Vector Network Coding Based on Subspace Codes Outperforms Scalar Linear Network Coding

Tuvi Etzion, *Fellow, IEEE*, and Antonia Wachter-Zeh, *Member, IEEE*

Abstract— This paper considers vector network coding solutions based on rank-metric codes and subspace codes. The main result of this paper is that vector solutions can significantly reduce the required alphabet size compared to the optimal scalar linear solution for the same multicast network. The multicast networks considered in this paper have one source with h messages, and the vector solution is over a field of size q with vectors of length t. For a given network, let the smallest field size for which the network has a scalar linear solution be q_s, then the *gap* in the alphabet size between the vector solution and the scalar linear solution is defined to be $q_s - q^t$. In this contribution, the achieved gap is $q^{(h-2)t^2/h+o(t)}$ for any $q \geq 2$ and any even $h \geq 4$. If $h \geq 5$ is odd, then the achieved gap of the alphabet size is $q^{(h-3)t^2/(h-1)+o(t)}$. Previously, only a gap of size one had been shown for networks with a very large number of messages. These results imply the same gap of the alphabet size between the optimal scalar linear and some scalar *nonlinear* network coding solution for multicast networks. For three messages, we also show an advantage of vector network coding, while for two messages the problem remains open. Several networks are considered, all of them are generalizations and modifications of the well-known combination networks. The vector network codes that are used as solutions for those networks are based on subspace codes, particularly subspace codes obtained from rank-metric codes. Some of these codes form a new family of subspace codes, which poses a new research problem.

Index Terms— Alphabet size, combination networks, multicast networks, rank-metric codes, scalar network coding, subspace codes, vector network coding.

I. Introduction

NETWORK coding has been attracting increasing attention over the last fifteen years. The trigger for this interest was Ahlswede *et al.*'s seminal paper [1], which revealed

that network coding increases the throughput compared to simple routing. This gain is achieved since in network coding, the nodes are allowed to forward a function of their received packets, while in routing packets can only be forwarded. The network coding problem can be formulated as follows: given a network with a set of sources (where each one has a set of messages), for each edge find a function of the packets received at the starting node of the edge, such that each receiver can recover all its requested information from its received packets. Such an assignment of a function to each edge is called a *solution* for the network. Therefore, the received packets on an edge can be expressed as functions of the messages of the sources. If these functions are linear, we obtain a *linear network coding solution*, else we speak about a *nonlinear solution*. In linear network coding, each linear function on an edge consists of coding coefficients for each incoming packet. If the coding coefficients and the packets are scalars, it is called a *scalar network coding solution*. A network which has a solution is called a *solvable* network. Throughout this paper, we use the short-hand terms *scalar linear solution* and *scalar nonlinear solution*. In [27], Kötter and Médard provided an algebraic formulation for the linear network coding problem and its scalar solvability.

Vector network coding as part of *fractional network coding* was mentioned in [2]. A solution of the network is called an (s, t) *fractional vector network coding solution*, if the edges transmit vectors of length t, but the message vectors are of length $s \leq t$. The case $s = t = 1$ corresponds to a scalar solution. Ebrahimi and Fragouli [11] have extended the algebraic approach from [27] to *vector network coding*. Here, all packets are vectors of length t and the coding coefficients are matrices. A set of $t \times t$ coding matrices for which all receivers can recover their requested information, is called a *vector network coding solution* (henceforth, it will be called *vector solution*). Notice that vector operations imply linearity over vectors; therefore, a vector solution is always a (vector) *linear* solution. In terms of the achievable rate, vector network coding outperforms scalar linear network coding [10], [35]. In [35], an example of a network which is not scalar linear solvable but is solvable by vector routing was shown. A generalization was given in [5]: Das and Rai proved that there exists a network with a vector linear solution of dimension m but with no vector linear solution over any finite field when the dimension is less than m. Furthermore, in [8] it was shown that not every solvable network has a vector solution. In particular, it is shown that there exists a network which has a nonlinear solution yet has no vector solutions over any finite field and any vector dimension. The hardness

of finding a capacity achieving vector solution for a general instance of the network coding problem is proven in [30]. Recently, Connelly and Zeger [4], have shown that in some cases, there exist networks with scalar linear solutions over some commutative ring but not over the field of the same size. In [3], it was proven that there exist networks with scalar linear solutions over some non-commutative ring, but not over any commutative ring, and such networks have vector linear solutions over a field but no scalar linear solutions over any field.

The *alphabet size* of the network coding solution is an important parameter that directly influences the complexity of the calculations at the network nodes and edges. In practical applications, it is usually desired to work over small binary finite fields in order to represent bits and bytes. The minimum required alphabet size has been a subject for comprehensive research throughout the last fifteen years of research on network coding, cf. Langberg's and Sprintson's tutorial [29].

Throughout this paper, we consider only (single source) *multicast networks*. A recent survey on the fundamental properties of network coding for multicast networks can be found in [20]. A multicast network has one source with h messages and all receivers want to receive all the h messages simultaneously. Notice that such a network is equivalent to a network with h sources, where each source transmits one message. Li, Yeung, Cai proved that any multicast network is solvable over every sufficiently large field [32]. Jaggi *et al.* [25] have shown a deterministic algorithm for finding a scalar linear solution for multicast networks whose field size is the least prime power that is at least the number of receivers N. The algorithm from [28] reduces the complexity to find such a solution for the network. Lehmann and Lehmann [31] proved that there are networks where the linear and nonlinear scalar solutions both require a field of size in the order of $\sqrt{N}$. In general, finding the minimum required field size of a (linear or nonlinear) scalar network code for a certain multicast network is NP-complete [31].

For a given network, a vector solution can be transformed into a nonlinear scalar solution. Dougherty *et al.* [9] have investigated several differences between scalar linear and scalar nonlinear solutions. For example, they showed that for any integer $h \geq 3$, there exists a multicast network with h messages that has a binary nonlinear solution, but no binary *linear* solution. Further, they also showed that a network that has a scalar solution over some alphabet might not have a scalar solution over a larger alphabet (which might not be a finite field). In [43], two multicast networks were given: one of which is solvable over the finite field $\mathbb{F}_7$ but not over $\mathbb{F}_8$, and one of which is solvable over $\mathbb{F}_{16}$ but not over $\mathbb{F}_{17}$. They provided the so-called *Swirl network* which is linearly solvable over $\mathbb{F}_5$ but not over any $\mathbb{F}_{2^m}$, where $2^m \leq h + 2$ and $2^m - 1$ is a Mersenne prime.

In a scalar linear solution, each coding coefficient can be chosen from q_s values (if the solution is over a field of size q_s). In vector network coding over a field of size q and dimension t, each coefficient is a $t \times t$ matrix and can be chosen from q^{t^2} possibilities. Therefore, vector network coding offers more freedom in choosing the coding coefficients than does

scalar linear coding for equivalent alphabet sizes, and a smaller alphabet size might be achievable [11].

This paper considers a widely studied family of networks, the combination networks, and several generalizations and modifications of them. We analyze the scalar linear and vector solutions of these networks. The proposed vector solutions are based on rank-metric codes and subspace codes. The main result of our paper is that for several of the analyzed networks, our vector solutions significantly reduce the required *alphabet size*. In one subfamily of these networks, the scalar linear solution requires a field size $q_s = q^{(h-2)t^2/h+o(t)}$, for even $h \geq 4$, where h denotes the number of messages, while we provide a vector solution of field size q and dimension t. Such a vector solution has the same alphabet size as a scalar solution of field size q^t, and we denote $q_v \triangleq q^t$. Therefore, the achieved gap between the alphabet size of the optimal scalar linear solution and our vector solution is $q^{(h-2)t^2/h+o(t)}$ for any even $h \geq 4$. Notice that throughout this paper whenever we refer to such a *gap*, we mean the difference between the *smallest* field (alphabet) size for which a scalar linear solution exists and the *smallest* alphabet size for which we can construct a vector solution, i.e., the gap is $q_s - q_v$. For odd $h \geq 5$, the achieved gap is $q^{(h-3)t^2/(h-1)+o(t)}$. To our knowledge, so far Sun *et al.* [41], [42] has been the only work which presents such a gap but only of size one. We improve significantly upon [41]. Further, the network of [41] has a large number of messages, whereas our results are based on simple networks and hold for any number of messages $h \geq 4$. For three messages and certain parameters, we provide a network in which the vector solution outperforms the optimal scalar linear solution but with a smaller gap. For two messages, the problem is open, and we conjecture that there is no advantage in the alphabet size when vector network coding is used. Finally, in the framework of [11], the coding matrices for the vector solutions have to be commutative, while in our solutions they are not necessarily commutative.

