On the Index Coding Problem and its Relation to Network Coding and Matroid Theory

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

***Abstract*— The *index coding* problem has recently attracted a significant attention from the research community due to its theoretical significance and applications in wireless ad-hoc networks. An instance of the index coding problem includes a sender that holds a set of information messages $X = \{x_1, \ldots, x_k\}$ and a set of receivers R. Each receiver $\rho = (x, H)$ in R needs to obtain a message $x \in X$ and has prior *side information* consisting of a subset H of X. The sender uses a noiseless communication channel to broadcast encoding of messages in X to all clients. The objective is to find an encoding scheme that minimizes the number of transmissions required to satisfy the demands of all the receivers.**

In this paper, we analyze the relation between the index coding problem, the more general network coding problem, and the problem of finding a linear representation of a matroid. In particular, we show that any instance of the network coding and matroid representation problems can be efficiently reduced to an instance of the index coding problem. Our reduction implies that many important properties of the network coding and matroid representation problems carry over to the index coding problem. Specifically, we show that *vector linear codes* outperform scalar linear index codes and that vector linear codes are insufficient for achieving the optimum number of transmissions.

***Index Terms*— Network coding, index coding, matroid theory, non-linear codes, side information.**

I. Introduction

In the recent years, there has been a significant interest in utilizing the broadcast nature of the wireless medium for improving the throughput and reliability of ad-hoc wireless networks. The wireless medium allows the sender node to deliver data to several neighboring nodes with a single transmission. Moreover, a wireless receiver node can opportunistically listen to the wireless channel and store all the overheard packets, including those designated for other users. As a result, wireless nodes can obtain side information which, in combination with proper encoding techniques, can lead to a substantial improvement in the performance of the wireless network.

Several recent studies have focused on wireless architectures that use coding techniques to benefit from the broadcast properties of the wireless channel. In particular, [1], [2] proposed new architectures, referred to as COPE and MIXIT, in which routers mix packets from different information sources to increase the overall network throughput. Birk and Kol [3] discussed applications of coding techniques in satellite networks with caching clients with a low-capacity reverse channel.

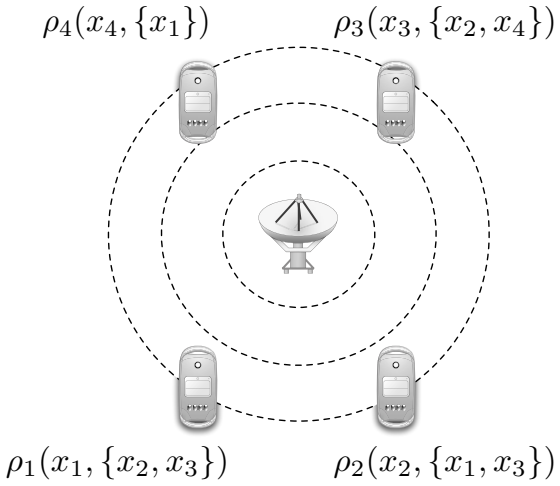

Fig. 1. An instance of the index coding problem with four messages and four clients $\rho_1, \ldots, \rho_i$. Each client is represented by a pair (x, H), where $x \in X$ is the packet demanded by the client, and $H \subseteq X$ represent its side information.

The major challenge in the design of opportunistic wireless networks is to identify an optimal encoding scheme that minimizes the number of transmissions necessary to satisfy all client nodes. This can be formulated as the *index coding* problem that includes a single sender node s and a set R of receiver nodes. The sender has a set of information messages $X = \{x_1, \ldots, x_k\}$ that need to be delivered to the receiver nodes. Each receiver $\rho = (x, H) \in R$ needs to obtain a single message x in X and has prior *side information* comprising a subset H of X. The sender can broadcast the encoding of messages in X to the receivers through a noiseless channel that can transmit one message per channel use. The objective is to find an optimal encoding scheme, referred to as an *index code*, that satisfies all the receiver nodes with zero-error and with minimum number of transmissions.

With *linear coding*, all the messages in X are taken to be elements of a finite field, and all the encoding operations are linear over that field. Figure 1 depicts an instance of the index coding problem that includes a sender with four messages $x_1, \ldots, x_4$ and four clients. We assume that each message is an element of $GF(2^n)$, represented by n bits. Note that the sender can satisfy the demands of all clients, in a straightforward way, by broadcasting all four messages

over the wireless channel. The encoding operation allows to reduce the number of messages by a factor of two. Indeed, it is sufficient to transmit just two messages $x_1 + x_2 + x_3$ and x_1+x_4 (all operations are over $GF(2^n)$) to satisfy the requests of all the clients. This example demonstrates that by using an efficient encoding scheme, the sender can significantly reduce the number of transmissions which, in turn, results in reducing the delay and the energy consumption.

The above example utilizes a *scalar linear* encoding scheme that performs coding over the original messages. In a *vector* encoding scheme, each message is divided into a number of smaller size messages, referred to as *packets*. The vector encoding scheme combines packets from different messages to minimize the number of transmissions. With *vector linear* index coding, all packets are elements of a certain finite field $\mathbb{F}$, and each transmitted packet is a linear combination of the original packets. For example, consider the instance depicted in Figure 1, and suppose that each message $x_i \in GF(2^n)$ (n even) is divided into two packets, $x_i^1, x_i^2 \in GF(2^{\bar{n}})$, of size $\bar{n} = \frac{n}{2}$. Then, a valid vector linear solution comprised of four packets, i.e., two transmissions, would be $\{x_1^1 + x_4^1, x_1^2 + x_4^2, x_1^1 + x_2^1 + x_3^1, x_1^2 + x_2^2 + x_3^2\}$.

