Scalar-linear Solvability of Matroidal Networks Associated with Representable Matroids

Anthony Kim and Muriel Médard
Research Laboratory of Electronics
Massachusetts Institute of Technology
Email: {tonyekim, medard}@mit.edu

***Abstract*—We study matroidal networks introduced by Dougherty et al., who showed that if a network is scalar-linearly solvable over some finite field, then the network is a matroidal network associated with a representable matroid over a finite field. In this paper, we prove the converse. It follows that a network is scalar-linearly solvable if and only if the network is a matroidal network associated with a representable matroid over a finite field and that determining scalar-linear solvability of a network is equivalent to finding a representable matroid over a finite field and a valid network-matroid mapping. As a consequence, we obtain a correspondence between scalar-linearly solvable networks and representable matroids over finite fields. We note that this result, combined with the construction method due to Dougherty et al., can generate potentially new scalar-linearly solvable networks.**

I. Introduction

In 2000, Ahlswede et al. [1] introduced the network coding scheme to the problem of communicating information in networks by allowing intermediate nodes to code on the incoming packets. They showed that the extended capability of intermediate nodes gives greater information throughput than in the traditional routing scheme. They also showed that the capacity of a multicast network is equal to the minimum of min-cuts between source and receiver nodes.

Li et al. [2] showed that linear network coding is sufficient for multicast networks. Koetter and Médard [3] reduced the problem of determining scalar-linear solvability to solving a set of polynomial equations over some finite field and suggested connections between scalar-linearly solvable networks and nonempty varieties in algebraic geometry. They showed that scalar-linear solvability of many special case networks, such as two-level multicast and disjoint multicast, can be determined by their method. Dougherty et al. [4] strengthened the connection by demonstrating solvably equivalent pairs of networks and polynomial collections; for any polynomial collection, there exists a network that is scalar-linearly solvable over field F if and only if the polynomial collection is solvable over F. It is known that scalar-linear network codes are not sufficient in general. The M-network due to Koetter in [5] is a network with no scalar-linear solution but has a vector-linear solution. Lehman and Lehman [6] using 3-CNF formulas also provided an example where a vector solution is necessary.

Dougherty et al. [7], [8] defined and studied matroidal networks and suggested connections between networks and matroids. They used matroidal networks constructed from well-known matroids to show in [9] that not all solvable networks have a linear solution over some finite-field alphabet and vector dimension. They also constructed a matroidal network to show that Shannon-type information inequalities are not sufficient for computing network coding capacities in general. Recently, El Rouayheb et al. [10] strengthened the connection between networks and matroids by constructing "solvably equivalent" pairs of networks and matroids via index codes with their own construction method; the network has a vector-linear solution over a field if and only if the matroid has a multilinear representation over the same field. In another recent work [11], Sun et al. studied the matroid structure of single-source networks which they define as network matroid and showed connections between the network matroids and a special class of linear network codes.

In this paper, we further study the matroidal networks introduced by Dougherty et al. [7]. We prove the converse of a theorem in [7] which states that, if a network is scalar-linearly solvable then it is a matroidal network associated with a representable matroid over a finite field. From [7] and our present work, it follows that a network is scalar-linearly solvable if and only if it is a matroidal network associated with a representable matroid over a finite field. The main idea of our work is to construct a scalar-linear network code from the network-matroid mapping between the matroid and network. Thereby, we show a correspondence between scalar-linearly solvable networks and representable matroids over finite fields in the framework of matroidal networks. It follows that determining scalar-linear solvability of a network $\mathcal{N}$ is equivalent to determining the existence of a representable matroid $\mathcal{M}$ over a finite field and a valid network-matroid mapping between $\mathcal{M}$ and $\mathcal{N}$. We also study a relationship between scalar-linear solvability of networks and field characteristics. Using our result and the matroidal network construction method due to Dougherty et al., we note that networks constructed from representable matroids over finite fields are scalar-linearly solvable. The constructed networks are potentially different from the classes of networks that are already known to be scalar-linearly solvable. It is possible that our approach provides a superset, but this is unknown at this time.