The rest of this paper is structured as follows. Section II provides notations and definitions of finite fields, network coding, and discusses rank-metric codes and subspace codes. Section III considers combination networks and derives their optimal scalar linear solutions and vector solutions based on rank-metric codes. Although our vector solutions do not provide an improvement in terms of the alphabet size for the unmodified combination networks, it helps to understand the principle of our vector solutions. Section IV gives an overview of the generalized combination networks for which a reduction in the alphabet size will be shown. In Section V, we present scalar linear and vector solutions for some generalized combination networks with additional direct links from the source to each receiver. Further, the nodes in these networks are connected via parallel links. The vector solutions for these networks are based on rank-metric codes, and the required alphabet size is significantly reduced. In particular, the largest achieved gap between scalar and vector network coding is $q^{(h-2)t^2/h+o(t)}$ for any even integer $h \geq 4$. In Section VI, we show that the constructions, which are based on rank-metric codes, can be seen as constructions based on subspace codes. Moreover, using subspace codes,

some results can be improved. Section VII analyzes and compares more generalized combination networks and the achieved gap in the alphabet size of the optimal scalar linear solutions and our vector solutions. The vector solutions for these networks are based on subspace codes. In particular, a gap between scalar and vector network coding of size $q^{(h-3)t^2/(h-1)+o(t)}$ is obtained for any odd integer $h \geq 5$ messages. A network where the vector solution also improves the alphabet size compared to the optimal scalar solution for $h = 3$ messages is shown in Section VIII. This network, as well as other similar networks, poses a new interesting problem related to subspace codes. Finally, concluding remarks are given in Section IX, and several open problems for future research are outlined.

II. PRELIMINARIES

A. Finite Fields

Let q be a power of a prime, $\mathbb{F}_q$ denote the finite field of order q, and $\mathbb{F}_{q^m}$ its extension field of order q^m. We use $\mathbb{F}_q^{m \times n}$ for the set of all $m \times n$ matrices over $\mathbb{F}_q$. Let $\mathbf{I}_s$ denote the $s \times s$ identity matrix and $\mathbf{0}_s$ the $s \times s$ all-zero matrix. The triple $[n, k, d]_q$ denotes a linear code over $\mathbb{F}_q$ of length n, dimension k, and minimum Hamming distance d. Let $\mathbb{F}_q[x]$ denote the ring of polynomials with coefficients in $\mathbb{F}_q$.

B. Network Coding

A *network* will be modeled as a finite directed acyclic multigraph, with a set of source nodes and a set $\mathcal{R} = \{R_1, \ldots, R_N\}$ of N receivers. The sources have sets of disjoint messages, which are symbols or vectors over a given finite field. To unify the description, we refer to *packets* for both cases, symbols and vectors. Each receiver demands (requests) a subset of the h messages. Each edge in the network has unit capacity, and it carries a packet which is either a symbol from $\mathbb{F}_{q_s}$ (in scalar network coding) or a vector of length t over $\mathbb{F}_q$ (in vector network coding). Note that the assumption of unit capacity does not restrict the considered networks, since edges of larger capacity can be represented by multiple parallel edges of unit capacity. The incoming and outgoing edges of a node V are denoted by $In(V)$ and $Out(V)$, respectively.

A *network code* is a set of functions of the packets on the edges of the network. For a source S, the edges in $Out(S)$ carry functions of the messages of S. For any vertex V, which is not a source or a receiver, the edges in $Out(V)$ carry functions of the packets on the edges of $In(V)$. The network code is called *linear* if all the functions are linear, and nonlinear otherwise. A network code is a *solution* for the network if each receiver can reconstruct its requested messages from the packets on its incoming edges. Such a network is called *solvable*. The network code is called a *scalar network code* if the packets are scalars from $\mathbb{F}_{q_s}$ and thus, each edge carries a scalar from $\mathbb{F}_{q_s}$. The network code is called a *vector network code* if the packets are vectors and each edge carries a vector of length t with entries from a field $\mathbb{F}_q$.

A *(single source) multicast network* is a network with exactly one source, where all receivers demand all the h messages simultaneously. This is possible if there exist h edge disjoint paths from the source to each receiver. This is equivalent to saying that the *min-cut* between the source and each receiver is at least h, where the min-cut is the minimum number of edges that have to be deleted to disconnect the source from the receiver. The network coding *max-flow/min-cut theorem* for multicast networks states that the maximum number of messages transmitted from the source to each receiver is equal to the smallest min-cut between the source and any receiver [1]. In the sequel, we will only write *network* instead of *multicast network* since this paper considers only multicast networks.

To formalize this description, let $x_1, \ldots, x_h$ denote the h source messages for scalar linear network coding. Each edge E in $Out(V)$, for any given vertex V, builds a linear combination of the symbols obtained from $In(V)$. The coefficient vector of such a linear combination is called the *local coding vector*. Clearly, from all the functions on the paths leading to V, the packet of E can be written as a linear combination of the h messages. The coefficients of this linear combination are called the *global coding vector*. Each receiver finally obtains several linear combinations of the h message symbols (its global coding vectors). Thus, any receiver R_j, $j \in \{1, \ldots, N\}$, has to solve the following linear system of equations:

$$\begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} = \mathbf{A}_j \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_h \end{pmatrix},$$

where $k = |In(R_j)|$, and $\mathbf{A}_j$ is a $k \times h$ *transfer matrix* which contains the global coding vectors on the edges of $In(R_j)$, and the symbols on $In(R_j)$ are $\{y_1, \ldots, y_k\}$. In scalar linear network coding, we therefore want to find edge coefficients such that the matrix $\mathbf{A}_j$ has full rank for every $j = 1, \ldots, N$. These coefficients should have field size q_s as small as possible.

In *vector network coding*, the edges transmit vectors, and therefore, the coding coefficients at each node are matrices. A *vector solution* is said to have dimension t over a field of size q if all these vectors are over a field of size q and have length t, where $q_v = q^t$. Let $\mathbf{x}_1, \ldots, \mathbf{x}_h$ denote h source messages which are now vectors of length t. Then, any receiver R_j has to solve the following linear system of equations:

$$\begin{pmatrix} \mathbf{y}_1 \\ \vdots \\ \mathbf{y}_k \end{pmatrix} = \mathbf{A}_j \cdot \begin{pmatrix} \mathbf{x}_1 \\ \vdots \\ \mathbf{x}_h \end{pmatrix},$$

where $k = |In(R_j)|$, and $\mathbf{A}_j$ is a $(kt) \times (ht)$ *transfer matrix* which contains the global coding vectors (vectors whose entries are matrices) on the edges of $In(R_j)$, and the vectors on $In(R_j)$ are $\{\mathbf{y}_1, \ldots, \mathbf{y}_k\}$. In vector network coding, we therefore want to find edge coefficients (which are matrices) such that the matrix $\mathbf{A}_j$ has full rank for each $j = 1, \ldots, N$ and such that $q_v = q^t$ is minimized.

When we want to compare scalar linear and vector network coding, the solutions are equivalent with respect to the alphabet size when $q_s = q_v$.

C. Rank-Metric Codes

Codewords of rank-metric codes will be used in some of our constructions as coding coefficients for vector solutions. Let $\mathrm{rk}(\mathbf{A})$ be the rank of a matrix $\mathbf{A} \in \mathbb{F}_q^{m \times n}$. The *rank distance* between $\mathbf{A}, \mathbf{B} \in \mathbb{F}_q^{m \times n}$ is defined by $d_{\mathsf{R}}(\mathbf{A}, \mathbf{B}) \triangleq \mathrm{rk}(\mathbf{A} - \mathbf{B})$. A linear $[m \times n, k, \delta]_q^{\mathsf{R}}$ rank-metric code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^{m \times n}$. It consists of q^k matrices of size $m \times n$ over $\mathbb{F}_q$ with minimum rank distance:

$$\delta \triangleq \min_{\mathbf{A} \in \mathcal{C}, \mathbf{A} \neq \mathbf{0}} \{ \mathrm{rk}(\mathbf{A}) \}.$$

The Singleton-like upper bound for rank-metric codes [6], [21], [38] implies that for any $[m \times n, k, \delta]_q^{\mathsf{R}}$ code, we have that $k \leq \max\{m, n\}(\min\{n, m\} - \delta + 1)$. Codes which attain this bound with equality are known for all feasible parameters [6], [21], [38]. They are called *maximum rank distance* (MRD) codes and denoted by $\mathcal{MRD}[m \times n, \delta]_q$.

Let $\mathbf{C}$ be the *companion matrix* of a primitive polynomial of degree t over $\mathbb{F}_q$. The set of matrices $\mathcal{D}_t = \{\mathbf{0}_t, \mathbf{I}_t, \mathbf{C}, \mathbf{C}^2, \dots, \mathbf{C}^{q^t-2}\}$ forms an $\mathcal{MRD}[t \times t, t]_q$ code of q^t pairwise *commutative* matrices (see [33], [38]).