Related Work

Witsenhausen [4] considered a related zero-error coding problem with side information. He studied the point-to-point scenario where a transmitter wants to send a random variable X, over a noisy channel, to a receiver that has prior knowledge of another random variable Y jointly distributed with X. The objective of this problem is to find an encoding scheme that allows the receiver to obtain X with zero error probability. He observed that if the transmitter knows the realizations of Y, then the solution can be found in a straightforward way. However, in the case where the transmitter is oblivious to the realizations of Y, the problem is much harder. Specifically, the minimum communication rate in this case is related to the chromatic number of the powers of the channel confusion graph. Simonyi [5] considered a more general case with multiple receivers and showed that the simple lower bound given by the rate needed by the "weakest" receiver is attainable. Index coding can be considered as a multi-terminal generalization of the setting studied in [4] with non-uniform demands and with the restriction that the side information is a subset of the original data available at the sender.

The index coding problem has been introduced by Birk and Kol [3] and was initially motivated by broadcast satellite applications[1]. In particular, they developed several heuristic solutions for this problem and proposed protocols for practical implementation in satellite networks. Bar-Yossef et al. studied in [6] the index coding problem from a graph-theoretical perspective and showed that it is equivalent to determining the *minrank* of a related graph. Finding the minrank of a graph, however, is an intractable problem [7]. Lubetzky and Stav [8] showed that non-linear scalar codes have a significant advantage over linear ones by constructing a family of instances with a large gap between the optimal number of transmissions required by non-linear and linear codes. In a concurrent work, Alon et al. demonstrated the advantages of vector linear index codes using graph theoretical techniques [9]. Wu et al. [10] studied the information-theoretical aspects of the problem with the goal of characterizing the admissible rate region[2]. Reference [11] analyzed the hardness of approximation of the index coding problem. References [12] and [13] presented several heuristic solutions based on graph coloring and SAT solvers.

Index coding can be considered as a special case of the network coding problem [14]. The network coding technique extends the capability of intermediate network nodes by allowing them to mix packets received from different incoming edges. The goal of the network coding problem is to find the maximum rate between source and destination pairs in a communication network with limited edge capacities. Initial works on network coding focused on establishing *multicast* connections. It was shown in [14] and [15] 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 value of all the cuts that separate the source s from any terminal $t \in T$. In a subsequent work, Koetter and Médard [16] 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. [17] to show that linear network codes can be efficiently constructed through a randomized algorithm. Jaggi et al. [18] proposed a deterministic polynomial-time algorithm for finding feasible network codes in multicast networks. References [19] and [20] provide a comprehensive overview of network coding.

Contributions

In this paper, we study the relation between the index coding problem and the more general network coding problem. In particular, we establish a reduction that maps any instance of the network coding problem to a corresponding instance of the index coding problem. We show that several important properties of network codes carry over to index codes. Specifically, by applying our reduction to the network presented in [21], we show that vector linear index codes are suboptimal. We also present an instance of the index coding problem in which splitting a message into two packets yields a smaller number of transmissions than a scalar linear solution.

We also study the relation between the index coding problem and matroid theory. In particular, we present a reduction that maps any matroid to an instance of the index coding problem such that the problem has a special optimal vector linear code (that we call *perfect index code*) if and only if the matroid has a multilinear representation. This construction constitutes a means to apply numerous results in the rich field of matroid theory to index coding, and in turn, to the network coding problems. For instance, we use results on the linear representability of matroids, particularly the non-Pappus

[1]Reference [3] refers to the index coding problem as the "informed source coding on demand" problem (ISCOD).

[2]Reference [10] refers to the index coding problem as the "local mixing problem".

matroid, to provide an additional example where vector linear outperform scalar linear codes.

Organization: The rest of the paper is organized as follows. In Section II, we discuss our model and formulate the index and network coding problems. In Section III, we present a reduction from the network coding problem to the index coding problem. In Section IV, we discuss the relation between the index coding problem and matroid theory. In Section V, we apply our reductions to show the sub-optimality of linear and scalar index codes. Next, in Section VI, we discuss the relationship between networks and matroids. Finally, conclusions appear in Section VII.

II. Model

In this section, we present a formulation of the network coding and index coding problems.

A. Index Coding

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, where $|\Sigma|=q$. A client is represented by a pair (x,H), where $x\in X$ is the message demanded by the client, and $H\subseteq X$ is set of messages available to the client as side information. Note that in this model each client requests exactly one message. This does not incur any loss of generality as any client that requests multiple messages can be substituted by several clients that require a single different message and have the same side information as the original one.

Each message x_i can be divided into n packets each belonging to the finite q-ary alphabet Σ, and we write $x=(x_{i1},\ldots,x_{in})\in\Sigma^n$. We denote by $\xi=(x_{11},\ldots,x_{1n},\ldots,x_{k1},\ldots,x_{kn})\in\Sigma^{nk}$ the concatenation of all the messages.

Definition 1 (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. Let $\ell(n,q)$ be the smallest integer c such that the above condition holds for a 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. In the case of a linear index code, the alphabet Σ is a finite field and the functions f and ψ_ρ are linear in the packet 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. Note that in the model adopted here a message can be requested by several clients. This is a slightly more general model than the one considered in references [6] and [8] where it was assumed that each message can only be requested by a single client.

Given n and q, the index coding problem consists of finding an optimal index code for a given instance. For an 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. We also denote by $\lambda^*(n,q)$ the minimum rate achieved by a vector linear solution of block length n over the finite field $\mathbb{F}_q$ of q elements. We are interested in the behavior of λ and λ^* as functions of n and q.

Let $\mu(\mathcal{I})$ be the maximum 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. To see this, let $Y^*=\arg\max_{Y\subseteq X}|\{x_i;\ (x_i,Y)\in R\}|$ and $W=\{x_i;(x_i,Y^*)\in R\}$, and remove all clients that do not have the set Y^* as side information. We note that, since $Y^*\cap W=\emptyset$, the minimum transmission rate of the resulting instance is equal to $|W|=\mu(\mathcal{I})$. Since the rate of the resulting instance is less or equal to $\lambda(n,q)$ it holds that $\lambda(n,q)\geq\mu(\mathcal{I})$.