The paper is organized as follows. In Section II, we give a network coding model. In Section III, we define matroids and three classes of matroids. In Section IV, we define ma-

troidal networks and provide the construction method due to Dougherty et al. [7]. In Section V, we prove the converse of a theorem by Dougherty et al. in [7] and show a relationship between scalar-linear solvability of networks and field characteristics. In Section VI, we provide an example of scalar-linearly solvable network constructed from a representable matroid over a finite field. In Section VII, we discuss some limitations in generalizing the main result of the paper and conclude.

II. Network Coding

We give a model of algebraic network coding that we will use in this paper. Most of it is adapted from [7].

A *network* $\mathcal{N}$ is a finite, directed, acyclic multigraph given by a 6-tuple $(\nu, \epsilon, \mu, \mathcal{A}, S, R)$ with a node set ν, an edge set ϵ, a message set μ, an alphabet $\mathcal{A}$, a source mapping $S : \nu \to 2^{\mu}$, and a receiver mapping $R : \nu \to 2^{\mu}$. We use a pair of nodes (x, y) to denote a directed edge from node x to node y. For each node x, if $S(x)$ is nonempty then x is a *source* and if $R(x)$ is nonempty then x is a *receiver*. The elements of $S(x)$ are called the *messages generated by* x and the elements of $R(x)$ are called the *messages demanded by* x. An *alphabet* $\mathcal{A}$ is a finite set with at least two elements. Each instance of a message is a vector of elements from the alphabet. For each node x, let $\mathrm{In}(x)$ denote the set of messages generated by x and in-edges of x. Let $\mathrm{Out}(x)$ denote the set of messages demanded by x and out-edges of x. For each node x, we fix an ordering of $\mathrm{In}(x)$ and $\mathrm{Out}(x)$ such that all messages occur before the edges in the resulting lists. In our definition of network, there could be multiple source nodes and receiver nodes with arbitrary demands.

We define edge function, decoding function, message assignment and symbol function with respect to a finite field F of cardinality greater than or equal to $|\mathcal{A}|$. We choose such F so that each element from $\mathcal{A}$ can be uniquely represented with an element from F. Let k and n be positive integers. For each edge $e = (x, y)$, an *edge function* is a map $f_e : (F^k)^{\alpha} \times (F^n)^{\beta} \to F^n$, and for each node $x \in \nu$ and message $m \in R(x)$, a *decoding function* is a map $f_{x,m} : (F^k)^{\alpha} \times (F^n)^{\beta} \to F^k$, where α and β are number of messages generated by x and in-edges of x, respectively. We call k and n the *source dimension* and *edge dimension*, respectively. Each source sends a message vector of length k and each edge carries a message vector of length n. We denote the collections of edge and decoding functions by $\mathcal{F}_e = \{f_e : e \in \epsilon\}$ and $\mathcal{F}_d = \{f_{x,m} : x \in \nu, m \in R(x)\}$. A *message assignment* is a map $a : \mu \to F^k$, i.e., each message is assigned with a vector from F^k. A *symbol function* is a map $s : \epsilon \to F^n$ defined recursively, with respect to $\mathcal{N}$ and $\mathcal{F}_e$, such that for all $e = (x, y) \in \epsilon$,

$$s(e) = f_e(a(m_1), \ldots, a(m_\alpha), s(e_{\alpha+1}), \ldots, s(e_{\alpha+\beta})),$$

where $m_1, \ldots, m_\alpha$ are the messages generated by x and $e_{\alpha+1}, \ldots, e_{\alpha+\beta}$ are the in-edges of x. Note that the symbol function is well-defined as network $\mathcal{N}$ is a directed acyclic multigraph.

