A New Construction Method for Networks from Matroids

Salim El Rouayheb, Alex Sprintson, and Costas Georghiades
Department of Electrical and Computer Engineering
Texas A&M University, College Station, TX 77843
{salim, spalex, c-georghiades}@ece.tamu.edu

***Abstract*—We study the problem of information flow in communication networks with noiseless links in which the dependency relations among the data flowing on the different network edges satisfy matroidal constraints. We present a construction that maps any given matroid to a network that admits vector linear network codes over a certain field if and only if the matroid has a multilinear representation over the same field. This new construction strengthens previous results in the literature and, thus, establishes a deeper connection between network coding and matroid theory. We also explore another, more general, mathematical construct referred to as *FD-relation* which characterizes a more general class of networks.**

I. Introduction

Traditionally, the problem of communicating information in networks with noiseless links was addressed using techniques inspired by the study of commodity flows in transportation networks, where the only difference taken into account between commodities and information was the possibility of duplicating information by copying. In 2000, Ahlswede et al. presented [1] a novel and original approach to this problem that formed the new paradigm of network coding. Network Coding techniques extend the capability of intermediate network nodes from mere copying to "mixing", i.e. encoding of, the different data packets received on their incoming edges. They proved that the classical approach of simply routing is sub-optimal and gave a better understanding of information flows in networks.

Matroids are mathematical structures that were first introduced and studied by Whitney [2] in 1935 in an effort to capture the abstract properties of the notions of dependence and independence encountered in several disciplines, such as linear algebra. These concepts appear also in probability theory and thereof in information theory in a more general form, where the correlation between different information sources can be quantified using Shannon's entropy function. Matroid theory has now grown into a mature field of discrete mathematics rich in interesting results and techniques and also in open problems. References [3] and [4] can be consulted for a detailed exposition of this theory.

Related Work

Initial work on network coding focused on establishing *multicast* connections. It was shown in [1] and [5] that the capacity of a multicast network, i.e., the maximum number of packets that can be sent from the source s to a set T of terminals per time unit is equal to the minimum capacity of all the cuts that separate the source s from any terminal $t \in T$. In a subsequent work, Koetter and Médard [6] developed an algebraic framework for network coding and investigated linear network codes for directed graphs with cycles. This framework was used by Ho et al. [7] to show that linear network codes can be efficiently constructed through a randomized algorithm. Jaggi et al. [8] proposed a deterministic polynomial-time algorithm for finding feasible network codes in multicast networks. References [9], [10] provide a comprehensive overview of network coding.

Dougherty et al. [11], [12] investigated the application of results in matroid theory to the general problem of information flow in networks. They introduced the class of matroidal networks and described a method for building a matroidal network from a given matroid. This construction has been applied on specific matroids to prove important results in the field such as the insufficiency of Shannon-type information inequalities and linear network coding for, respectively, computing and achieving network capacity. The authors of [13] associate with every multicast network a matroid based on the structure of edge-disjoint paths in the network. Moreover, they study the relation between the obtained matroid and linear network codes corresponding to the original network.

Contributions

We present a new method for building networks associated with matroids. This construction maps any given matroid to a network such that the obtained network has a vector linear solution over a certain field if and only if the matroid has a multilinear representation over the same field. A major intermediate step in our construction is building an *index code* [14], [15] that capture important properties of the given matroid; the network description then follows immediately. This construction establishes a strong relation between network coding and matroid theory, and constitutes a means to apply numerous results in the rich field of matroid theory to communication problems in networks.

In contrast to the method described in [12], the network obtained by our construction reflects exactly all the dependency and independency relations in the given matroid which ties the existence of network codes to the representability properties of the matroid.

We also explore another, more general, mathematical construct called *FD-relation* which has the advantage of better representing networks.

Organization

The rest of the paper is organized as follows. In Section II we discuss our model for network codes and index codes.

In Section III, we define matroids and discuss the notion of their multilinear representation. In section IV we present our main theorem which describes the relation between index codes and matroid theory. In section V, we complete our construction by showing the method of constructing networks from index codes. Next, in section VI, we focusing on FD-relations and their applications in representing data flow in networks. Finally, conclusions appear in Section VII.

II. Model

In this section, we define network codes and give a formulation of the related index coding problem adopting the same models described in [15] .