Definition 2: Let $\mathcal{I}(X,R)$ be an instance of the index coding problem. An index code for $\mathcal{I}(X,R)$ that achieves $\lambda(n,q)=\mu(\mathcal{I})$ is referred to as a *perfect index code*.

Note that the index code for the example in Figure 1 is optimal but not perfect, since for this particular instance we have $\lambda\neq\mu$ ($\lambda=2$, but $\mu=1$).

B. 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 the edges in E of zero in-degree and let $D\subset E$ be the subset of the 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 in the graph G, $k=|S|$ 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 $E=\{e_1,\ldots,e_m\}, S=\{e_1,\ldots,e_k\}$ 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 the message x_i, also denoted as $x(e_i)$. Each message x_i belongs to a certain alphabet Σ^n, where n is a positive integer and $|\Sigma|=q$. 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 $x(\delta(e_i))$ demanded by its head node. We refer to $\delta(\cdot)$ as the *demand function*. Each message x_i is divided into n packets, $x_i=(x_{i1},\ldots,x_{in})\in\Sigma^n$. We also denote by $\xi=(x_{11},\ldots,x_{1n},\ldots,x_{k1},\ldots,x_{kn})\in\Sigma^{nk}$ the concatenation of all the packets at the input edges.

Definition 3 (Network Code): A q-ary *network code* of block length n, also referred to as an (n,q) network code,

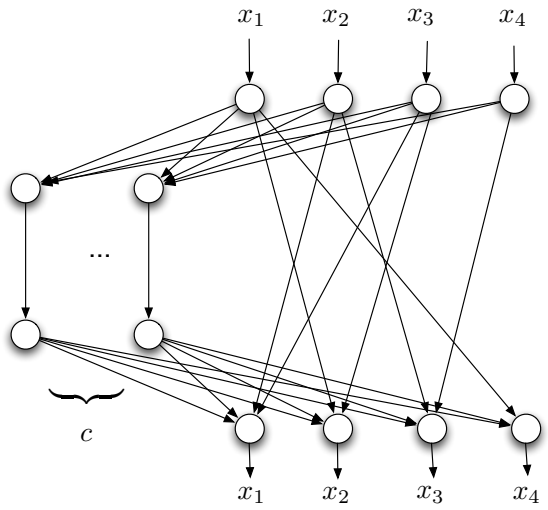

Fig. 2. An instance to the network coding problem equivalent to the instance of the index coding problem depicted in Figure 1.

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 mostly interested 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}. Note that a scalar linear network code over $\mathbb{F}$ naturally induces a vector linear network code of any block length n over the same field; however, the converse is not necessarily true as shown in Section V-A.

III. Connection to Network Coding

We first note that network coding is a more general problem than index coding. Indeed, for every instance of the index coding problem and a given integer c, there exists a corresponding instance of the network coding problem that has an (n,q) network code solution if and only if there exists an (n,q) index code of length $c \cdot n$. For example, Figure 2 depicts the instance of the network coding problem that corresponds to the instance of the index coding problem presented in Figure 1, where the broadcast channel is represented by c "bottleneck" edges.

In this section we present a reduction from the network coding problem to the index coding problem showing that these two problems are equivalent in the linear case. Specifically, for each instance $\mathcal{N}(G(V,E),\delta)$ of the network coding problem, we construct a corresponding instance $\mathcal{I}_{\mathcal{N}}(Y,R)$ of the index coding problem, such that $\mathcal{I}_{\mathcal{N}}$ has an (n,q) perfect linear index code if and only if there exists an (n,q) linear network for $\mathcal{N}$.

Definition 4: Let $\mathcal{N}(G(V,E),\delta)$ be an instance of the network coding problem. We form an instance $\mathcal{I}_{\mathcal{N}}(Y,R)$ of the index coding problem as follows:

1) The set of messages Y includes a message y_i for each edge $e_i \in E$ and all the messages $x_i \in X$, i.e., $Y = \{y_1, \ldots, y_m\} \cup X$;
2) The set of clients $R = R_1 \cup R_2 \cup R_3 \cup R_4 \cup R_5$ is defined as follows:
   a) $R_1 = \{(x_i, \{y_i\}); e_i \in S\}$
   b) $R_2 = \{(y_i, \{x_i\}); e_i \in S\}$
   c) $R_3 = \{(y_i, \{y_j; e_j \in \mathcal{P}(e_i)\}); e_i \in E \setminus S\}$
   d) $R_4 = \{(x(\delta(e_i)), \{y_i\}); e_i \in D\}$
   e) $R_5 = \{(y_i, X); i = 1, \ldots, m\}$

It is easy to verify that instance $\mathcal{I}_{\mathcal{N}}(Y,R)$ satisfies $\mu(\mathcal{I}_{\mathcal{N}}) = m$.

Theorem 5: Let $\mathcal{N}(G(V,E),\delta)$ be an instance of the network coding problem, and let $\mathcal{I}_{\mathcal{N}}(Y,R)$ be the corresponding instance of the index coding problem, as defined above. Then, there exists an (n,q) perfect linear index code for $\mathcal{I}_{\mathcal{N}}$ if and only if there exists a linear (n,q) network code for $\mathcal{N}$.

Proof: Suppose there is a linear (n,q) network code $C = \{f_e(X); f_e : (\mathbb{F}_q^n)^k \to \mathbb{F}_q^n, e \in E\}$ for $\mathcal{N}$ over the finite field $\mathbb{F}_q$ of size q for some block length n.