Theorem 1: Let $\mathcal{D}_t \triangleq \{\mathbf{0}_t, \mathbf{I}_t, \mathbf{C}, \mathbf{C}^2, \dots, \mathbf{C}^{q^t-2}\}$, where $\mathbf{C}$ is a companion matrix:

$$\mathbf{C} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & \dots & 0 & 1 \\ -p_0 & -p_1 & -p_2 & \dots & -p_{t-2} & -p_{t-1}, \end{pmatrix},$$

and $p(x) = p_0 + p_1 x + \dots + p_{t-2} x^{t-2} + p_{t-1} x^{t-1} + x^t \in \mathbb{F}_q[x]$ is a primitive polynomial. Then, $\mathcal{D}_t$ is an $\mathcal{MRD}[t \times t, t]_q$ code.

The set of matrices $\mathcal{D}_t$ and the finite field $\mathbb{F}_{q^t}$ are isomorphic. In particular, if α is a root of the primitive polynomial $p(x)$, then $\alpha^i \cdot \alpha^j$ can be implemented by multiplying the corresponding two matrices $\mathbf{C}^i \cdot \mathbf{C}^j = \mathbf{C}^{i+j}$, where $\mathbf{C}$ is the companion matrix based on $p(x)$. Similarly, $\alpha^i + \alpha^j$ corresponds to $\mathbf{C}^i + \mathbf{C}^j$. Notice that $\mathbf{C}^0 = \mathbf{C}^{q^t-1} = \mathbf{I}_t$. This property will be needed later in our constructions. These matrices are very useful when we design a vector network code for the combination networks (see Section III).

Moreover, to prove that any network (multicast or non-multicast) has a vector solution of dimension t over $\mathbb{F}_q$ if there exists a scalar linear solution over $\mathbb{F}_{q^t}$, we can simply replace any coefficient α^s by $\mathbf{C}^s$. Due to the isomorphism, addition and multiplication can be done in matrix representation as well. Further, the matrices of the code $\mathcal{D}_t$ are useful in encoding and decoding used in the network. Instead of computing in the field $\mathbb{F}_{q^t}$, we can use the related matrices of the code to obtain the vector solution and translate it to the scalar solution only at the receivers.

D. Subspace Codes

In our constructions of vector network codes, the global coding vector consists of h matrices from $\mathbb{F}_q^{t \times t}$. These h matrices can be appended together to form a $t \times (ht)$ matrix which is a basis for a subspace of $\mathbb{F}_q^{ht}$ whose dimension is at most t. In the sequel of the paper, we will see that if we use a set of

subspaces spanned by such matrices with additional properties, then they can be used as our coding coefficients.

Let $\langle \mathbf{A} \rangle$ denote the space spanned by the rows of a matrix $\mathbf{A}$. Similarly, for k vectors $\mathbf{a}_1, \dots, \mathbf{a}_k$, let $\langle \mathbf{a}_1, \dots, \mathbf{a}_k \rangle$ denote the space spanned by these vectors. The *Grassmannian* of dimension k is denoted by $\mathcal{G}_q(n, k)$ and is the set of all subspaces of $\mathbb{F}_q^n$ of dimension $k \leq n$. The cardinality of $\mathcal{G}_q(n, k)$ is the well-known q-binomial (also known as Gaussian coefficient):

$$|\mathcal{G}_q(n, k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q \triangleq \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i},$$

where $q^{k(n-k)} \leq \begin{bmatrix} n \\ k \end{bmatrix}_q < 4 \, q^{k(n-k)}$. The set of all subspaces of $\mathbb{F}_q^n$ is called the *projective space of order n* and is denoted by $\mathcal{P}_q(n)$, i.e., $\mathcal{P}_q(n) = \bigcup_{k=0}^n \mathcal{G}_q(n, k)$. For two subspaces $\mathcal{U}, \mathcal{V} \in \mathcal{P}_q(n)$, let $\mathcal{U} + \mathcal{V}$ denote the smallest subspace containing the union of $\mathcal{U} \in \mathcal{P}_q(n)$ and $\mathcal{V} \in \mathcal{P}_q(n)$. The *subspace distance* between $\mathcal{U} \in \mathcal{P}_q(n)$ and $\mathcal{V} \in \mathcal{P}_q(n)$ is defined by $d_s(\mathcal{U}, \mathcal{V}) \triangleq 2 \dim(\mathcal{U} + \mathcal{V}) - \dim(\mathcal{U}) - \dim(\mathcal{V})$. A *subspace code* is a set of subspaces; if the subspaces in the subspace code have the same dimension, then the code is called a *constant dimension code* or a *Grassmannian code*. These codes were considered for error-correction in random linear network coding [26]. Bounds on the sizes of such codes and properties which are relevant for our discussion can be found in [12], [14], [15], and [17]. Let $A_q(n, k, d)$ denote the maximum cardinality of a constant dimension code in $\mathcal{G}_q(n, k)$ with minimum subspace distance d. The following bounds can be found in [15] and [26].

Theorem 2: For $\delta > 1$,

$$q^{(n-k)(k-\delta+1)} \leq A_q(n, k, 2\delta) \leq 2q^{(n-k)(k-\delta+1)},$$

and for $\delta = 1$

$$q^{(n-k)k} \leq A_q(n, k, 2) = \begin{bmatrix} n \\ k \end{bmatrix}_q \leq 4q^{(n-k)k}.$$

III. THE COMBINATION NETWORKS

The $\mathcal{N}_{h,r,s}$ combination network (where $s \geq h$) is shown in Fig. 1 (see also [37]). The network has three layers: the first layer consists of a source with h messages. The source transmits r packets to the r nodes of the middle layer. Any s nodes in the middle layer are connected to a receiver, and each one of the $\binom{r}{s}$ receivers demands all the h messages. For vector coding, the messages $\mathbf{x}_1, \dots, \mathbf{x}_h$ are vectors of length t, and for scalar coding, the messages are scalars, denoted by $x_1, \dots, x_h$. In a combination network, the local and the global coding vectors are the same, and therefore, we will not distinguish between the two. Next, we consider the case where $s = h$.

A. Scalar Solution

The $\mathcal{N}_{h,r,h}$ combination network has a scalar linear solution of field size q_s if and only if an $[r, h, d = r - h + 1]_{q_s}$ MDS code exists [37]. From the known theory on MDS codes [34, pp. 317–331] it is known that such a code exists for every prime power q_s such that $q_s \geq r - 1$. The only
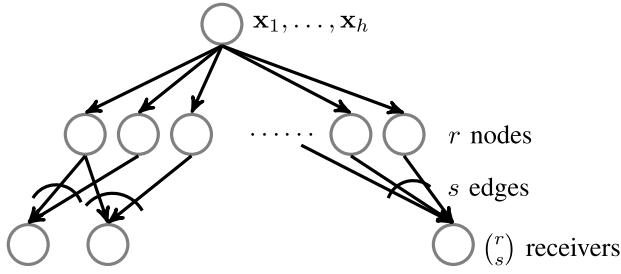
Fig. 1. The $\mathcal{N}_{h,r,s}$ combination network: it has an edge from the source to each of the r nodes in the middle layer. Each of the $\binom{r}{s}$ receivers is connected to a unique set of s middle-layer nodes and demands all of the messages $\mathbf{x}_1, \ldots, \mathbf{x}_h$.

exceptions are when $h \in \{3, q_s - 1\}$ and q_s is a power of two, where such a code exists for every prime power q_s such that $q_s \geq r - 2$ [34, p. 328]. The symbols transmitted to and from each node in the middle layer form together a codeword of the MDS code (encoded from the h message symbols), and each receiver obtains h symbols. Each receiver can correct $r - h$ erasures and therefore can reconstruct the h message symbols.

Corollary 1: If $h = 3$ and $r - 2$ is a power of two, let $q^* = r - 2$, else let $q^* = r - 1$. For the $\mathcal{N}_{h,r,h}$ combination network, a scalar linear solution of field size q_s exists if and only if $q_s \geq q^*$.

B. Vector Solution

In the sequel, we present a vector solution based on MRD codes for the $\mathcal{N}_{h,r,h}$ combination network. The case $h = 2$ was solved similarly in [41]. Our construction uses the isomorphism between the field $\mathbb{F}_{q^t}$ and the powers of the companion matrix, i.e., the set $\mathcal{D}_t$ (Theorem 1). This isomorphism leads to the following theorem.

Theorem 3: Let $\alpha \in \mathbb{F}_{q^t}$ be a root of the primitive polynomial $p(x)$ of $\mathbb{F}_{q^t}$. Let $\mathbf{M} \in \mathbb{F}_{q^t}^{\ell \times \ell}$ be an arbitrary matrix. Define the block matrix $\mathbf{M}' \in \mathbb{F}_q^{(\ell t) \times (\ell t)}$ by replacing each entry of $\mathbf{M}$ as follows: if $M_{ij} = \alpha^k$, $k \in \{0, \ldots, q^t - 2\}$, replace it by $\mathbf{C}^k$ for all $i, j = 1, \ldots, \ell$, where $\mathbf{C}$ denotes the companion matrix based on $p(x)$. If $M_{ij} = 0$, then replace it by $\mathbf{0}_t$.

Any set of λ linearly independent columns of $\mathbf{M}$ is linearly independent over $\mathbb{F}_{q^t}$ if and only if the columns of the related λ blocks of columns in $\mathbf{M}'$ are linearly independent over $\mathbb{F}_q$.