A. Network Coding

Let $G(V,E)$ be a directed acyclic graph with vertex set V and edge set $E \subset V \times V$. For each edge $e(u,v) \in E$, we define the in-degree of e to be the in-degree of its tail node u, and its out-degree to be the out-degree of its head node v. Furthermore, we define $\mathcal{P}(e)$ to be the set of the parent edges of e, i.e., $\mathcal{P}(e(u,v)) = \{(w,u);\ (w,u) \in E)\}$. Let $S \subset E$ be the subset of edges in E of zero in-degree and let $D \subset E$ be the subset of edges of zero out-degree. We refer to edges in S as *input* edges, and those in D as *output* edges. Also, we define $m = |E|$ to be the total number of edges, $k = |S|$ be the total number of input edges, and $d = |D|$ be the total number of output edges. Moreover, we assume that the edges in E are indexed from 1 to m such that $S = \{e_1, \ldots, e_k\}$ and $D = \{e_{m-d+1}, \ldots, e_m\}$.

We model a communication network by a pair $\mathcal{N}(G(V,E),\delta)$ formed by a graph $G(V,E)$ and an onto function $\delta : D \longrightarrow S$ from the set of output edges to the set of input edges. We assume that the tail node of each input edge e_i, $i = 1, \ldots, k$ holds a message x_i, also denoted as $x(e_i)$. Each message $x_i = (x_{i1}, \ldots, x_{in})$ belongs to a certain alphabet Σ^n, for a positive integer n. The edges of the graph represent communication links of unit capacity, i.e., each link can transmit one message per channel use. The function δ specifies for each output edge e_i, $i = m-d+1, \ldots, m$, the source message $x(\delta(e_i))$ required by its head node. We refer to δ as the *demand function*. We denote by $\xi = (x_{11}, \ldots, x_{1n}, \ldots, x_{k1}, \ldots, x_{kn}) \in \Sigma^{nk}$ the concatenation of all packets at the input edges.

Definition 1 (Network Code): A q-ary *network code* of block length n, or an (n,q) network code, for the network $\mathcal{N}(G(V,E),\delta)$ is a collection

$$\mathcal{C} = \{f_e = (f_e^1, \ldots, f_e^n); e \in E, f_e^i : \Sigma^{nk} \longrightarrow \Sigma, i = 1, \ldots, n\},$$

of functions, called *global encoding* functions, indexed by the edges of G, that satisfy, for all $\xi \in \Sigma^{nk}$, the following conditions:

(N1) $f_{e_i}(\xi) = x_i$, for $i = 1, \ldots, k$;
(N2) $f_{e_i}(\xi) = x(\delta(e_i))$, for $i = m-d+1, \ldots, m$;
(N3) For each $e = (u,v) \in E \setminus S$ with $\mathcal{P}(e) = \{e_1, \ldots, e_{p_e}\}$, there exists a function $\phi_e : \Sigma^{np_e} \longrightarrow \Sigma^n$, referred to as the *local encoding function* of e, such that $f_e(\xi) = \phi_e(f_{e_1}(\xi), \ldots, f_{e_{p_e}}(\xi))$, where p_e is the in-degree of e, and $\mathcal{P}(e)$ is the set of parent edges of e.

When $n = 1$, the network code is referred to as a *scalar* network code. Otherwise, when $n > 1$, it is called a *vector* or a *block* network code. We are interested here in linear network codes where Σ is a finite field $\mathbb{F}$, and all the global and local encoding functions are linear functions of the packets x_{ij}.

B. Index Coding

The Index Coding problem was recently introduced in [14] and has been the subject of several studies [16], [17]. An instance of the Index Coding problem includes a server/transmitter that holds a set of information messages X and a set of receivers R, each one of them has some side information represented by a subset of X, known to the server, and demands another subset of X. The server can broadcast encodings of messages in X over a noiseless channel. The objective is to identify an encoding scheme, known as index code, that satisfies the demands of all clients with the minimum number of transmissions. Although, there is no network or graph involved in the formulation of the index coding problem, index codes and network codes turned out to be strongly related and this relation was investigated in [15].