Define $g : (\mathbb{F}_q^n)^{m+k} \to (\mathbb{F}_q^n)^m$ such that $\forall Z = (x_1, \ldots, x_k, y_1, \ldots, y_m) \in (\mathbb{F}_q^n)^{m+k}, g(Z) = (g_1(Z), \ldots, g_m(Z))$ where $g_i(Z) = y_i + f_{e_i}(X)$, $i = 1, \ldots, m$. More specifically, we have

$$\begin{aligned} g_i(Z) &= y_i + x_i && i = 1, \ldots, k, \\ g_i(Z) &= y_i + f_{e_i}(X) && i = k+1, \ldots, m-d, \\ g_i(Z) &= y_i + x(\delta(e_i)) && i = m-d+1, \ldots, m. \end{aligned}$$

Next, we show that $g(Z)$ is indeed an index code for $\mathcal{I}_{\mathcal{N}}$ by proving the existence of the decoding functions. We consider the following five cases:

1) $\forall \rho = (x_i, \{y_i\}) \in R_1, \psi_\rho = g_i(Z) - y_i$,
2) $\forall \rho = (y_i, \{x_i\}) \in R_2, \psi_\rho = g_i(Z) - x_i$,
3) $\forall \rho = (y_i, \{y_{i_1}, \ldots, y_{i_p}\}) \in R_3$, since C is a linear network code for $\mathcal{N}$, there exists a linear function ϕ_{e_i} such that $f_{e_i}(X) = \phi_{e_i}(f_{e_{i_1}}(X), \ldots, f_{e_{i_p}}(X))$. Thus, $\psi_\rho = g_i(Z) - \phi_{e_i}(g_{i_1}(Z) - y_{i_1}, \ldots, g_{i_p}(Z) - y_{i_p})$,
4) $\forall \rho = (x(\delta(e_i)), \{y_i\}) \in R_4, e_i \in D, \psi_\rho = g_i(Z) - y_i$,
5) $\forall \rho = (y_i, X) \in R_5, \psi_\rho = g_i(Z) - f_{e_i}(X)$.

This index code is optimal since it is of length $\lambda(n,q) = \mu(\mathcal{I}_{\mathcal{N}}) = m$. To prove the converse, we assume that $g : (\mathbb{F}_q^n)^{m+k} \longrightarrow (\mathbb{F}_q^n)^m$ is a perfect linear (n,q) index code for $I_{\mathcal{N}}$ over the field $\mathbb{F}_q$. Again, we denote $Z = (x_1, \ldots, x_k, y_1, \ldots, y_m) \in (\mathbb{F}_q^n)^{m+k}$, and $g(Z) = (g_1(Z), \ldots, g_m(Z))$, x_i, y_i and $g_i(Z) \in \mathbb{F}_q^n$. We also write

$$g_i(Z) = \sum_{j=1}^{k} x_j A_{ij} + \sum_{j=1}^{m} y_j B_{ij},$$

for $i = 1, \ldots, m$, and $A_{ij}, B_{ij} \in M_{\mathbb{F}_q}(n, n)$, where $M_{\mathbb{F}_q}(n, n)$ is the set of $n \times n$ matrices with elements in $\mathbb{F}_q$.

The functions ψ_ρ exist for all $\rho \in R_5$ if and only if the matrix $M = [B_{ij}] \in M_{\mathbb{F}_q}(nm, nm)$, which has the matrix B_{ij} as a block submatrix in the (i, j)-th position, is invertible. Define $h : (\mathbb{F}_q^n)^{m+k} \longrightarrow (\mathbb{F}_q^n)^m$, such that

$$h(Z) = g(x_1, \ldots, x_k, (y_1, \ldots, y_m)M^{-1}),$$

$\forall Z \in (\mathbb{F}_q^n)^{m+k}$. So, we obtain

$$h_i(Z) = y_i + \sum_{j=1}^{k} x_j C_{ij}, i = 1, \ldots, m,$$

where $C_{ij} \in M_{\mathbb{F}_q}(n, n)$. We note that $h(Z)$ is a valid index code for $\mathcal{I}_\mathcal{N}$. In fact, for any client $\rho = (x, H) \in R$ with a decoding function $\psi_\rho(g, (z)_{z\in H})$ corresponding to the index code $g(Z)$, the function $\psi'_\rho(h, (z)_{z\in H}) = \psi_\rho(hM, (z)_{z\in H}))$ is a valid decoding function the index code $h(Z)$.

For all $\rho \in \ R_1 \cup R_4$, ψ'_ρ exists iff for $i = 1, \ldots, k, m - d + 1, \ldots, m, j = 1 \ldots k$ and $j \neq i$ it holds that $C_{ij} = [0] \in M_{\mathbb{F}_q}(n, n)$ and C_{ii} is invertible, where $[0]$ denotes the all-zero matrix. This implies that

$$\begin{aligned} h_i(Z) &= y_i + x_i C_{ii}, i = 1, \ldots, k, \\ h_i(Z) &= y_i + \sum_{j=1}^{k} x_j C_{ij}, i = k + 1, \ldots, m - d, \\ h_i(Z) &= y_i + x(\delta(e_i))C_{ii}, i = m - d + 1, \ldots, m. \end{aligned} \tag{1}$$

Next, we define the functions $f_{e_i} : (\mathbb{F}_q^n)^k \longrightarrow \mathbb{F}_q^n, e_i \in E$, as follows:

1) $f_{e_i}(X) = x_i$, for $i = 1, \ldots, k$
2) $f_{e_i}(X) = \sum_{j=1}^{k} x_j C_{ij}$, for $i = k + 1, \ldots, m - d$
3) $f_{e_i}(X) = x(\delta(e_i))$, for $i = m - d + 1, \ldots, m$.

We will show that $C = \{f_{e_i}; e_i \in E\}$ is a linear (n, q) network code for $\mathcal{N}$ by showing that it satisfies condition N3.