Proof: Denote by $\mathbf{M}_\lambda$ a full-rank $\lambda \times \lambda$ submatrix of $\mathbf{M}$. Define a corresponding $(\lambda t) \times (\lambda t)$ matrix $\mathbf{M}'_\lambda$ over $\mathbb{F}_q$ by replacing α^k by $\mathbf{C}^k$ and 0 by $\mathbf{0}_t$. Clearly, the determinant of $\mathbf{M}_\lambda$ is a function of its entries $M_{\lambda,ij}$, $i, j = 1, \ldots, \ell$. The determinant of $\mathbf{M}'_\lambda$ has the same form as $\det(\mathbf{M}_\lambda)$, with the only difference that each $M_{\lambda,ij} = \alpha^k$ is replaced by $\mathbf{C}^k$ (and if $M_{\lambda,ij} = 0$, it is replaced by $\mathbf{0}_t$). Thus, $\det(\mathbf{M}'_\lambda)$ is non-zero if and only if $\det(\mathbf{M}_\lambda)$ is non-zero and the difference and the product of any two distinct matrices $\mathbf{C}^i$ and $\mathbf{C}^j$ (where at least one of them is non-zero) has full rank. The second property is true since the powers of the companion matrix form a full-rank MRD code, see Theorem 1, and hence, the statement follows. ∎

The following corollary considers block Vandermonde matrices which will be used for our vector solution. Recall that $\mathbf{I}_t = \mathbf{C}^{q^t - 1} \in \mathcal{D}_t$.

Corollary 2: Let $\mathcal{D}_t$ be the $\mathcal{MRD}[t \times t, t]_q$ code defined by the companion matrix $\mathbf{C}$ (Theorem 1). Let $\mathbf{C}_i$, $i = 1, \ldots, h$, be distinct codewords of $\mathcal{D}_t$. Define the following $(ht) \times (ht)$ block matrix:

$$\mathbf{M} = \begin{pmatrix} \mathbf{I}_t & \mathbf{C}_1 & \mathbf{C}_1^2 & \cdots & \mathbf{C}_1^{h-1} \\ \mathbf{I}_t & \mathbf{C}_2 & \mathbf{C}_2^2 & \cdots & \mathbf{C}_2^{h-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{I}_t & \mathbf{C}_h & \mathbf{C}_h^2 & \cdots & \mathbf{C}_h^{h-1} \end{pmatrix}.$$

*Then, any $(ht) \times (\ell t)$ submatrix consisting of $h\ell$ blocks of **consecutive columns** has full rank ℓt, for any $\ell = 1, \ldots, h$.* Note that the blocks of rows do not have to be consecutive, but a block has to be included with all its t rows in the submatrix.

Based on this corollary, we can now provide a vector network code.

Construction 1: Let $\mathcal{D}_t = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_{q^t}\}$ be the $\mathcal{MRD}[t \times t, t]_q$ code defined by the companion matrix $\mathbf{C}$ (Theorem 1) and let $r \leq q^t + 1$. Consider the $\mathcal{N}_{h,r,h}$ combination network with message vectors $\mathbf{x}_1, \ldots, \mathbf{x}_h$. One node from the middle layer receives and transmits $\mathbf{y}_r = \mathbf{x}_h$ and the other $r - 1$ nodes of the middle layer receive and transmit $\mathbf{y}_i = \left(\mathbf{I}_t \ \mathbf{C}_i \ \mathbf{C}_i^2 \ \cdots \ \mathbf{C}_i^{h-1} \right) \cdot \left(\mathbf{x}_1 \ \mathbf{x}_2 \ \cdots \ \mathbf{x}_h \right)^T \in \mathbb{F}_q^t$, for $i = 1, \ldots, r - 1$.
The matrices $\mathbf{I}_t, \mathbf{C}_i, \mathbf{C}_i^2, \ldots, \mathbf{C}_i^{h-1}$, $i = 1, \ldots, r - 1$, are the coding coefficients of the incoming and outgoing edges of node i in the middle layer.

Theorem 4: Construction 1 provides a vector linear solution of field size q and dimension t to the $\mathcal{N}_{h,q^t+1,h}$ combination network, i.e., $\mathbf{x}_1, \ldots, \mathbf{x}_h$ can be reconstructed at all receivers.

Proof: Each receiver obtains h vectors and has to solve one of the following two systems of linear equations:

$$\begin{pmatrix} \mathbf{y}_{i_1} \\ \vdots \\ \mathbf{y}_{i_{h-1}} \\ \mathbf{y}_{i_h} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_t & \mathbf{C}_{i_1} & \mathbf{C}_{i_1}^2 & \cdots & \mathbf{C}_{i_1}^{h-1} \\ \mathbf{I}_t & \mathbf{C}_{i_2} & \mathbf{C}_{i_2}^2 & \cdots & \mathbf{C}_{i_2}^{h-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{I}_t & \mathbf{C}_{i_h} & \mathbf{C}_{i_h}^2 & \cdots & \mathbf{C}_{i_h}^{h-1} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_h \end{pmatrix}$$

or

$$\begin{pmatrix} \mathbf{y}_{i_1} \\ \vdots \\ \mathbf{y}_{i_{h-1}} \\ \mathbf{y}_1 \end{pmatrix} = \begin{pmatrix} \mathbf{I}_t & \mathbf{C}_{i_1} & \mathbf{C}_{i_1}^2 & \cdots & \mathbf{C}_{i_1}^{h-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{I}_t & \mathbf{C}_{i_{h-1}} & \mathbf{C}_{i_{h-1}}^2 & \cdots & \mathbf{C}_{i_{h-1}}^{h-1} \\ \mathbf{0}_t & \mathbf{0}_t & \mathbf{0}_t & \cdots & \mathbf{I}_t \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_h \end{pmatrix},$$

for some distinct $i_1, \ldots, i_h \in \{2, \ldots, r\}$. Due to Corollary 2, in both cases, the corresponding matrix has full rank and there is a unique solution for $(\mathbf{x}_1 \ \mathbf{x}_2 \ \cdots \ \mathbf{x}_h)$. ∎

The decoding at each receiver consists of solving a linear system of equations of size $(ht) \times (ht)$. The following theorem analyzes the decoding complexity of this vector solution. Thereby, we use the MRD code from Theorem 1 which is formed by the companion matrix and its powers. Thus, the inverse of these matrices can be calculated with less than quadratic complexity.

Theorem 5: For the $\mathcal{N}_{h,q^t+1,h}$ combination network, a vector solution of field size q and dimension t exists. The decoding complexity is in $\mathcal{O}(ht \log^2 h \log^2 t)$ over $\mathbb{F}_q$ for each receiver.

Proof: From Theorem 4 it is clear that such a solution exists. For the decoding complexity, it remains to prove that inverting the matrix $\mathbf{M}$ from Corollary 2 can be done with $\mathcal{O}(ht \log^2 h \log^2 t)$ operations over $\mathbb{F}_q$. Since the submatrices are commutative, the inverse of this block Vandermonde matrix can be calculated in the same way as the inverse of a usual Vandermonde matrix [44]. The only difference is that multiplication and addition of elements from $\mathbb{F}_q$ are now replaced by multiplication and addition of the commutative code matrices. Due to the isomorphism between $\mathbb{F}_{q^t}$ and $\mathcal{D}_t$, this multiplication and addition is equivalent to fast polynomial multiplication and fast polynomial addition modulo the primitive polynomial $p(x)$, and thus, the matrix additions and multiplications are in the order of $\mathcal{O}(t \log^2 t)$ over $\mathbb{F}_q$ [23]. Thus, the complexity of inverting $\mathbf{M}$ costs $t \log^2 t$ times the complexity of inverting an $h \times h$ Vandermonde matrix, which is $\mathcal{O}(h \log^2 h)$ [23]. ∎

Further, for the $\mathcal{N}_{3,q^t+2,3}$-combination network with three messages and when q^t is a power of two, we can use the matrices from Construction 1 and additionally transmit $\mathbf{x}_2 = (\mathbf{0}_t \; \mathbf{I}_t \; \mathbf{0}_t) \cdot (\mathbf{x}_1 \; \mathbf{x}_2 \; \mathbf{x}_3)^T$ to obtain a vector solution.

C. Analysis

Due to the isomorphism of $\mathbb{F}_{q^t}$ and the code $\mathcal{D}_t$, both solutions are equivalent. Hence, in practice, implementing the scalar solution can actually be done by implementing the vector solution. We can therefore construct a vector linear solution of field size q and dimension t for the $\mathcal{N}_{h,q^t+1,h}$ combination network, where equivalently a scalar solution from an MDS code exists for $q_s \geq q^t$. The decoding complexity when implementing the vector solution is in $\mathcal{O}(ht \log^2 h \log^2 t)$ operations over $\mathbb{F}_q$ for each receiver.