Formally, an instance of the Index Coding problem $\mathcal{I}(X,R)$ includes

1) A set of k messages $X = \{x_1, \ldots, x_k\}$,
2) A set of clients or receivers $R \subseteq \{(x,H); x \in X, H \subseteq X \setminus \{x\}\}$.

Here, X represents the set of messages available at the sender. Each message x_i belongs to a certain alphabet Σ^n. A client is represented by a pair (x,H), where $x \in X$ is the message required by the client, and $H \subseteq X$ is set of messages available to the client as side information. Here also we assume that each message x_i can be divided into n packets, and we write $x = (x_{i1}, \ldots, x_{in}) \in \Sigma^n$. We denote by $\xi = (x_{11}, \ldots, x_{1n}, \ldots, x_{k1}, \ldots, x_{kn}) \in \Sigma^{nk}$.

Definition 2 (Index Code): An (n,q) index code for $\mathcal{I}(X,R)$ is a function $f : \Sigma^{nk} \longrightarrow \Sigma^c$, for a certain integer c, satisfying that for each client $\rho = (x,H) \in R$, there exists a function $\psi_\rho : \Sigma^{c+n|H|} \longrightarrow \Sigma^n$ such that $\psi_\rho(f(\xi),(x_i)_{x_i \in H}) = x$, $\forall \xi \in \Sigma^{nk}$.

We refer to c as the *length* of the index code. Define $\ell(n,q)$ to be the smallest integer c such that the above condition holds for the given alphabet size q and block length n. If the index code satisfies $c = \ell(n,q)$, it is said to be *optimal*.

We refer to ψ_ρ as the decoding function for client ρ. With a linear index code, the alphabet Σ is a field and the functions f and ψ_ρ are linear in variables x_{ij}. If $n = 1$ the index code is called a scalar code, and for $n > 1$, it is called a vector or block code.

Given n and q, the Index Coding problem consists of finding an optimal index code for an index coding instance. for a given instance $\mathcal{I}(X,R)$ of the Index Coding problem, we define by $\lambda(n,q) = \ell(n,q)/n$ the transmission rate of the optimal solution over an alphabet of size q.

Let $\mu(\mathcal{I})$ be the maximum of the total number of messages requested by a set of clients with identical side information, i.e., $\mu(\mathcal{I}) = \max_{Y \subseteq X} |\{x_i; (x_i, Y) \in R\}|$. Then, it is easy to verify that the optimal rate $\lambda(n,q)$ is lower bounded by $\mu(\mathcal{I})$, independently of the values of n and q.

Definition 3: Let $\mathcal{I}(X,R)$ be an instance of the Index Coding problem. Then, an index code for $\mathcal{I}(X,R)$ that achieves $\lambda(n,q) = \mu(\mathcal{I})$ is referred to as a *perfect index code*.

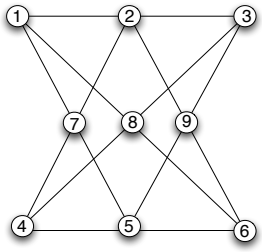

Fig. 1. A graphical representation of the non-Pappus matroid of rank 3 [3, p.43]. Cycles are represented by straight lines.

III. Matroids

There are many different equivalent definitions of a matroid. The following one is the most useful for our analysis here.

A matroid $\mathcal{M}(Y,r)$ is a couple formed by a set Y and a function $r: 2^Y \longrightarrow \mathbb{N}_0$, where 2^Y is the power set of Y and $\mathbb{N}_0$ is the set of non-negative integer numbers $\{0,1,2,\dots\}$, satisfying the following three conditions:

(M1) $r(A) \leq |A|$ for $\forall A \subseteq Y$;
(M2) $r(A) \leq r(B)$ for $\forall A \subseteq B \subseteq Y$;
(M3) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$ for $\forall A, B \subseteq Y$.