Let e_i be an edge in $E \setminus S$ with the set of parent edges $\mathcal{P}(e_i) = \{e_{i_1}, \ldots, e_{i_p}\}$. We denote by $I_i = \{i_1, \ldots, i_p\}$ and $\rho_i = (y_i, \{y_{i_1}, \ldots, y_{i_p}\}) \in R_3$. Then, there is a linear function ψ'_{ρ_i} such that $y_i = \psi'_{\rho_i}(h_1, \ldots, h_m, y_{i_1}, \ldots, y_{i_p})$. Hence, there exist matrices $T_{ij}, T'_{i\alpha} \in M_{\mathbb{F}_q}(n, n)$ such that

$$y_i = \sum_{j=1}^{m} h_j T_{ij} + \sum_{\alpha\in I_i} y_\alpha T'_{i\alpha}. \tag{2}$$

Substituting the expressions of the h_j's given by Eq. (1) in Eq. (2), we get that the following:

- T_{ii} is the identity matrix,
- $T'_{i\alpha} = -T_{i\alpha}, \forall \alpha \in I_i$,
- $T_{ij} = [0], \forall j \notin I_i \cup \{i\}$.

Therefore, we obtain

$$f_{e_i} = -\sum_{\alpha\in I_i} f_{e_\alpha} T_{i\alpha}, \forall e_i \in E \setminus S,$$

and C is a feasible network code for $\mathcal{N}$. ∎

Lemma 6: Let $\mathcal{N}(G(V, E), \delta)$ be an instance of the network coding problem, and let $\mathcal{I}_\mathcal{N}(Y, R)$ be the corresponding index coding problem. If there is an (n, q) network code (not necessarily linear) for $\mathcal{N}$, then there is a perfect (n, q) index code for $\mathcal{I}_\mathcal{N}$.

Proof: Suppose there is an (n, q) network code $C = \{f_e(X); f_e : (\Sigma^n)^k \to \Sigma^n, e \in E\}$ for $\mathcal{N}$ over the q-ary alphabet Σ. Without loss of generality, we assume that $\Sigma = \{0, 1, \ldots, q - 1\}$.

Define $g : (\Sigma^n)^{m+k} \to (\Sigma^n)^m$ such that $\forall Z = (x_1, \ldots, x_k, y_1, \ldots, y_m) \in (\Sigma^n)^{m+k}, g(Z) = (g_1(Z), \ldots, g_m(Z))$ with

$$g_i(Z) = y_i + f_{e_i}(X), \quad i = 1, \ldots, m$$

where "+" designates the entry-wise addition modulo q. Then, the same argument of the previous proof holds similarly here, and g is an index code for $\mathcal{I}_\mathcal{N}$. ∎

IV. Connection To Matroid Theory

A. Overview of Matroid Theory

A matroid $\mathcal{M}(Y, r)$ is a pair 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 $\{0, 1, 2, \ldots\}$, satisfying the following three conditions:

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

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 the 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 its circuits.

Matroid theory is a well studied field in discrete mathematics. References [22] and [23] provide a comprehensive discussion of this subject. Linear and multilinear representations of matroids over finite fields are major topics in matroid theory (see [22, Chapter 6], [24], and [25]).

Definition 7: Let $Y = \{y_1, \ldots, y_m\}$ be a set whose elements are indexed by the integers from 1 to m. For any collection of m matrices $M_1, \ldots, M_m \in \mathbb{M}_\mathbb{F}(n, k)$, and any subset $I = \{y_{i_1}, \ldots, y_{i_\delta}\} \subseteq Y$, with $i_1 < \cdots < i_\delta$, define

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

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

Definition 8: Let $\mathcal{M}(Y, r)$ be a matroid of rank $r_\mathcal{M} = k$ with ground set $Y = \{y_1, \ldots, y_m\}$. 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 $M_1, \ldots, M_m \in \mathbb{M}_\mathbb{F}(kn, n)$ such that,

$$\operatorname{rank}(M_I) = n \cdot r(I), \forall I \subseteq Y. \tag{3}$$

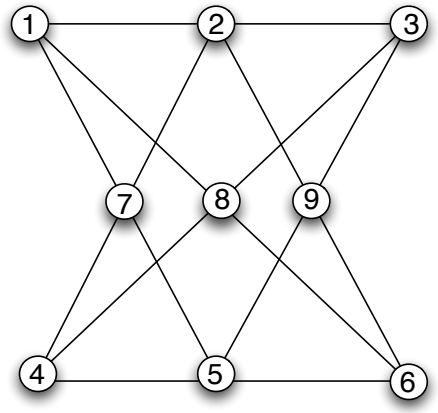

Fig. 3. A geometric representation of the non-Pappus matroid [22, p.43]. Circuits of order three are represented by straight lines.

Linear representation corresponding to $n = 1$ is the most studied case in matroid theory, see for example [22, Chapter 6]. Multilinear representation is a generalization of this concept from vectors to vector spaces and was discussed in [24], [25].

Example 9: 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 the vectors $M_1 = [1 \quad 0]^T, M_2 = [0 \quad 1]^T, M_3 = [1 \quad 1]^T$ 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:

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

Example 10: The non-Pappus matroid (see e.g., [22, §1.5]) $\mathcal{M}_{np}(Y, r)$ is defined over a ground set $Y = \{y_1, \ldots, y_9\}$ and can be represented geometrically as shown in Figure 3. Let $Y_0 = \{\{1,2,3\}, \{1,5,7\}, \{3,5,9\}, \{2,4,7\}, \{4,5,6\}, \{2,6,9\}, \{1,6,8\}, \{3,4,8\}\}$. The rank function of the non-Pappus matroid is given by

$$r(I) = \begin{cases} \min(|I|, 3) & \forall I \in 2^Y \setminus Y_0, \\ 2 & \forall I \in Y_0. \end{cases}$$

It is known from Pappus theorem [22, p.173] that the non-Pappus matroid is not linearly representable over any field. However, it was shown in [24] and [25], that it has a 2-linear representation over $GF(3)$, given below by the following 6×2 matrices $M_1, \ldots, M_9$:

$$[M_1|\ldots|M_9] = \begin{pmatrix} 10 & 10 & 00 & 10 & 00 & 10 & 10 & 10 & 00 \\ 01 & 01 & 00 & 01 & 00 & 01 & 01 & 01 & 00 \\ 00 & 00 & 00 & 10 & 10 & 21 & 01 & 10 & 10 \\ 00 & 00 & 00 & 02 & 01 & 20 & 12 & 02 & 01 \\ 00 & 10 & 10 & 01 & 00 & 01 & 00 & 11 & 10 \\ 00 & 01 & 01 & 21 & 00 & 21 & 00 & 10 & 01 \end{pmatrix}. \tag{4}$$

B. From Matroids to Index Codes

In the rest of this section we present a reduction from the problem of finding a linear representation for a given matroid to the index coding problem.