A *network code* on $\mathcal{N}$ is a 5-tuple $(F, k, n, \mathcal{F}_e, \mathcal{F}_d)$ where F is a finite field, with $|F| \geq |\mathcal{A}|$. There are several special classes of network codes: routing network codes where edge and decoding functions simply copy input components to output components, linear network codes where edge and decoding functions are linear over F, and nonlinear network codes where edge and decoding functions are nonlinear over F. Vector-linear network codes are linear network codes with $k = n$. Scalar-linear network codes are linear network codes with $k = n = 1$. A network code $(F, k, n, \mathcal{F}_e, \mathcal{F}_d)$ is a *network code solution*, or *solution* for short, if for every message assignment $a : \mu \to F^k$,

$$f_{x,m}(a(m_1), \ldots, a(m_\alpha), s(e_{\alpha+1}), \ldots, s(e_{\alpha+\beta})) = a(m),$$

for all $x \in \nu$ and $m \in R(x)$. Note that $m_1, \ldots, m_\alpha$ are messages generated by x and $e_{\alpha+1}, \ldots, e_{\alpha+\beta}$ are in-edges of x. A network $\mathcal{N}$ is *routing-solvable* if it has a routing network code solution. Similarly, we say that network $\mathcal{N}$ is *linearly solvable* (*scalar-linearly solvable, vector-linearly solvable, nonlinearly solvable*) if it has a *linear* (*scalar-linear, vector-linear, nonlinear*) network code solution.

A *global linear network code* is a 5-tuple $(F, k, n, \phi_{msg}, \phi_{edge})$ where F is a finite field, $|F| \geq |\mathcal{A}|$, k is the source dimension, n is the edge dimension,

1) ϕ_{msg} is the global coding vector function on messages, $\phi_{msg} : \mu \to (F^{k\times k})^{|\mu|}$, such that for message m, $\phi_{msg}(m) = (M_1, \ldots, M_{|\mu|})^t$ where M_i is a $k \times k$ matrix over F, and
2) ϕ_{edge} is the global coding vector function on edges, $\phi_{edge} : \epsilon \to (F^{n\times k})^{|\mu|}$, such that for each edge e, $\phi_{edge}(e) = (M_1, \ldots, M_{|\mu|})^t$ where M_i is a $n \times k$ matrix over F.

A global linear network code $(F, k, n, \phi_{msg}, \phi_{edge})$ is a *global linear network code solution*, if $|F| \geq |\mathcal{A}|$ and the following conditions are satisfied:

1) for each message $m \in \mu$, $\phi_{msg}(m) = (0, \ldots, 0, I^{k\times k}, 0, \ldots, 0)^t$ where $I^{k\times k}$ is the $k \times k$ identity matrix over F and is in the coordinate corresponding to message m;
2) for each node $x \in \nu$ and edge $e \in \mathrm{Out}(x)$, if $\phi_{edge}(e) = (M_1, \ldots, M_{|\mu|})^t$ then there exist matrices $C_1, \ldots, C_{\alpha+\beta}$ over F such that $M_i = \sum_{j=1}^{\alpha+\beta} C_j M_i^j$, for $i = 1, \ldots, |\mu|$;
3) for each node $x \in \nu$ and message $m \in \mathrm{Out}(x)$, if $\phi_{msg}(m) = (M_1, \ldots, M_{|\mu|})^t$ then there exist matrices $C'_1, \ldots, C'_{\alpha+\beta}$ over F such that $M_i = \sum_{j=1}^{\alpha+\beta} C'_j M_i^j$, for $i = 1, \ldots, |\mu|$,

where if $m_1, \ldots, m_\alpha$ are messages generated by x and $e_{\alpha+1}, \ldots, e_{\alpha+\beta}$ are in-edges of x, $\phi_{msg}(m_j) = (M_1^j, \ldots, M_{|\mu|}^j)^t$ for $j = 1, \ldots, \alpha$ and $\phi_{edge}(e_j) = (M_1^j, \ldots, M_{|\mu|}^j)^t$ for $j = \alpha + 1, \ldots, \alpha + \beta$; $C_1, \ldots, C_\alpha$ are $n \times k$ matrices and $C_{\alpha+1}, \ldots, C_{\alpha+\beta}$ are $n \times n$ matrices that would appear as coefficients in a linear edge function; and $C'_1, \ldots, C'_\alpha$ are $k \times k$ matrices and $C'_{\alpha+1}, \ldots, C'_{\alpha+\beta}$ are $k \times n$ matrices that would appear as coefficients in a linear decoding function.