The set Y is called the *ground set* of the matroid $\mathcal{M}$. The function r is called the *rank function* of the matroid. The rank $r_{\mathcal{M}}$ of the matroid $\mathcal{M}$ is defined as $r_{\mathcal{M}} = r(Y)$. We refer to $B \subseteq Y$ as an *independent* set if $r(B) = |B|$, otherwise, it is referred to as a *dependent* set. A maximal independent set is referred to as a *basis*. It can be shown that all bases in a matroid have the same number of elements. In fact, for any basis B, it holds that $r(B) = |B| = r_{\mathcal{M}}$. A minimal dependent subset $C \subseteq Y$ is referred to as a *circuit*. For each element c of C it holds that $r(C \setminus \{c\}) = |C| - 1 = r(C)$. We define $\mathfrak{B}(\mathcal{M})$ to be the set of all the bases of the matroid $\mathcal{M}$, and $\mathfrak{C}(\mathcal{M})$ be the set of all circuits of $\mathcal{M}$.

Definition 4: Let $Y = \{y_1, \dots, y_m\}$ be a set whose elements are indexed by the integers from 1 to m. For any collection of m matrices $M_1, \dots, M_m \in \mathbb{M}_{\mathbb{F}}(n,k)$, the set of $n \times k$ matrices over the field $\mathbb{F}$, and any subset $I = \{y_{i_1}, \dots, y_{i_\delta}\} \subseteq Y$, with $i_1 < \dots < i_\delta$, define

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

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

Definition 5: Let $\mathcal{M}(Y,r)$ be a matroid of rank $r_{\mathcal{M}} = k$ on the ground set $Y = \{y_1, \dots, y_m\}$. The matroid $\mathcal{M}$ is said to have a multilinear representation of dimension n, or an n-linear representation, over a field $\mathbb{F}$, if there exist matrices $M_1, \dots, M_m \in \mathbb{M}_{\mathbb{F}}(kn, n)$ such that, $\forall I \subseteq Y$,

$$\operatorname{rank}(M_I) = n \cdot r(I). \tag{1}$$

Linear representation corresponding to the case of $n = 1$ is the most studied case in matroid theory, see for example [3, Chapter 6]. Multilinear representation is a generalization of this concept from vectors to vector spaces, and was discussed in [18], [19].

Example 6: The uniform matroid $U_{2,3}$ is defined on a ground set $Y = \{y_1, y_2, y_3\}$ of three elements, such that $\forall I \subseteq Y$ and $|I| \leq 2, r(I) = |I|$, and $r(Y) = 2$. It is easy to verify that matrices $M_1 = [0 \quad 1]^T, M_2 = [0 \quad 1]^T, M_3 = [1 \quad 1]^T$ form a linear representation of $U_{2,3}$ of dimension 1 over any field. This will automatically induce a multi-linear representation of dimension 2, for instance, of $U_{2,3}$ over any field:

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

Note that there exist matroids that are not linearly representable but admit a multilinear representation. A notable example of this case is the non-Pappus matroid depicted geometrically in Fig. (1). This matroid does not have a linear representation but has a 2-linear one over $GF(3)$ as detailed in [18] and [19].

IV. From Matroids to Index Codes

Starting with a matroid, we describe here the construction of an instance of the index coding problem that captures important properties of the matroid. The existence of corresponding vector linear index codes is then linked to the matroid multilinear representations.

Definition 7: Given a matroid $\mathcal{M}(Y,r)$ of rank k over ground set $Y = \{y_1, \dots, y_m\}$, we define the corresponding Index Coding problem $\mathcal{I}_{\mathcal{M}}(Z,R)$ as follows:

1) $Z = Y \cup X$, where $X = \{x_1, \dots, x_k\}$,
2) $R = R_1 \cup R_2 \cup R_3$ where
   a) $R_1 = \{(x_i, B); B \in \mathfrak{B}(\mathcal{M}), i = 1, \dots, k\}$
   b) $R_2 = \{(y, C \setminus \{y\}); C \in \mathfrak{C}(\mathcal{M}), y \in C\}$
   c) $R_3 = \{(y_i, X); i = 1, \dots, m\}$

Note that $\mu(\mathcal{I}_{\mathcal{M}}) = m$.

Theorem 8: Let $\mathcal{M}(Y,r)$ be a matroid on the set $Y = \{y_1, \dots, y_m\}$, and $\mathcal{I}_{\mathcal{M}}(Z,R)$ be its corresponding Index Coding problem. Then, the matroid $\mathcal{M}$ has an n-linear representation over $\mathbb{F}_q$ if and only if there exists a perfect linear (n,q) index code for $\mathcal{I}_{\mathcal{M}}$.