Definition 11: Given a matroid $\mathcal{M}(Y, r)$ of rank k over a ground set $Y = \{y_1, \ldots, y_m\}$, we define the corresponding index coding problem $\mathcal{I}_{\mathcal{M}}(Z, R)$ as follows:

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

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

Theorem 12: Let $\mathcal{M}(Y, r)$ be a matroid on the set $Y = \{y_1, \ldots, y_m\}$ and $\mathcal{I}_{\mathcal{M}}(Z, R)$ be the 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 $y_i = (y_{i1}, \ldots, y_{in})$, $x_i = (x_{i1}, \ldots, x_{in}) \in \mathbb{F}_q^n$, $\xi = (x_{11}, \ldots, x_{1n}, \ldots, x_{k1}, \ldots, x_{kn}) \in \mathbb{F}_q^{kn}$, and $\chi = (y_{11}, \ldots, y_{1n}, \ldots, y_{m1}, \ldots, y_{mn}, x_{11}, \ldots, x_{1n}, \ldots, x_{k1}, \ldots, x_{kn}) \in \mathbb{F}_q^{(m+k)n}$.

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

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

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:

1) Fix a basis $B = \{y_{i_1}, \ldots, y_{i_k}\} \in \mathfrak{B}(\mathcal{M})$, with $i_1 < i_2 < \cdots < i_k$, and let $\rho_i = (x_i, B) \in R_1$, $i = 1, \ldots, k$. By Eq. (3), $\mathrm{rank}(M_B) = kn$, hence the $kn \times kn$ matrix M_B is invertible. Thus, the corresponding decoding functions can be written as
$$\psi_{\rho_i} = [f_{i_1} - y_{i_1}| \ldots |f_{i_k} - y_{i_k}]U_i,$$
where the U_i's are the $kn \times n$ block matrices that form M_B^{-1} in the following way:
$$[U_i| \ldots |U_k] = M_B^{-1}.$$
2) 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
$$\psi_\rho = f_{i_1} - [f_{i_2} - y_{i_2}| \ldots |f_{i_c} - y_{i_c}]T.$$
3) 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 it induces an n-linear representation of the matroid $\mathcal{M}$ over $\mathbb{F}_q$.

Due to the clients in R_3, we can use the same reasoning used in the proof of the converse of Theorem 5 and assume that the functions $f_i(\chi), i = 1, \ldots, m$, have the following diagonalized form

$$f_i(\chi) = y_i + \xi A_i, \tag{5}$$

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 the matroid $\mathcal{M}$ over $\mathbb{F}_q$. To prove this, it suffices to show that the matrices A_i's satisfy Eq. (3) for all the bases and cycles of $\mathcal{M}$.

Let $B \in \mathfrak{B}(\mathcal{M})$ a basis. Then, by Eq. (5), 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 $C \in \mathfrak{C}(\mathcal{M})$ be 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 independent, and there is a basis B of $\mathcal{M}$ such that $C' \subseteq B$ (by the independence augmentation axiom [22, 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. Properties of Index Codes

A. Block Encoding

Index coding, as previously noted, is related to the problem of zero-error source coding with side information, studied by Witsenhausen in [4]. Two cases were studied there, depending on whether the transmitter knows the side information available to the receiver or not. It was shown that in the former case the repeated scalar encoding is optimal, i.e., block encoding does not have any advantage over the scalar encoding. We will demonstrate in this section that this result does not always hold for the index coding problem, which can be seen as an extension of the point-to-point problem discussed in [4].

Medard et al. introduced in [26] a special network, called the M-network (see Figure 4) with a very interesting property. This network does not have a scalar linear network code, but has a vector linear one of block length 2. Interestingly, such a vector linear solution does not require encoding and consists of a simple routing scheme. Moreover, it was shown in [27] that the M-network admits vector linear network codes of even block lengths only.

Let $\mathcal{N}_1$ be the M-network and consider the instance $I_{\mathcal{N}_1}$ of the index coding problem corresponding to the M-network obtained by the construction of Definition 4. Due to the properties of the M-network, $I_{\mathcal{N}_1}$ does not admit a perfect scalar linear index code, but has a perfect vector linear index code of block length 2, over any field. Thus, $\mathcal{I}_{\mathcal{N}_1}$ is an instance of the index coding problem where vector linear outperforms

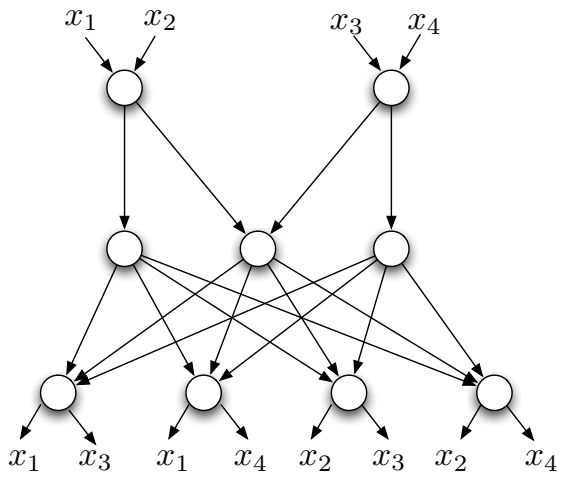

Fig. 4. The M-Netwrok $\mathcal{N}_1$ [26].

scalar linear coding. This result can be summarized by the following corollary which follows from Theorem 5.