To be more specific on parameters k and n, we will use the prefix (k, n) before codes. When k and n are clear from the context, we will sometimes omit them. It is straightforward to check that the notions of linear network code solution and global linear network code solution are equivalent, as noted in previous works in algebraic network coding [3] for the $k = n = 1$ case.

Proposition 1: Let $\mathcal{N} = (\nu, \epsilon, \mu, \mathcal{A}, S, R)$ be a network. Then $\mathcal{N}$ has a (k, n) linear network code solution if and only if it has a (k, n) global linear network code solution.

In this paper, we will focus on scalar-linear network codes, that is linear network codes with $k = n = 1$.

III. Matroids

We define matroids and three classes of matroids. See [12] for more background on matroids.

Definition 2: A matroid $\mathcal{M}$ is an ordered pair $(\mathcal{S}, \mathcal{I})$ consisting of a set $\mathcal{S}$ and a collection $\mathcal{I}$ of subsets of $\mathcal{S}$ satisfying the following conditions:

1) $\emptyset \in \mathcal{I}$;
2) If $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$;
3) If I_1 and I_2 are in $\mathcal{I}$ and $|I_1| < |I_2|$, then there is an element e of $I_2 \setminus I_1$ such that $I_1 \cup \{e\} \in \mathcal{I}$.

The set $\mathcal{S}$ is called the *ground set* of the matroid $\mathcal{M}$. A subset X of $\mathcal{S}$ is an *independent set* if it is in $\mathcal{I}$; X is a *dependent set* if not. A *base* B of $\mathcal{M}$ is a maximal independent set; for all elements $e \in \mathcal{S} \setminus B$, $B \cup \{e\} \notin \mathcal{I}$. It can be shown that all bases have the same cardinality. A *circuit* of $\mathcal{M}$ is a minimal dependent set; for all elements e in C, $C \setminus \{e\} \in \mathcal{I}$. For each matroid, there is an associated function r called *rank* that maps the power set $2^{\mathcal{S}}$ into the set of nonnegative integers. The rank of a set $X \subseteq \mathcal{S}$ is the maximum cardinality of an independent set contained in X.

Definition 3: Two matroids $\mathcal{M}_1 = (\mathcal{S}_1, \mathcal{I}_1)$ and $\mathcal{M}_2 = (\mathcal{S}_2, \mathcal{I}_2)$ are isomorphic if there is a bijection map ψ from $\mathcal{S}_1$ to $\mathcal{S}_2$ such that for all $X \subseteq \mathcal{S}_1$, X is independent in $\mathcal{M}_1$ if and only if $\psi(X)$ is independent in $\mathcal{M}_2$.

Definition 4 (Uniform Matroids): Let c, d be nonnegative integers such that $c \leq d$. Let $\mathcal{S}$ be a d-element set and $\mathcal{I}$ be the collection $\{X \subseteq \mathcal{S} : |X| \leq c\}$. We define the uniform matroid of rank c on the d-element set to be $U_{c,d} = (\mathcal{S}, \mathcal{I})$.

Definition 5 (Graphic Matroids): Let G be an undirected graph with the set of edges, $\mathcal{S}$. Let $\mathcal{I} = \{X \subseteq \mathcal{S} : X \text{ does not contain a cycle}\}$. We define the graphic matroid associated with G as $\mathcal{M}(G) = (\mathcal{S}, \mathcal{I})$.

Definition 6 (Representable/Vector Matroid): Let A be a $d_1 \times d_2$ matrix over some field F. Let $\mathcal{S} = \{1, \ldots, d_2\}$ where element i in $\mathcal{S}$ corresponds to the ith column vector of A and $\mathcal{I} = \{X \subseteq \mathcal{S} : \text{corresponding column vectors form an independent set}\}$. We define the vector matroid associated with A as $\mathcal{M}(A) = (\mathcal{S}, \mathcal{I})$. A matroid $\mathcal{M}$ is F-representable if it is isomorphic to a vector matroid of some matrix over field F. A matroid is representable if it is representable over some field. Note that F is not necessarily finite.