Proof: First, we assume that in $\mathcal{I}_{\mathcal{M}}(Z,R)$ all messages are split into n packets, and we write $y_i = (y_{i1}, \dots, y_{in})$, $x_i = (x_{i1}, \dots, x_{in}) \in \mathbb{F}_q^n$, $\xi = (x_{11}, \dots, x_{1n}, \dots, x_{k1}, \dots, x_{kn}) \in \mathbb{F}_q^{kn}$, and $\chi = (y_{11}, \dots, y_{1n}, \dots, y_{m1}, \dots, y_{mn}, x_{11}, \dots, x_{1n}, \dots, x_{k1}, \dots, x_{kn}) \in \mathbb{F}_q^{(m+k)n}$.

Let $M_1, \dots, M_m \in \mathbb{M}_{\mathbb{F}_q}(kn, n)$ be an n-linear representation of the matroid $\mathcal{M}$. Consider the following linear map $f(\chi) = (f_1(\chi), \dots, f_m(\chi))$

$$f_i(\chi) = y_i + \xi M_i \in \mathbb{F}_q^n, i = 1, \dots, m.$$

We claim that f is a perfect (n,q) linear index code for $\mathcal{I}_{\mathcal{M}}$. To this end, we show the existence of the decoding functions of condition (I1) for all the clients in R:

- Fix a basis $B = \{y_{i_1}, \dots, y_{i_k}\} \in \mathfrak{B}(\mathcal{M})$, with $i_1 < i_2 < \dots < i_k$, and let $\rho_i = (x_i, B) \in R_1$, $i = 1, \dots, k$. By Eq. (1) $\operatorname{rank}(M_B) = kn$, hence the $kn \times kn$ matrix M_B is invertible. Thus, the corresponding decoding functions can be written as $\psi_{\rho_i} = [f_{i_1} - y_{i_1} | \dots | f_{i_k} - y_{i_k}] U_i$, where the U_i's are the $kn \times n$ the block matrices that form M_B^{-1} in the following way: $[U_i | \dots | U_k] = M_B^{-1}$.

- Let $C = \{y_{i_1}, \ldots, y_{i_c}\} \in \mathfrak{C}(\mathcal{M})$, with $i_1 < i_2 < \cdots < i_c$, and $\rho = (y_{i_1}, C') \in R_2$, with $C' = C - y_{i_1}$. We have $\mathrm{rank}(M_{C'}) = \mathrm{rank}(M_C)$ by the definition of matroid cycles. Therefore, there is a matrix $T \in \mathbb{M}_{\mathbb{F}_q}(cn - n, n)$, such that, $M_{i_1} = M_{C'}T$. Now, note that $[f_{i_2} - y_{i_2}|\ldots|f_{i_c} - y_{i_c}] = \xi M_{C'}$. Therefore, the corresponding decoding function is $\psi_\rho = f_{i_1} - [f_{i_2} - y_{i_2}|\ldots|f_{i_c} - y_{i_c}]T$.
- For all $\rho = (y_i, X) \in R_3, \psi_\rho(f, \xi) = f_i - \xi M_i$.

Since this index code satisfies the lower bound $\mu(\mathcal{I}_\mathcal{M}) = m$, it is a perfect index code.

Now, suppose that $f(\chi) = (f_1(\chi), \ldots, f_m(\chi))$, $f_i(\chi) \in \mathbb{F}_q^n$, is a perfect (n, q) linear index code for $\mathcal{I}_\mathcal{M}$. We will show that this will induce an n-linear representation of the matroid $\mathcal{M}$ over $\mathbb{F}_q$.Due to the clients in R_3, we can assume without loss of generality that the functions $f_i(\chi), i = 1, \ldots, m$, have the following form

$$f_i(\chi) = y_i + \xi A_i, \tag{2}$$

where the A_i's are $kn \times n$ matrices over $\mathbb{F}_q$. We claim that these matrices form an n-linear representation of $\mathcal{M}$ over $\mathbb{F}_q$. To prove this, it suffices to show that the matrices A_i's satisfy Eq. (1) for all the bases and cycles of $\mathcal{M}$.