IV. A FAMILY OF GENERALIZED COMBINATION NETWORKS

In this section, we discuss the generalizations and modifications of the combination networks which are considered in this paper. We therefore define a generalization of the $\mathcal{N}_{h,r,s}$ combination network, called the ϵ-*direct links* ℓ-*parallel links* $\mathcal{N}_{h,r,s}$ *network*, in short the (ϵ, ℓ)-$\mathcal{N}_{h,r,s}$ network. All our considered networks (including the unmodified combination networks) are special cases of the (ϵ, ℓ)-$\mathcal{N}_{h,r,s}$ network.

We start by describing the structure of the generalized networks and then we will consider the main subfamilies of this family of networks. An example of an (ϵ, ℓ)-$\mathcal{N}_{h,r,s}$ network is shown in Fig. 2 and consists of three layers. In the first layer, there is a source with h messages. In the middle layer, there are r nodes. The source has ℓ parallel links to each node in the middle layer. From any $\alpha = \frac{s-\epsilon}{\ell}$ nodes in the middle layer, there are ℓ parallel links to one receiver in the third layer. Additionally, from the source there are ϵ direct parallel links to each one of the $\binom{r}{\alpha}$ receivers in the third layer. Therefore, each receiver has $s = \alpha \ell + \epsilon$ incoming links. We will assume some relations between the parameters h, α, ϵ, and ℓ such that the resulting network is interesting and does not have a trivial or no solution (see Theorem 8).

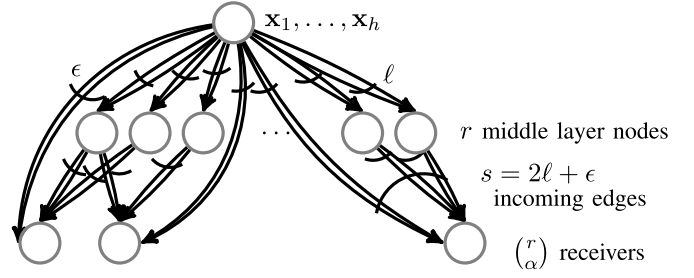Fig. 2. The (ϵ, ℓ)-$\mathcal{N}_{h,r,s}$ network for $\alpha = \frac{s-\epsilon}{\ell} = 2$, where each of the $\binom{r}{\alpha}$ receivers is connected to a unique set of α middle layer nodes and demands all the messages $\mathbf{x}_1, \ldots, \mathbf{x}_h$.

Remark 1: Our definition of the generalized combination networks depends on five parameters, ϵ, ℓ, h, r, and s, where ϵ and ℓ are parameters which do not appear in the combination networks. The value of h is the number of messages, r is the number of nodes in the middle layer, and the parameter s is the in-degree of each receiver. The parameter α denotes the number of edges leaving each middle node. Hence, one might equivalently define the generalized combination networks by using α instead of s.

Notice first that the *local* and *global* coding vectors for the (ϵ, ℓ)-$\mathcal{N}_{h,r,s}$ network must be the same (since only at the source the encoding can make a difference). Hence, we will not distinguish between them in the sequel. Second, it should be remarked that if $s > h$, then the min-cut of the (ϵ, ℓ)-$\mathcal{N}_{h,r,s}$ network is larger than the number of messages h. An equivalent network in which the min-cut is h, which is solved with an alphabet of the same size, can be constructed as follows: replace the i-th receiver R_i by a node T_i from which there are h links to h vertices P_{ij}, $1 \leq j \leq h$. From P_{ij}, $1 \leq j \leq h$, there is a link to a new receiver R_i'. Similarly, we can avoid parallel links in the network. Assume there are ℓ parallel links from vertex U to vertex V. We can remove these links and add ℓ vertices $W_1, W_2, \ldots, W_\ell$, such that there exists a link from U to W_i, $1 \leq i \leq \ell$, and there exists a link from each vertex W_i, $1 \leq i \leq \ell$, to V. Again, the new network is solvable over the same alphabet as the old network. In the (ϵ, ℓ)-$\mathcal{N}_{h,r,s}$ network, this transformation can be done by simply replacing each node in the middle layer by ℓ nodes.

The following subsections list several instances of the (ϵ, ℓ)-$\mathcal{N}_{h,r,s}$ network. In the next section, we will analyze the scalar linear solution and the vector solution for some of these special (ϵ, ℓ)-$\mathcal{N}_{h,r,s}$ networks and compare them in terms of the alphabet size q_s and q_v.

A. The Combination Networks

The $\mathcal{N}_{h,r,s}$ combination network is clearly a special case of the (ϵ, ℓ)-$\mathcal{N}_{h,r,s}$ network, where $\epsilon = 0$ and $\ell = 1$. This network with $h = s$ was already considered in Section III. We are not aware of any set of parameters for which a vector solution outperforms the optimal scalar linear solution in the unmodified combination network with respect to the alphabet size.

On the other hand, we can prove that there are combination networks for which the vector solution cannot outperform the scalar linear solution with respect to the alphabet size.
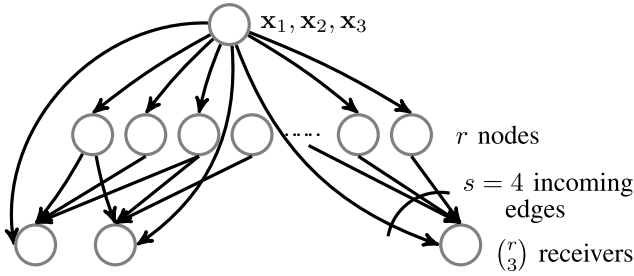
Fig. 3. The $(1,1)$-$\mathcal{N}_{3,r,4}$ network with $\binom{r}{3}$ receivers. For the same alphabet size $q_s = q_v = 4$, in the optimal scalar linear solution the number of middle layer nodes is $r \leq 42$, while in the optimal vector solution the number of middle layer nodes is $r \geq 51$ (see Section VIII), i.e., a vector solution outperforms the optimal scalar linear solution.

One interesting such an example is the $\mathcal{N}_{2,r,2}$ combination network. As was pointed out before, such a network has a solution of field size q_s if and only if an $[r, 2, d = r - 1]_{q_s}$ MDS code exists [37]. Such a code is also equivalent to a set of $r - 2$ pairwise orthogonal Latin squares of order q_s. The largest r so that such a code and a set can exist is $r = q_s + 1$. For every prime power q_s such a linear code and a set do exist. Hence, there is no difference between the alphabet size of the scalar linear solution and the scalar nonlinear solution. Since any vector solution can be translated to a scalar nonlinear solution over the same alphabet size, it follows that the vector solution cannot outperform the scalar linear solution with respect to the alphabet size. Unfortunately, we have no result of this kind for the $\mathcal{N}_{h,r,h}$ combination network when $h \geq 3$. We elaborate more on this in Section IX.

B. The Direct Links Combination Network

Another interesting family of networks that will be considered is the combination network with $\epsilon \geq 1$ additional direct links, i.e., the $(\epsilon, 1)$-$\mathcal{N}_{h,r,s}$ network. This network with $h = s = 3$ and $\epsilon = 1$ is discussed in Section VIII. It is the only network with three messages for which we obtained an advantage of a vector solution compared to the optimal scalar linear solution with respect to the alphabet size. Both the optimal scalar linear solution and the given vector solution for this subfamily of networks motivate some interesting questions on a classic coding problem and on a new type of subspace code problem, which will be discussed in the sequel. For $h = s = 3$ and $\epsilon = 1$ this network is illustrated in Fig. 3.

C. The <mark>One-Direct Link ℓ-Parallel Links $\mathcal{N}_{2\ell,r,2\ell+1}$ Network</mark>

The $(1, \ell)$-$\mathcal{N}_{2\ell,r,2\ell+1}$ network is shown in Fig. 4. It has three layers: a source in the first layer with $h = 2\ell$ messages and r nodes in the middle layer, where there are ℓ links from the source to each node in the middle layer. There are $\binom{r}{2}$ receivers, which form the third layer, where each set of two nodes from the middle layer is connected to a different receiver. If a node V from the middle layer is connected to a receiver R, then there are ℓ links from V to R. There is also one direct link from the source to each receiver. The total number of edges entering a receiver is $2\ell + 1$. This is the subfamily with the smallest number of direct links from the source to the receivers for which our vector solution outperforms the optimal scalar linear solution.
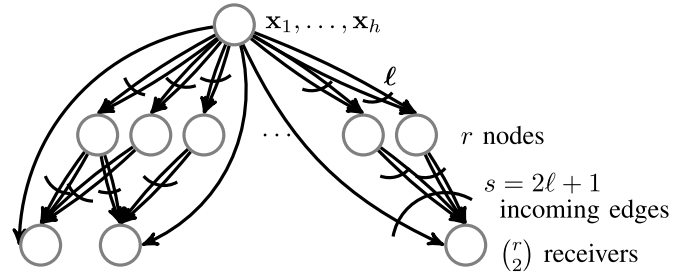