The bases of $U_{c,d} = (\mathcal{S}, \mathcal{I})$ are exactly subsets of $\mathcal{S}$ of cardinality c and the circuits are subsets of $\mathcal{S}$ of cardinality $c+1$. Each base of $\mathcal{M}(G)$ is a spanning forest of G, hence an union of spanning trees in connected components of G, and each circuit is a single cycle within a connected component. It is known that the graphic matroids are representable over any field F. On the other hand, the uniform matroid $U_{2,4}$ is not representable over $GF(2)$.

IV. Matroidal Networks

We define matroidal networks and present a method for constructing matroidal networks from matroids; for more details and relevant results, we refer to [7].

Definition 7: Let $\mathcal{N}$ be a network with message set μ, node set ν, and edge set ϵ. Let $\mathcal{M} = (\mathcal{S}, \mathcal{I})$ be a matroid with rank function r. The network $\mathcal{N}$ is a *matroidal network* associated with $\mathcal{M}$ if there exists a function $f : \mu \cup \epsilon \to \mathcal{S}$, called the *network-matroid mapping*, such that the following conditions are satisfied:

1) f is one-to-one on μ;
2) $f(\mu) \in \mathcal{I}$;
3) $r(f(\mathrm{In}(x))) = r(f(\mathrm{In}(x) \cup \mathrm{Out}(x)))$, for every $x \in \nu$.

We define $f(A)$ to be $\{f(x) \,|\, x \in A\}$ for a subset A of $\mu \cup \epsilon$.

Theorem 8 (Construction Method): Let $\mathcal{M} = (\mathcal{S}, \mathcal{I})$ be a matroid with rank function r. Let $\mathcal{N}$ denote the network to be constructed, μ its message set, ν its node set, and ϵ its edge set. Then the following construction method will construct a matroidal network $\mathcal{N}$ associated with $\mathcal{M}$. We do not address issues of complexity of the method.

We choose the alphabet $\mathcal{A}$ to be any set with at least two elements. The construction will simultaneously construct the network $\mathcal{N}$, the network-matroid mapping $f : \mu \cup \epsilon \to \mathcal{S}$, and an auxiliary function $g : \mathcal{S} \to \nu$, where for each $x \in \mathcal{S}$, $g(x)$ is either

1) a source node with message m and $f(m) = x$; or
2) a node with in-degree 1 and whose in-edge e satisfies $f(e) = x$.

The construction is completed in 4 steps and each step can be completed in potentially many different ways:

Step 1: Choose any base $B = \{b_1, \ldots, b_{r(\mathcal{S})}\}$ of $\mathcal{M}$. Create network source nodes $n_1, \ldots, n_{r(\mathcal{S})}$ and corresponding messages $m_1, \ldots, m_{r(\mathcal{S})}$, one at each node. Let $f(m_i) = b_i$ and $g(b_i) = n_i$.

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

1) a new node y and edges $e_1, \ldots, e_j$ such that e_i connects $g(x_i)$ to y. Let $f(e_i) = x_i$.
2) a new node n_0 with a single in-edge e_0 that connects y to n_0. Let $f(e_0) = x_0$ and $g(x_0) = n_0$.

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

Step 4: (can be repeated arbitrarily many times).
Choose a base $B = \{x_1, \ldots, x_{r(\mathcal{S})}\}$ of $\mathcal{M}$ and create a

receiver node y that demands all the network messages and has in-edges $e_1, \ldots, e_{r(\mathcal{S})}$ where e_i connects $g(x_i)$ to y. Let $f(e_i) = x_i$.

The following theorem is from [7]. The original theorem states with a representable matroid, but the same proof still works with a representable matroid over a finite field.

Theorem 9: If a network is scalar-linearly solvable over some finite field, then the network is matroidal. Furthermore, the network is associated with a representable matroid over a finite field.

V. Scalar-linear Solvability

We prove the converse of Theorem 9 and that a network is scalar-linearly solvable over a finite field of characteristic p if and only if the network is a matroidal network associated with a representable matroid over a finite field of characteristic p. In what follows, we assume that $d_2 \geq d_1$.