Let $B \in \mathfrak{B}(\mathcal{M})$ a basis. Then, by Eq. (2), the clients $(x_j, B), j = 1, \ldots, k$, will be able to decode their required messages iff A_B is invertible. Therefore, $\mathrm{rank}(A_B) = nk = nr(B)$.

Let $C \in \mathfrak{C}(\mathcal{M})$ a circuit. Pick $y_{i_1} \in C$ let $C' = C - y_{i_1}$. We have $r(C') = |C| - 1 = |C'|$, i.e., C' is an independent set of the matroid, and there is a basis B of $\mathcal{M}$ such that $C' \subseteq B$ (by the independence augmentation axiom [3, chap. 1]). Thus, from the previous discussion, $A_{C'}$ has full rank, i.e. $\mathrm{rank}(A_{C'}) = (|C| - 1)n$. Now consider the client $\rho = (y_{i_1}, C') \in R_2$, the existence of the corresponding linear decoding function ψ_ρ implies that there exists a matrix $T \in \mathbb{M}_\mathbb{F}(|C|n - n, n)$ such that $A_{i_1} = A_{C'}T$. So, $\mathrm{rank}(A_C) = \mathrm{rank}(A_{C'}) = n(|C| - 1) = nr(C)$. ∎

V. From Index Codes to Networks

In this section, we complete our construction by describing how to build a network from the index coding problem associated with a matroid obtained from the construction discussed in the previous section. This network consists of input edges representing all the messages available at the transmitter and output edges corresponding to the clients where, the availability of the side information is captured by direct edges connecting a client to the corresponding nodes carrying the side information. The noiseless channel is modeled in the network by a set of "bottleneck" edges connected to all the input and output edges.

Definition 9: Let $\mathcal{M}(Y, r)$ be a matroid of rank k defined on the set $Y = \{y_1, \ldots, y_m\}$, and $\mathcal{I}_\mathcal{M}(Z, R)$ the corresponding Index Coding problem as described in Definition 7. We associate to it the 6-partite network $\mathcal{N}(\mathcal{I}_\mathcal{M})$ over the graph $G(V, E)$ constructed as follows:

1) $V \supset V_1 \cup V_2 \cup V_3$, where $V_1 = \{s_1, \ldots, s_{m+k}\}$, $V_2 = \{n'_1, \ldots, n'_m\}$, and $V_3 = \{n''_1, \ldots, n''_m\}$.
2) Connect each node $s_i, i = 1, \ldots, k$, to an input edge carrying an information source x_i at its tail node, and each node $s_i, i = k + 1, \ldots, m + k$, to an input edge carrying an information source y_i.
3) Add edges (s_i, n'_j), for $i = 1, \ldots, m + k$ and $j = 1, \ldots, m$.
4) Add edges (n'_j, n''_j) for $j = 1, \ldots, m$.
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 $j = 1, \ldots, m$.

Theorem 10: The matroid $\mathcal{M}$ has an n-linear representation over $\mathbb{F}_q$ iff the network $\mathcal{N}(\mathcal{I}_\mathcal{M})$ has an (n, q) linear network code.

Proof: Let $f = (f_1, \ldots, f_m), f_i : \mathbb{F}_q^{(m+k)n} \to \mathbb{F}_q^n$, be an (n, q) perfect linear index code for $\mathcal{I}_\mathcal{M}$. Then, taking $f_{(n'_j, n''_j)} = f_j$, for $j = 1, \ldots, m$, will give an (n, q) linear network code for $\mathcal{N}(\mathcal{I}_\mathcal{M})$ (the other edge functions are trivial), and vice versa. The proof follows, then, directly from Theorem 8. ∎

Figure 2 shows a sub-network of the network resulting from the construction of Definition 9 applied to the non-Pappus matroid of Figure 1. Node n_1 represents the clients in the set R_3, n_2 the basis $\{1, 2, 4\}$ of the non-Pappus matroid, and n_3, n_4, n_5 the cycle $\{1, 2, 3\}$. By Theorem 10, this network does not have a scalar linear network code, but has a vector linear code of length 2 over $GF(3)$.