Fig. 4. The $(1, \ell)$-$\mathcal{N}_{2\ell,r,2\ell+1}$ network with $\binom{r}{2}$ receivers. For the alphabet sizes, we obtain $q_v = q^t$ and $q_s > q^{t^2/2}$ (see Section V-D), where $r = q^{\ell t(t+1)}$, i.e., when $r = q^{\ell t(t+1)}$, this network has a vector solution with $q_v = q^t$ and scalar solutions only if $q_s > q^{t^2/2}$.
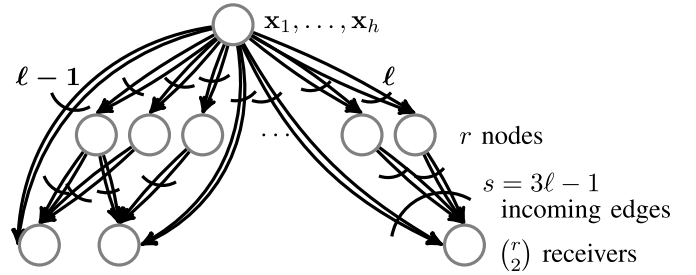

Fig. 5. The $(\ell-1, \ell)$-$\mathcal{N}_{2\ell,r,3\ell-1}$ network with $\binom{r}{2}$ receivers. For the alphabet sizes, we obtain $q_v = q^t$ and $q_s > q^{t^2(\ell-1)/\ell}$ (see Section V-E), where $r = q^{\ell(\ell-1)t^2+\ell t}$, i.e., when $r = q^{\ell(\ell-1)t^2+\ell t}$, this network has a vector solution with $q_v = q^t$ and scalar solutions only if $q_s > q^{t^2(\ell-1)/\ell}$.

D. The $(\ell - 1)$-Extra Links ℓ-Parallel Links $\mathcal{N}_{2\ell,r,3\ell-1}$ Network

The second subfamily in which vector solutions outperform scalar solutions is the $(\ell - 1, \ell)$-$\mathcal{N}_{2\ell,r,3\ell-1}$ network, which is shown in Fig. 5. This is a nontrivial subfamily in which the number of direct links from the source to the receivers is the largest one. It has three layers, with a source carrying $h = 2\ell$ messages in the first layer. In the second layer, there are r nodes and in the third layer, there are $\binom{r}{2}$ receivers. This network yields the largest gap in the alphabet size between our vector solution and the optimal scalar solution for an even number $h \geq 4$ of messages. The intersection with the previous subfamily, the $(1, \ell)$-$\mathcal{N}_{h,r,s}$ network, is when $\ell = 2$ and the related network is the $(1, 2)$-$\mathcal{N}_{4,r,5}$ network shown in Fig. 6.

V. VECTOR SOLUTIONS USING RANK-METRIC CODES WHICH OUTPERFORM SCALAR SOLUTIONS

A. Overview

In this section, we will consider vector solutions based on rank-metric codes for some of the generalized combination networks. We will start with a basic example of the $(1, 2)$-$\mathcal{N}_{4,r,5}$ network. The idea of the optimal scalar linear solution for this network will demonstrate the general idea of all our results with $h \geq 4$ messages. The gap between scalar and vector network coding is $q^{t^2/2+o(t)}$. The more general network that we consider later is the $(\ell - 1, \ell)$-$\mathcal{N}_{2\ell,r,3\ell-1}$ network for which the gap between scalar and vector network coding is $q^{(\ell-1)t^2/\ell+o(t)}$ for any $\ell \geq 2$.
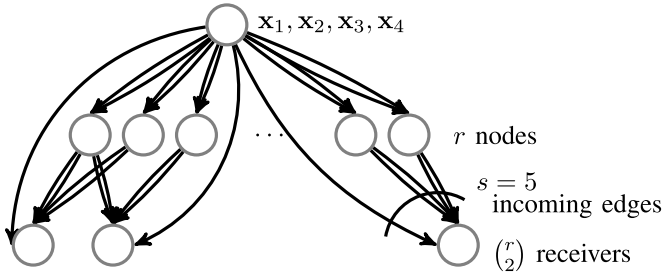
Fig. 6. The $(1, 2)$-$\mathcal{N}_{4,r,5}$ network with $\binom{r}{2}$ receivers. For the alphabet sizes, we obtain $q_v = q^t$ and $q_s > q^{t^2/2}$ (see Section V-B), where $r = q^{2t(t+1)}$, i.e., when $r = q^{2t(t+1)}$, this network has a vector solution with $q_v = q^t$ and scalar solutions only if $q_s > q^{t^2/2}$.

B. Scalar Linear Solution for the $(1, 2)$-$\mathcal{N}_{4,r,5}$ Network

For ease of understanding, the $(1, 2)$-$\mathcal{N}_{4,r,5}$ network is shown in Fig. 6.

Lemma 1: There is a scalar linear solution of field size q_s for the $(1, 2)$-$\mathcal{N}_{4,r,5}$ network if and only if $r \leq (q_s^2 + 1)(q_s^2 + q_s + 1)$.

Proof: Let $\mathbf{B}$ be a $4 \times (2r)$ matrix, divided into r blocks of two columns, with the property that any two blocks together have rank at least three. Each one of the r nodes in the middle layer of the network transmits two symbols (from one block) of $(x_1, x_2, x_3, x_4) \cdot \mathbf{B}$ (these symbols were transmitted to the node from the source). Each direct link transmits a symbol $p_i = \sum_{j=1}^{4} p_{ij} x_j$, for $i = 1, \ldots, \binom{r}{2}$, which is chosen such that the related 4×4-submatrix of $\mathbf{B}$ with the additional vector column $(p_{i1}, p_{i2}, p_{i3}, p_{i4})^T$ has full rank. Clearly, there is a scalar solution over $\mathbb{F}_{q_s}$ if and only if such a matrix over $\mathbb{F}_{q_s}$ exists.

These blocks are defined to be any 4×2 matrix representations of all two-dimensional subspaces of $\mathbb{F}_{q_s}^4$. Any two blocks together form a 4×4 matrix of rank at least three (since any two such subspaces are distinct).

From every node in the middle layer, there are two links to the appropriate receivers. Therefore, we associate each middle node with one block. The number of blocks is at most the number of distinct two-dimensional subspaces of $\mathbb{F}_{q_s}^4$, i.e., $r \leq \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{q_s}$ and therefore, a scalar solution exists if:

$$r \leq \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{q_s} = (q_s^2 + 1)(q_s^2 + q_s + 1).$$

To prove the "only if", we need to show that there is no scheme that provides more blocks. Assume, one block is a rank-one matrix. Then, all other blocks must have rank two and the space that they span has to be disjoint to the rank-one block. Therefore, with this scheme there are at most $1 + \begin{bmatrix} 3 \\ 2 \end{bmatrix}_{q_s} < \begin{bmatrix} 4 \\ 2 \end{bmatrix}_{q_s}$ blocks. Thus, for the largest r all blocks should have rank two, and taking all two-dimensional subspaces provides the maximum number of blocks. ∎

C. Vector Solution for the $(1, 2)$-$\mathcal{N}_{4,r,5}$-Network

Construction 2: Let $\mathcal{C} = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_{q^{2t^2+2t}}\}$ be an $\mathcal{MRD}[2t \times 2t, t]_q$ code and let $r \leq q^{2t^2+2t}$. Consider the

$(1, 2)$-$\mathcal{N}_{4,r,5}$ network with message vectors $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4 \in \mathbb{F}_q^t$. The i-th middle node receives and transmits:

$$\begin{pmatrix} \mathbf{y}_{i_1} \\ \mathbf{y}_{i_2} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_{2t} & \mathbf{C}_i \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \mathbf{x}_3 \\ \mathbf{x}_4 \end{pmatrix} \in \mathbb{F}_q^{2t}, \quad i = 1, \ldots, r.$$

The direct link from the source which ends in the same receiver as the links from two distinct nodes $i, j \in \{1, 2, \ldots, r\}$, of the middle layer transmits the vector $\mathbf{z}_{ij} = \mathbf{P}_{ij} \cdot (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4)^T \in \mathbb{F}_q^t$, where the $t \times (4t)$ matrix $\mathbf{P}_{ij}$ is chosen such that

$$\text{rk} \begin{pmatrix} \mathbf{I}_{2t} & \mathbf{C}_i \\ \mathbf{I}_{2t} & \mathbf{C}_j \\ & \mathbf{P}_{ij} \end{pmatrix} = 4t. \tag{1}$$

Since

$$\text{rk} \begin{pmatrix} \mathbf{I}_{2t} & \mathbf{C}_i \\ \mathbf{I}_{2t} & \mathbf{C}_j \end{pmatrix} = \text{rk} \begin{pmatrix} \mathbf{I}_{2t} & \mathbf{C}_i \\ \mathbf{0}_{2t} & \mathbf{C}_j - \mathbf{C}_i \end{pmatrix} \geq 3t,$$

it follows that the t rows of $\mathbf{P}_{ij}$ can be chosen such that the overall rank of the matrix from (1) is $4t$.