Lemma 10: Let A be a $d_1 \times d_2$ matrix over a finite field F and $\mathcal{M}(A)$ be the corresponding representable matroid. Then there exists an arbitrarily large finite field F' and a $d_1 \times d_2$ matrix A' over F' such that the corresponding matroid $\mathcal{M}(A')$ is isomorphic to $\mathcal{M}(A)$.

Proof: We show that any finite field F' that contains F as a subfield works; for instance, extension fields of F. We consider the same matrix A over F', so choose $A' = A$, and show that a set of column vectors of A is independent over F if and only if it is independent over F'. Assume columns $v_1, \ldots, v_k$ are dependent by some scalars a_i's in F, $a_1 v_1 + \cdots + a_k v_k = 0$. Since F' contains F, all operations with elements of the subfield F stay in the subfield, and the same scalars still work in F', i.e., $a_1 v_1 + \cdots + a_k v_k = 0$ in F'. Hence, the vectors are dependent over F'. Assume column vectors $v_1, \ldots, v_k$ are independent over F. We extend the set of vectors to a basis of F^{d_1}. Then the matrix formed by the basis has a nonzero determinant over F. By similar reasons as before, the same matrix has a nonzero determinant when considered as a matrix over F'. Hence, the column vectors of the basis matrix are independent over F' and, in particular, the column vectors $v_1, \ldots, v_k$ are independent over F'. ∎

Theorem 11: If a network $\mathcal{N}$ is matroidal and is associated with a representable matroid over a finite field F, then $\mathcal{N}$ is scalar-linearly solvable.

Proof: Let $\mathcal{N} = (\nu, \epsilon, \mu, \mathcal{A}, S, R)$ be a matroidal network. Let A be the $d_1 \times d_2$ matrix over the finite field F such that $\mathcal{N}$ is a matroidal network associated with the corresponding matroid $\mathcal{M}(A) = (\mathcal{S}, \mathcal{I})$. By Lemma 10, we assume that the finite field F is large enough to represent all elements in $\mathcal{A}$, i.e., $|F| \geq |\mathcal{A}|$. By Definition 7, there exists a network-matroid mapping $f : \mu \cup \epsilon \to \mathcal{S}$. Assume $r(\mathcal{S}) = d_1$; otherwise we remove redundant rows without changing the structure of the matroid. Let $f(\mu) = \{i_1, \ldots, i_{|\mu|}\}$. As $f(\mu) \in \mathcal{I}$, the columns indexed by $f(\mu)$ form an independent set. We extend $f(\mu)$ to a basis B of F^{d_1}, if necessary, by adding column vectors of A. Without loss of generality, assume the first d_1 columns of A form the basis B after reordering. By performing elementary row operations, we uniquely express A in the form

$$A = [I_{d_1} \mid A']$$

where A' is a $d_1 \times (d_2 - d_1)$ matrix and such that $\{i_1, \ldots, i_{|\mu|}\}$ now corresponds to the first $|\mu|$ columns of A. Note that the structure of the corresponding matroid stays the same. We introduce dummy messages $m_{|\mu|+1}, \ldots, m_{d_1}$, if necessary, by adding a disconnected node that generates these messages. We assign global coding vectors on the resulting $\mathcal{N}$ as follows:

1) for each edge e, let $\phi_{edge}(e) = A_{f(e)}$; and
2) for each message m, let $\phi_{msg}(m) = A_{f(m)}$,