Corollary 13: For $\mathcal{I}_{\mathcal{N}_1}, \lambda(2,2) = \lambda^*(2,2) < \lambda^*(1,2)$.

Another similar instance of the index coding problem is $\mathcal{I}_{\mathcal{M}_{np}}$ obtained by applying the construction of Definition 11 to the non-Pappus matroid $\mathcal{M}_{np}$. Since the non-Pappus matroid $\mathcal{M}_{np}$ does not admit any linear representation, by Theorem 12, there is also no perfect scalar linear index code for $\mathcal{I}_{\mathcal{M}_{np}}$. Nevertheless, the multilinear representation of the non-Pappus matroid over $GF(3)$ described in Example 10 induces a perfect $(3, 2)$ vector linear index code for $\mathcal{I}_{\mathcal{M}_{np}}$. Using Theorem 12, we get:

Corollary 14: For the instance $\mathcal{I}_{\mathcal{M}_{np}}$ of the index coding problem it holds that $\lambda(2,3) = \lambda^*(2,3) < \lambda^*(1,3)$.

B. Linearity vs. Non-Linearity

Linearity is a desired property for any code, including index codes. It was conjectured in [6] that scalar linear index codes over $GF(2)$ are optimal, meaning that $\lambda^*(1,2) = \lambda(1,2)$ for all index coding instances. Lubetzky and Stav disproved this conjecture in [8] for the *scalar linear* case by providing, for any given number of messages k and field $\mathbb{F}_q$, a family of instances of the index coding problem with a large gap between $\lambda^*(1,q)$ and $\lambda(1,q)$.

In this section, we show that *vector linear* codes are still suboptimal. In particular, we provide an instance where non-linear index codes outperform vector linear codes for any choice of field and block length n. Our proof is based on the insufficiency of linear network codes result proved by Dougherty et al. [21]. Specifically, reference [21] showed that the network $\mathcal{N}_3$ depicted in Figure 5 has the following property:

Theorem 15: The network $\mathcal{N}_3$ does not admit a linear network code but has a $(2, 4)$ non-linear one [21].

Let $\mathcal{I}_{\mathcal{N}_3}$ be the instance of the index coding problem that corresponds to $\mathcal{N}_3$, constructed according to Definition 4. Theorem 15 implies that $\mathcal{I}_{\mathcal{N}_3}$ does not have a perfect linear index code. However, by Lemma 6, a $(2, 4)$ non-linear code of

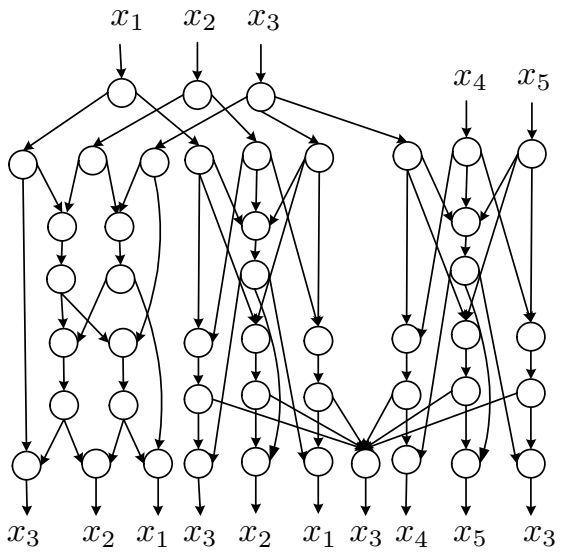

Fig. 5. The network $\mathcal{N}_3$ of [21]. $\mathcal{N}_3$ does not admit a vector linear network code over any field, but has a non-linear network code over a quaternary alphabet.

$\mathcal{N}_3$ can be used to construct a $(2,4)$ non-linear perfect index code for $\mathcal{I}_{\mathcal{N}_3}$ that satisfies $\lambda(2,4) = \mu(\mathcal{I})$. We summarize this result in the following corollary.

Corollary 16: For the instance $\mathcal{I}_{\mathcal{N}_3}$ of the index coding problem, it holds that $\lambda(2,4) = \mu(\mathcal{I}_{\mathcal{N}_3}) < \lambda^*(n,q), \forall n \in \mathbb{N}$, and q a prime power.

VI. Matroids and Networks

Dougherty et al. [21], [27] used results on the representability of matroids to construct the network $\mathcal{N}_3$ which is depicted in Figure 5 and which served as a counter-example to the conjecture of the sufficiency of linear network codes for achieving network capacity. They defined also the concept of matroidal networks, and presented a method for constructing networks from matroids [27, Section V.B]. Given a certain matroid, they design an instance to the network coding problem that forces the same independency relations of the matroid to exist in the set of source and edge messages. However, not all of the matroid dependency relations are reflected in this network. As a result, a linear representation for the matroid will give a linear network code for the corresponding network. However, the converse is not always true for this construction

In this section, we present a new construction that avoids this problem and that is based on the result of Theorem 12 which can be used as an intermediate step to build a connection between network codes and matroid linear representability. We describe below how to build a network from an index coding problem associated with a matroid and obtained by the construction discussed in Section IV. The reduction presented here provides a stronger connection between matroids and network codes. Specifically, for a given matroid, we 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. This result will permit the application of many important results on matroid linear representability to network coding theory.