Theorem 6: Construction 2 provides a vector solution of field size q and dimension t to the $(1, 2)$-$\mathcal{N}_{4,r,5}$ network for any $r \leq q^{2t(t+1)}$.

Proof: Each receiver R_{ij} obtains the vectors $\mathbf{y}_{i_1}, \mathbf{y}_{i_2}, \mathbf{y}_{j_1}, \mathbf{y}_{j_2}$ and the vector $\mathbf{z}_{ij}$ from the direct link. From these five vectors, the receiver wants to reconstruct the message vectors $\mathbf{x}_1, \ldots, \mathbf{x}_4$ by solving the following linear system of equations:

$$\begin{pmatrix} \mathbf{y}_{i_1} \\ \mathbf{y}_{i_2} \\ \mathbf{y}_{j_1} \\ \mathbf{y}_{j_2} \\ \mathbf{z}_{ij} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_{2t} & \mathbf{C}_i \\ \mathbf{I}_{2t} & \mathbf{C}_j \\ & \mathbf{P}_{ij} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \mathbf{x}_3 \\ \mathbf{x}_4 \end{pmatrix}$$

The choice of $\mathbf{P}_{ij}$ from Construction 2 guarantees that this linear system of equations has a unique solution for $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4)$. ∎

D. Comparison of the Solutions for the $(1, 2)$-$\mathcal{N}_{4,r,5}$ Network

For the $(1, 2)$-$\mathcal{N}_{4,r,5}$ network, we obtain a significant improvement in the alphabet size for the vector solution compared to the optimal scalar linear solution. The alphabet size of the vector solution is $q_v = q^t$, while the field size q_s of the optimal scalar linear solution has to satisfy $r \leq (q_s^2 + 1)(q_s^2 + q_s + 1)$. Since r can be chosen to be q^{2t^2+2t}, the size of the gap is $q^{t^2/2+o(t)}$.

The same gap in the alphabet size can be obtained for the $(1, \ell)$-$\mathcal{N}_{2\ell,r,2\ell+1}$ network, for any $\ell \geq 2$, by using the same approach with an $\mathcal{MRD}[\ell t \times \ell t, (\ell - 1)t]_q$ code.

E. Solutions for the $(\ell - 1, \ell)$-$\mathcal{N}_{2\ell,r,3\ell-1}$ Network

To improve the gap on the alphabet size, i.e., to show that the advantage of our vector solution compared to the optimal scalar linear solution is even more significant, we consider in this subsection the $(\ell - 1, \ell)$-$\mathcal{N}_{2\ell,r,3\ell-1}$ network from Section IV-D.

Let us first consider the optimal scalar linear solution for this network.

Lemma 2: There is a scalar linear solution of field size q_s for the $(\ell-1, \ell)$-$\mathcal{N}_{2\ell,r,3\ell-1}$ network with 2ℓ messages, where $\ell \geq 2$, if and only if $r \leq \begin{bmatrix} 2\ell \\ \ell \end{bmatrix}_{q_s}$.

Proof: Let $\mathbf{B}$ be a $(2\ell) \times (\ell r)$ matrix, divided into r disjoint blocks of ℓ columns, with the property that any two blocks together have rank at least $\ell + 1$. Each of the r nodes in the middle layer of the network transmits ℓ symbols (from one block) of $(x_1, \ldots, x_{2\ell}) \cdot \mathbf{B}$ (these symbols were transmitted to the node from the source). Each direct link transmits a symbol $p_i = \sum_{j=1}^{2\ell} p_{ij} x_j$, for $i = 1, \ldots, \binom{r}{2}$, which is chosen such that the related $(2\ell) \times (2\ell)$ submatrix of $\mathbf{B}$ with the additional vector column $(p_{i1}, p_{i2}, p_{i3}, p_{i4})^T$ has full rank. Clearly, there is a scalar solution over $\mathbb{F}_{q_s}$ if and only if such a matrix over $\mathbb{F}_{q_s}$ exists.

Thus, each of these r blocks forms an ℓ-dimensional subspace of $\mathbb{F}_{q_s}^{2\ell}$ such that any two such ℓ-dimensional subspaces intersect in a subspace of dimension at most $(\ell - 1)$. Hence, the subspace distance between two such subspaces is at least two, and all ℓ-dimensional subspaces of $\mathcal{G}_{q_s}(2\ell, \ell)$ can be used. The size of $\mathcal{G}_{q_s}(2\ell, \ell)$ is $\begin{bmatrix} 2\ell \\ \ell \end{bmatrix}_{q_s}$ which completes the proof. ∎

Let us now consider the vector solution.

Construction 3: Let $\mathcal{C} = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_{q^{\ell(\ell-1)t^2+\ell t}}\}$ be an $\mathcal{MRD}[\ell t \times \ell t, t]_q$ code and let r be any integer such that $r \leq q^{\ell(\ell-1)t^2+\ell t}$. Consider the $(\ell-1, \ell)$-$\mathcal{N}_{2\ell,r,3\ell-1}$ network with message vectors $\mathbf{x}_1, \ldots, \mathbf{x}_{2\ell} \in \mathbb{F}_q^t$, where $\ell \geq 2$. The i-th middle node receives and transmits:

$$\begin{pmatrix} \mathbf{y}_{i_1} \\ \mathbf{y}_{i_2} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_{\ell t} & \mathbf{C}_i \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \vdots \\ \mathbf{x}_{2\ell} \end{pmatrix} \in \mathbb{F}_q^{\ell t}, \quad i = 1, \ldots, r.$$

The $\ell - 1$ direct links from the source, which end at the same receiver as the links from two distinct nodes $i, j \in \{1, 2, \ldots, r\}$ of the middle layer, transmit the vectors $\mathbf{z}_{ijs} = \mathbf{P}_{ijs} \cdot (\mathbf{x}_1, \ldots, \mathbf{x}_{2\ell})^T \in \mathbb{F}_q^t$, for $s = 1, \ldots, \ell - 1$, where the $t \times (2\ell t)$ matrices $\mathbf{P}_{ijs}$ are chosen such that

$$\mathrm{rk} \begin{pmatrix} \mathbf{I}_{\ell t} & \mathbf{C}_i \\ \mathbf{I}_{\ell t} & \mathbf{C}_j \\ & \mathbf{P}_{ij1} \\ & \vdots \\ & \mathbf{P}_{ij(\ell-1)} \end{pmatrix} = 2\ell t. \tag{2}$$

By the rank distance of $\mathcal{C}$ we have that $\mathrm{rk} \begin{pmatrix} \mathbf{I}_{\ell t} & \mathbf{C}_i \\ \mathbf{I}_{\ell t} & \mathbf{C}_j \end{pmatrix} \geq \ell t + t = (\ell+1)t$, and hence the $(\ell-1)t$ rows of the matrices $\mathbf{P}_{ijs}$ can be chosen such that the overall rank of the matrix from (2) is $2\ell t$.

The following result is an immediate consequence of this construction.

Corollary 3: Construction 3 provides a vector solution of field size q and dimension t to the $(\ell-1, \ell)$-$\mathcal{N}_{2\ell,r,3\ell-1}$ network for any $r \leq q^{\ell(\ell-1)t^2+\ell t}$ with 2ℓ messages for each $\ell \geq 2$.

For $r = q^{\ell(\ell-1)t^2+\ell t}$, we have that the field size q_s for any scalar linear solution has to satisfy $r = q^{\ell(\ell-1)t^2+\ell t} \leq \begin{bmatrix} 2\ell \\ \ell \end{bmatrix}_{q_s} < 4\, q_s^{\ell^2}$ (see Section II-D) and therefore the size of the

gap between the scalar and vector network coding solutions is $q^{(\ell-1)t^2/\ell+o(t)}$, for any $\ell \geq 2$. Further, the size of the gap tends to $q^{t^2+o(t)}$ for large ℓ.

VI. VECTOR SOLUTIONS USING SUBSPACE CODES

In this section, we will improve our vector solutions by using subspace codes. In the sequel it will be explained how larger gaps, as a function of t, between the alphabet size of the vector solution and the scalar linear solution can be obtained by using large subspace codes. However, the leading term in the exponent of the alphabet size in the gap will not change, i.e., *asymptotically*, there is no improvement compared to the subspace codes based on rank-metric codes. Moreover, the description with rank-metric codes is simpler and easier to analyze. However, by using larger subspace codes, we may be able to find vector solutions which outperform the optimal scalar solution (with respect to the alphabet size) in cases where this cannot be done using rank-metric codes. Finally, as we will see in Section VIII, there are important networks on which such improvements occur. Note that we have already used subspace codes for the scalar solutions of the generalized combination networks (see, e.g., Lemma 1 and Lemma 2). Also, our vector network coding constructions from the previous sections are based on rank-metric codes, but these codes can be seen as so-called *lifted rank-metric codes*, which are special subspace codes [40].

In this section and the following ones, we explain the simple formulation of these constructions, demonstrate how our rank-metric code based constructions can be improved by using larger subspace codes, and present a general question on subspace codes. Finally, we show a multicast network with three messages in which a vector solution outperforms the optimal scalar linear network solution, where the key is to use special classes of subspace codes.