where A_i denotes the ith column of A. We show that the global linear network code defined above is valid and satisfies all the demands. For each node $x \in \nu$, we have $r(f(\mathrm{In}(x))) = r(f(\mathrm{In}(x) \cup \mathrm{Out}(x)))$. It follows that for each edge $e \in \mathrm{Out}(x)$, $A_{f(e)}$ is a linear combination of $\{A_{f(e')} : e' \in \mathrm{In}(x)\}$. Equivalently, $\phi_{edge}(e)$ is a linear combination of coding vectors in $\{\phi_{msg}(m) : m \in \mathrm{In}(x)\} \cup \{\phi_{edge}(e) : e \in \mathrm{In}(x)\}$. For each message $m \in \mathrm{Out}(x)$, $A_{f(m)}$ is a linear combination of $\{A_{f(e')} : e' \in \mathrm{In}(x)\}$. Similarly, $\phi_{msg}(m)$ is a linear combination of coding vectors in $\{\phi_{msg}(m) : m \in \mathrm{In}(x)\} \cup \{\phi_{edge}(e) : e \in \mathrm{In}(x)\}$. Note, furthermore, that $\phi_{msg}(m)$ is the standard basis vector corresponding to m. It follows that the global linear network code $(F, \mathcal{F}_e, \mathcal{F}_d)$ thus defined is a global linear network code solution. Removing the dummy messages, it follows that $\mathcal{N}$ is scalar-linearly solvable. ∎

Given an arbitrary matrix A, assigning its column vectors as global coding vectors will not give a global linear network code solution necessarily. In essence, the theorem shows that, while we cannot use column vectors of A directly, we can do the described operations to produce an equivalent representation of A from which we can derive a global linear network code solution. From Theorems 8 and 11, we obtain a method for constructing scalar-linearly solvable networks: pick any representable matroid over a finite field F and construct a matroidal network $\mathcal{N}$ using Theorem 8. Combining Theorems 9 and 11, we obtain the following theorem.

Theorem 12: A network is scalar-linearly solvable if and only if the network is a matroidal network associated with a representable matroid over a finite field.

One implication of the theorem is that the class of scalar-linearly solvable networks in the algebraic network coding problem corresponds to the class of representable matroids over finite fields in the framework of matroidal networks. In effect, our results show a connection between scalar-linearly solvable networks, which are tractable networks for network coding, and representable matroids over finite fields, which are also particularly tractable in terms of description size.

In light of Dougherty et al.'s approach [7], [8], relationships between field characteristics and linear solvability of matroidal networks are important. In the case of scalar-linear network codes, we fully characterize a relationship with the following theorem. Note that a network might be a matroidal network with respect to more than one representable matroids of

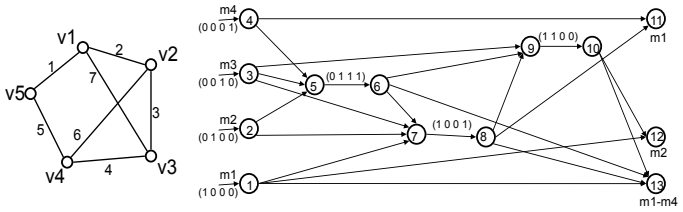

Fig. 1. Graph G and a matroidal network $\mathcal{N}$ constructed from $\mathcal{M}(G)$.

different field characteristics and so is possibly scalar-linearly solvable with respect to fields of different characteristics.

Theorem 13: A network is scalar-linearly solvable over a finite field of characteristic p if and only if the network is a matroidal network associated with a representable matroid over a finite field of characteristic p.

Proof: We extend Theorems 9 and 11 and Lemma 10 to include field characteristic p, and the statement follows. ■

Corollary 14: Any matroidal network $\mathcal{N}$ associated with an uniform matroid is scalar-linearly solvable over a sufficiently large finite field of any characteristic. The same holds for the graphic matroids.

Proof: It is straightforward to show that for any uniform matroid $\mathcal{M}$ and a prime p, there is a sufficiently large finite field of characteristic p and a matrix A such that $\mathcal{M}$ is a representable matroid associated with A over F. The same is true for graphic matroids. ■

As a consequence, any matroidal networks constructed from uniform or graphic matroids will not have interesting properties like those constructed from the Fano and non-Fano matroids in Dougherty et al. [7], [8].

VI. An Example

In this section, we provide an example of a scalar-linearly solvable network that follows from Theorem 11. As mentioned before, we get a method for constructing scalar-linearly solvable networks from Theorems 8 and 11: pick any representable matroid over a finite field F and construct a matroidal network.

