$. During the construction of $\mathcal{W}^3$ matroidal network, we use the base $\{b, w, y\}$ and the dependence restrictions $a \rightarrow bwy$, $x \rightarrow ay$, $c \rightarrow ab$, $b \rightarrow xyw$, $w \rightarrow cx$, $y \rightarrow bcw$. 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, $\{a, b, c\}, \{a, x, y\}, \{c, w, x\}$, any size-2 subset of each circuit is an independence restriction. For example, $\{a, b\}$ should be an independence restriction since if a is dependent on b, then a must be a constant multiple of b. Then c can not contain any information about message y, and receiver n_{10} can not recover y. Not all the independence restrictions are so easy to deduce though, for example, $\{a, c\}$. If a is the same as c, then x should be a linear combination of c and y. Then receiver n_{11} can only decode c or y. As c can not be w, n_{11} can't decode w. Given these independence restrictions and 6 dependence restrictions, by applying the rules, we can finally deduce all the 33 dependence relations. □

From this case we can see for non-uniform 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].

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 $\mathbb{F}_2$.

V. Conclusion

We proposed a method for constructing matroidal networks for all uniform matroids, which is low in time complexity, and creates matroidal networks of minimum sizes. The technique of dependence deduction used may be of independent interest, and is shown to be applicable beyond uniform matroids. The $U_{2,n}$ matroidal networks we constructed advances the state-of-art in designing smallest networks that require network coding over a field $\mathbb{F}_q$, for all prime power q's. We also discover the first planar multiple unicast network not solvable over $\mathbb{F}_2$.

Acknowledgment

The authors would like to thank Randall Dougherty for helpful discussions during the research.

References

[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, C. Wu, and Z. Li, "Network coding in planar networks," Dept. of Computer Science, Univ. of Calgary, Calgary, AB, Canada.

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