VI. Beyond Matroids: FD-Relations

Theorem 10 suggests that network codes can be regarded as a generalization of the concept of matroid representation. As a matter of fact, matroids, as dependency structures, have to satisfy constraints that do not usually apply to networks. For instance, any subset of the ground set of a matroid has to be either dependent or independent. This is, however, not always the case for the set of edge messages in a network. For instance, the simple network defined on three nodes s, t_1 and t_2, where s carries two information sources x_1, x_2 both demanded by t_1 and t_2, and where there are two edges e_1, e_2 that connects s to t_1, and similarly two other edges e_3, e_4 that connect s to t_2. Two possible network codes over $GF(2)$ might be either $\{f_{e_1} = f_{e_3} = x_1, f_{e_2} = f_{e_4} = x_2\}$ or $\{f_{e_1} = x_1, f_{e_2} = f_{e_4} = x_2, f_{e_3} = x_1 + x_2\}$. Both are valid network codes. But, notice that the messages carried by e_1 and e_3 are linearly dependent in the first case, while independent in the second one. So, the network does not dictate beforehand any relation between the messages on e_1 and e_3. One can also associate to a network code solution for a certain network a *polymatroid* resulting from applying Shannon entropy function to the set of random variables representing the edge messages. The obtained polymatroid, however, captures essentially the properties of the network code, but not the underlying network.

A related concept that captures the properties of networks, better than matroids or polymatroids, is that of *Functional Dependency Relation* or *FD-relation*, which were defined by Matúš in [20] and arise in the field of database theory.

Definition 11 (FD-relation): Let X be a finite set, and $\mathcal{Q}(X) := \{(I, J); I, J \subseteq X\}$. A subset $\mathcal{F}$ of $\mathcal{Q}(X)$ is called an FD-relation on X if it satisfies the following three conditions

1) $I \subseteq J \subseteq X \Rightarrow (I, J) \in \mathcal{F}$,
2) $(I, J) \in \mathcal{F}$ and $(J, K) \in \mathcal{F} \Rightarrow (I, K) \in \mathcal{F}$,

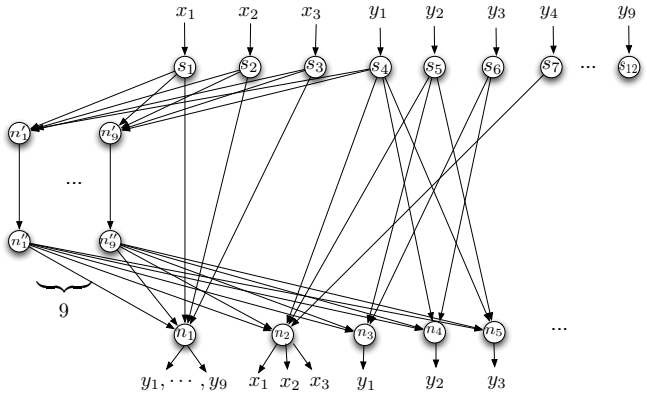

Fig. 2. Part of the network equivalent to the non-Pappus matroid resulting from the construction of Definition 9.

3) $(I, J) \in \mathcal{F}$ and $(I, K) \in \mathcal{F} \Rightarrow (I, J \cup K) \in \mathcal{F}$.

In analogy with the matroid case, one can study representations of FD-relations. For $i \in X$, let f_i be a function defined on a non-empty set B and taking values in a set C. For any subset I of X, define $C_I = \prod_{i \in I} C$, and define $f_I : B \to C_I$, s.t. $f_I(b) = (f_i(b))_{i \in I}, \forall b \in B$. Then, the functions f_i form a *functional representation* [20, example 3] of $\mathcal{F}$ iff

$$\forall (I, J) \in \mathcal{F}, \exists g^I_J : C_I \to C_J, s.t.\ f_J = g^I_J \circ f_I.$$

Given a network $\mathcal{N}(G(V, E), \delta)$, we can define a corresponding FD-relation $\mathcal{F}_\mathcal{N}$ as follows. Let V' be the set of nodes in V not connected to an output edge and of positive out-degree and in-degree, V'' that of nodes connected to an output edge. Define also $\mathcal{P}'(v), \mathcal{C}'(v)$ to be, respectively,the set of edges incoming and outgoing from node v. Then $\mathcal{F}_\mathcal{N}$ is the FD-relation defined on the set E of edges of the network and generated by the following set,

$$\{(\mathcal{P}'(v), \mathcal{C}'(v)); v \in V'\} \cup \{(\mathcal{P}'(v), \delta(\mathcal{C}'(v)); v \in V''\},$$

i.e., the smallest subset of $\mathcal{Q}(E)$ containing the above set and that satisfies the above three conditions. Then, we have the following result that can be easily checked.