Assume $\mathcal{A} = \{0, 1\}$. Consider the graph G and the matroidal network $\mathcal{N}$ constructed from $\mathcal{M}(G)$ in Fig. 1. The ground set $\mathcal{S}$ of $\mathcal{M}(G)$ is $\{1, \ldots, 7\}$, representing the edges of G. Nodes 1-4 are the source nodes and nodes 11-13 are the receiver nodes. $\mathcal{M}(G)$ is a representable matroid over field $\mathbb{F}_2$ and by Theorem 11, the network has a scalar-linear network code solution over $\mathbb{F}_2$, as shown by the global coding vectors on $\mathcal{N}$ in Fig. 1. This example shows that our results provide networks which are different from the networks previously known to be scalar-linearly solvable such as multicast, 2-level multicast and disjoint multicast. It is possible that network $\mathcal{N}$ can be constructed from a set of polynomials as in Dougherty et al. [4] or via index codes as in El Rouayheb et al. [10].

VII. Discussion and Conclusion

In this paper, we showed that any matroidal network associated with a representable matroid over a finite field is scalar-linearly solvable. Combined with an earlier result of Dougherty et al., it follows that a network is scalar-linearly solvable if and only if it is a matroidal network associated with a representable matroid over a finite field. It also follows that determining scalar-linear solvability of a network is equivalent to finding a representable matroid over a finite field and a valid network-matroid mapping. We also showed a relationship between scalar-linear solvability of networks and field characteristics. As a result, we obtained a method for generating scalar-linearly solvable networks from representable matroids over finite fields and a set of scalar-linearly solvable networks that is possibly different from those networks we already know to be scalar-linearly solvable.

Unfortunately, the results presented in this paper do not seem to generalize to vector-linear network coding or more general network coding schemes. The difficulty is that the matroid structure requires that a subset of the ground set of a matroid is either independent or dependent, but what this corresponds to in vector-linear codes, for instance, is not clear. Instead of vectors over fields, we now have vectors over rings (matrices over a field, to be more specific) in vector-linear network coding and we are unaware of suitable matroids on vectors over rings for our purpose. In fact, El Rouayheb et al. [10] also made a similar observation and suggested that FD-relations are more related to networks than are matroids.

Acknowledgment

This material is based upon work supported by the Air Force Office of Scientific Research (AFOSR) under award No. 016974-002.

References

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

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

[3] R. Koetter and M. Médard, "An algebraic approach to network coding," *Networking, IEEE/ACM Transactions on*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[4] R. Dougherty, C. Freiling, and K. Zeger, "Linear network codes and systems of polynomial equations," *Information Theory, IEEE Transactions on*, vol. 54, no. 5, pp. 2303–2316, May 2008.

[5] M. Médard, M. Effros, T. Ho, and D. Karger, "On coding for non-multicast networks," in *Proc. 41st Annual Allerton Conference on Communication, Control and Computing*, Oct. 2003.

[6] A. R. Lehman and E. Lehman, "Complexity classification of network information flow problems," in *Proceedings of the ACM-SIAM Symposium on Discrete Algorithms*, Jan. 2004, pp. 142–150.

[7] R. Dougherty, C. Freiling, and K. Zeger, "Networks, matroids, and non-shannon information inequalities," *Information Theory, IEEE Transactions on*, vol. 53, no. 6, pp. 1949–1969, June 2007.

[8] ——, "Matroidal networks," in *Allerton Conference on Communication, Control, and Computing*, September 2007.

[9] ——, "Insufficiency of linear coding in network information flow," *Information Theory, IEEE Transactions on*, vol. 51, no. 8, pp. 2745–2759, Aug. 2005.

[10] S. El Rouayheb, A. Sprintson, and C. Georghiades, "A new construction method for networks from matroids," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, 28 2009-July 3 2009, pp. 2872–2876.

[11] Q. Sun, S. T. Ho, and S.-Y. Li, "On network matroids and linear network codes," in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, 6-11 2008, pp. 1833 –1837.

[12] J. Oxley, *Matroid Theory*. New York: Oxford Univ. Press, 1992.