Definition 17 describes this reduction which is a generalization of the construction of the network in Figure 2. The obtained network consists of input edges representing all the messages available at the transmitter and output edges corresponding to the clients. The availability of the side information is captured by direct edges connecting a client to the corresponding nodes carrying the side information. The noiseless broadcast channel is modeled in the network by a set of "bottleneck" edges connected to all the input and output edges.

Definition 17: 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 11. We associate to it the 6-partite network $\mathcal{N}(\mathcal{I}_{\mathcal{M}})$ constructed as follows:

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

Proposition 18: 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) vector linear network code.

Proof: It can be easily seen that any (n,q) perfect linear index code for $\mathcal{I}_{\mathcal{M}}$ will imply an (n,q) linear network code for $\mathcal{N}(\mathcal{I}_{\mathcal{M}})$, and vice versa. The proof follows, then, directly from Theorem 12. ∎

Figure 6 shows a sub-network of $\mathcal{N}(\mathcal{I}_{\mathcal{M}np})$ resulting from the construction of Definition 17 applied to the non-Pappus matroid $\mathcal{M}_{np}$ of Figure 3. Node n_1 represents the clients in the set R_3 of $\mathcal{I}_{\mathcal{M}np}$, n_2 the basis $\{1,2,4\}$ of the non-Pappus matroid, and n_3, n_4, n_5 the cycle $\{1,2,3\}$.

VII. Conclusion

This paper focused on the index coding problem and its relation to network coding and matroid theory. First, we presented a reduction that maps an instance $\mathcal{N}$ of the network coding problem to an instance $\mathcal{I}_{\mathcal{N}}$ of the index coding problem such that $\mathcal{N}$ has a vector linear solution if and only if there is a perfect index code for $\mathcal{I}_{\mathcal{N}}$. Our reduction implies that many important results on the network coding problem carry over to the index coding problem. In particular, using the M-network described in [26], we showed that vector linear index codes outperform scalar ones. In addition, by using the results of Dougherty et al. in [21] we showed that non-linear index codes outperform vector linear codes.

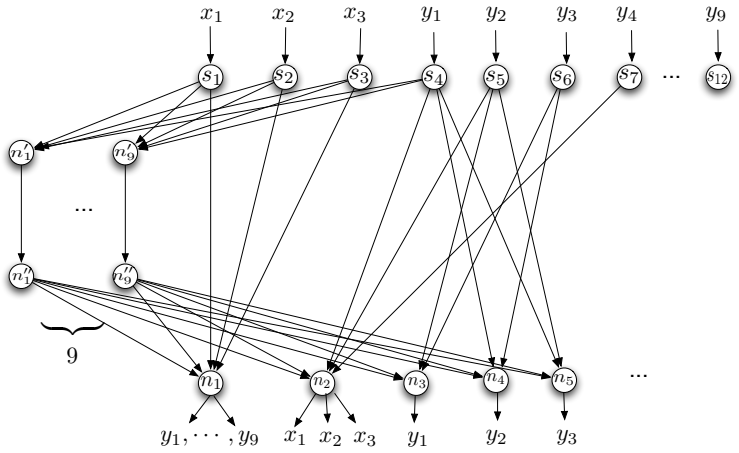

Fig. 6. Part of the network equivalent to the non-Pappus matroid resulting from the construction of Definition 17.

Next, we presented a reduction that maps an instance of the matroid representation problem to an instance of the index coding problem. In particular, for any given matroid $\mathcal{M}$ we constructed an instance of the index coding problem $\mathcal{I}_{\mathcal{M}}$, such that $\mathcal{M}$ has a multilinear representation if and only if $\mathcal{I}_{\mathcal{M}}$ has a vector linear solution over the same field. Using the properties of the non-Pappus matroid, we gave a second example where vector linear outperform scalar linear index codes. Our results imply that there exists a strong connection between network coding and matroid theory.

REFERENCES

[1] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft. XORs in the Air: Practical Wireless Network Coding. In *SIGCOMM '06: Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 243–254, New York, NY, USA, 2006. ACM Press.

[2] S. Katti, D. Katabi, H. Balakrishnan, and M. Medard. Symbol-level network coding for wireless mesh networks. In *ACM SIGCOMM*, Seattle, WA, 2008.

[3] Y. Birk and T. Kol. Coding-on-demand by an informed source (ISCOD) for efficient broadcast of different supplemental data to caching clients. *IEEE Transactions on Information Theory*, 52(6):2825–2830, June 2006. Infocom.

[4] H.S.Witsenhausen. The zero-error side information problem and chromatic numbers. *IEEE Transactions on Information Theory*, 22(5):592–593, 1976.

[5] G. Simonyi. On Witsenhausen's zero-error rate for multiple sources. *IEEE Transactions on Information Theory*, 49(12):3258–3261, December 2003.

[6] 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.

[7] R. Peeters. Orthogonal representations over finite fields and the chromatic number of graphs. *Combinatorica*, 16(3):417–431, 1996.

[8] 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.

[9] N. Alon, E. Lubetzky, U. Stav, A. Weinstein, and A. Hasidim. Broadcasting with side information. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 823–832, Philadelphia, PA, October 2008.

[10] Y. Wu, J. Padhye, R. Chandra, V. Padmanabhan, and P. A. Chou. The local mixing problem. In *Proc. Information Theory and Applications Workshop*, San Diego, Feb. 2006.

[11] M. Langberg and A. Sprintson. On the hardness of approximating the network coding capacity. In *Proceedings of ISIT*, Toronto, Canada, June 2008 2008.

[12] 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.

[13] M. A. R. Chaudhry and A. Sprintson. Efficient algorithms for index coding. In *Infocom'08 student workshop*, 2008.

[14] 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.

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

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

[17] 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.

[18] 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.

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

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

[21] 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.

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

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

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

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

[26] M. Medard, M. Effros, T. Ho, and D. R. Karger. On coding for non-multicast networks. In *Proceedings of 41st Annual Allerton Conference on Communication, Control, and Computing*, October 2003.

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