Proposition 12: The network $\mathcal{N}$ has an (n, q) network code iff $\mathcal{F}_\mathcal{N}$ has a functional representation with $|B| = q^{kn}$ and $|C| = q^n$.

VII. Conclusion

This paper focused on network codes and their relation to matroid theory. For a given matroid, we presented a method to construct a network such that any multilinear representation of the matroid will induce a vector linear network code for the obtained network over the same field, and vice versa. An important feature of this new construction is the use of the properties of index codes which can be regarded as a sub-family of network codes. Through index codes, we were able to establish a connection, that is stronger then what is already described in the literature, between network coding and matroids. Our result implies that linear index codes are a generalization of the concept of matroid representation. From this point of view, we presented *FD-relations* as structures, more suitable than matroids, to capture the dependencies and independencies that characterizes network and index codes.

References

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Network Information Flow. *IEEE Transactions on Information Theory*, 46(4):1204–1216, 2000.

[2] H. Whitney. On the abstract properties of linear dependence. *Amer. J. Math.*, 57:509–533, 1935.

[3] J. G. Oxley. *Matroid Theory*. Oxford University Press, USA, New York, NY, USA, January 1993.

[4] D.J.A. Welsh. *Matroid Theory*. Academic Press, London, London, 1976.

[5] S.-Y. R. Li, R. W. Yeung, and N. Cai. Linear Network Coding. *IEEE Transactions on Information Theory*, 49(2):371 – 381, 2003.

[6] R. Koetter and M. Medard. An Algebraic Approach to Network Coding. *IEEE/ACM Transactions on Networking*, 11(5):782 – 795, 2003.

[7] T. Ho, R. Koetter, M. Medard, D. Karger, and M. Effros. The Benefits of Coding over Routing in a Randomized Setting. In *Proceedings of the IEEE International Symposium on Information Theory*, 2003.

[8] 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. *IEEE Transactions on Information Theory*, 51(6):1973–1982, 2005.

[9] C. Fragouli and E. Soljanin. *Network Coding Fundamentals (Foundations and Trends in Networking)*. Now Publishers Inc, 2007.

[10] R. Yeung, S-Y. Li, and N. Cai. *Network Coding Theory (Foundations and Trends in Communications and Information Theory)*. Now Publishers Inc, 2006.

[11] R. Dougherty, C. Freiling, and K. Zeger. Insufficiency of linear coding in network information flow. *IEEE Transactions on Information Theory*, 51(8):2745–2759, 2005.

[12] R. Dougherty, C. Freiling, and K. Zeger. Networks, matroids, and non-shannon information inequalities. *IEEE Transactions on Information Theory*, 53(6), June 2007.

[13] Q. Sun, S. T. Ho, and S.-Y.R. Li. On network matroids and linear network codes. *Proc. of IEEE International Symposium on Information Theory (ISIT08)*, 2008.

[14] Z. Bar-Yossef, Y. Birk, T. S. Jayram, and T. Ko. Index coding with side information. In *Proc. of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 197–206, 2006.

[15] S. El Rouayheb, A. Sprintson, and C. N. Georghiades. On the relation between the index coding and the network coding problems. *Proc. of IEEE International Symposium on Information Theory (ISIT08)*, 2008.

[16] S. El Rouayheb, M.A.R. Chaudhry, and A. Sprintson. On the minimum number of transmissions in single-hop wireless coding networks. In *IEEE Information Theory Workshop (Lake Tahoe)*, 2007.

[17] E. Lubetzky and U. Stav. Non-linear index coding outperforming the linear optimum. In *Proc. of the 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 161–167, 2007.

[18] J. Simonis and A. Ashikhmin. Almost affine codes. *Desings, Codes and Cryptography*, 14:179–797, 1998.

[19] F. Matús. Matroid representations by partitions. *Discrete Mathematics*, 203:169–194, 1999.

[20] F. Matúš. Abstract functional dependency structures. *Theoretical Computer Science*, 81(1):117–126, April 1991.