The formulation of the solutions with subspace codes is as follows. Each message in the vector solution is a vector of length t. The global coding vectors for a given edge consists of h coding coefficients $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_h$, which are $t \times t$ matrices over $\mathbb{F}_q$. The packet associated with this edge is $(\mathbf{A}_1\, \mathbf{A}_2\, \cdots\, \mathbf{A}_h) \cdot (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_h)^T$. Instead of choosing these h coding coefficients based on lifted rank-metric codes, as in our previous constructions, we can use a $t \times (ht)$ matrix over $\mathbb{F}_q$ which is a basis for a t'-dimensional subspace of $\mathbb{F}_q^{ht}$, for some $t' \leq t$. A receiver R can recover the h messages if the $t \times (ht)$ matrices on $In(R)$ span the (ht)-dimensional space $\mathbb{F}_q^{ht}$. Each of these $t \times (ht)$ matrices is divided into h matrices from $\mathbb{F}_q^{t \times t}$ which are the global coding vectors on the edges. As before, we have to distinguish between the local coding vectors and the global coding vectors. We omit the discussion on the local coding vectors since in our networks, the local and global coding vectors are equal.

We will now consider some of the networks used in our discussion and analyze them with respect to a solution with subspace codes. We thereby consider only *Grassmannian codes*, i.e., all subspaces have the same dimension. Note that in some cases, better codes might be obtained by using subspaces of different dimensions. However, we will not consider them in this paper, as the general idea can be understood from the

Grassmannian codes, and the order of magnitude does not change (which is the same as the one by the constructions based on rank-metric codes). We should note that if we append the h coding coefficients which are $t \times t$ matrices in the general framework of vector network coding, we will obtain $t \times (ht)$ matrices which are a basis of a subspace, and we will obtain a construction based on subspace codes. However, to figure out which $t \times t$ matrices to take for this purpose is an almost impossible mission without going through the related subspace codes.

Now, we consider the (ϵ, ℓ)-$\mathcal{N}_{2\ell,r,s}$ network. In such a network, the sets of ℓ parallel edges carry subspaces from $\mathcal{G}_q(2\ell t, \ell t)$, while the ϵ parallel direct links from the unique source to the receivers carry subspaces from $\mathcal{G}_q(2\ell t, \epsilon t)$. The (ℓt)-dimensional subspaces on the edges from the source to the middle layer form a code $\mathbb{C}$ in $\mathcal{G}_q(2\ell t, \ell t)$ such that any two codewords (subspaces) of $\mathbb{C}$ span a subspace of $\mathbb{F}_q^{2\ell t}$ whose dimension is at least $(2\ell - \epsilon)t$, i.e., the minimum subspace distance of $\mathbb{C}$ is at least $(2\ell - 2\epsilon)t$.

We now consider the solution for the $(\ell - 1, \ell)$-$\mathcal{N}_{2\ell,r,3\ell-1}$ network. The scalar solution and the vector solution are very similar for this network. Recall that the optimal scalar solution (given in Lemma 2) is obtained when we consider that a node in the middle layer is transmitting ℓ blocks, each one with 2ℓ symbols from the alphabet q_s. In the optimal scalar linear solution, each of these ℓ blocks forms an ℓ-dimensional subspace of $\mathbb{F}_{q_s}^{2\ell}$ such that any two such ℓ-dimensional subspaces intersect in an at most $(\ell - 1)$-dimensional subspace. Hence, the subspace distance between two such subspaces is at least two, i.e., the largest such set of subspaces consists of all the ℓ-dimensional subspaces of $\mathcal{G}_{q_s}(2\ell, \ell)$. The size of $\mathcal{G}_{q_s}(2\ell, \ell)$ is $\begin{bmatrix} 2\ell \\ \ell \end{bmatrix}_{q_s} < 4q_s^{\ell^2}$ (see Section II-D). For the vector solution, we use a subspace code $\mathbb{C}$ in $\mathcal{G}_q(2\ell, \ell t)$ with subspace distance at least $2t$. The maximum size of such a code is larger than $q^{\ell(\ell-1)t^2+\ell t}$ (see Theorem 2). Thus, we have that $q_s = q^{(\ell-1)t^2/\ell+o(t)}$, while $q_v = q^t$.

Constructions of large codes for this purpose can be found for example in [14]. However, as said the improvement is not large since asymptotically the subspace code obtained from an MRD code which was used for example in Construction 2 is optimal and can be improved by at most a factor of two (see Theorem 2).

VII. ANALYZING GENERALIZED COMBINATION NETWORKS WITH VECTOR SOLUTIONS

In this section, we will compare the optimal scalar linear solution to our vector solution with respect to the alphabet size for some subfamilies of the generalized combination networks.

Consider first the unmodified $\mathcal{N}_{h,r,s}$ combination network. It was proven in [37] that the network has a scalar solution (not necessarily linear) if and only if a code over $\mathbb{F}_{q_s}$ with q_s^h codewords and minimum Hamming distance $r - s + 1$ exists. A scalar linear solution exists for related linear codes. For a vector solution based on subspace codes, we need a code $\mathbb{C}$ which is a subset of $\mathcal{G}_q(ht, t)$ such that any s codewords of $\mathbb{C}$ span $\mathbb{F}_q^{ht}$. Such a vector solution can be constructed from the scalar linear solution by using the companion matrix and its powers; and it is equivalent to the scalar solution. In order to

outperform the scalar linear solution, we would need a larger such code. However, no set of parameters for which such a code exists is known.

The next considered subfamily of generalized combination networks is the $(\epsilon, 1)$-$\mathcal{N}_{h,r,s}$ network (Section IV-B). Three messages and $s = h$ will be considered in the next section, where we will discuss also the other networks in this subfamily and also related networks.

From the given framework of the vector network solution using subspace codes, it is easy to verify that if we want to use error-correcting constant dimension codes for our vector solution of the (ϵ, ℓ)-$\mathcal{N}_{h,r,s}$ network, with $\ell \geq 1$, then it is required that $\frac{s-\epsilon}{\ell}$ equals two. Hence, the number of receivers is $\binom{r}{2}$, as each receiver gets its information from two distinct nodes from the middle layer; otherwise the requirement is that at least three codewords will participate when we examine the dimension spanned by the appropriate number of subspaces. The two examples of networks for which our vector solution outperforms the optimal scalar linear solution (see Section V) have this property, and $\frac{s-\epsilon}{\ell} = 2$. Clearly, we must also have that $\epsilon + \ell < h$, since otherwise the information on the ϵ direct links can always complete the information on the ℓ parallel links to the ambient h-space. Another requirement is that $h - 2\ell \leq \epsilon$, since otherwise the cut at the receivers will be $2\ell + \epsilon < h$, and hence the receiver will not be able to recover h messages, as h is larger than the min-cut. Therefore, we have that $h - 2\ell \leq \epsilon < h - \ell$, or equivalently $\epsilon < h - \ell \leq \epsilon + \ell$. Since the ϵ direct links can always be chosen in a way that they complete the information with the other 2ℓ links to the ambient h-space, it follows that the value of r depends only on the choice of the information on the 2ℓ links entering any given receiver. Each receiver should obtain a $(2\ell - \epsilon)$-subspace of $\mathbb{F}_{q_s}^h$. Hence, for the scalar linear solution we require to have a code $\mathbb{C}$ in the Grassmannian $\mathcal{G}_{q_s}(h, \ell)$ such that its minimum subspace distance $d = 2\delta$ satisfies $h - \epsilon = \ell + \delta$, i.e., $\delta = h - \ell - \epsilon$. For the optimal scalar linear solution, we distinguish between two cases: $h - \ell \leq \ell$ and $h - \ell \geq \ell$. If $h - \ell \geq \ell$, then our code $\mathbb{C}$ has at least size $q_s^{(h-\ell)(2\ell-h+\epsilon+1)}$ by Theorem 2. If $h - \ell \leq \ell$, then our code $\mathbb{C}$ has at least size $q_s^{\ell(\epsilon+1)}$ by Theorem 2.

For our vector solution, our best code $\mathbb{C}$ is in the Grassmannian $\mathcal{G}_q(ht, \ell t)$, and with the same reasons, its minimum subspace distance is $2(h - \ell - \epsilon)t$. We distinguish again between the same two cases: $h - \ell \leq \ell$ and $h - \ell \geq \ell$. If $h - \ell \geq \ell$, then our code $\mathbb{C}$ has size at least $q^{(h-\ell)t(2\ell t-ht+\epsilon t+1)}$ by Theorem 2. If $h - \ell \leq \ell$, then our code $\mathbb{C}$ has size at least $q^{\ell t(\epsilon t+1)}$ by Theorem 2. The following theorem summarizes the minimal order of q_s.

Theorem 7: For the (ϵ, ℓ)-$\mathcal{N}_{h,r,2\ell+\epsilon}$ network, there exists a vector solution of dimension t over a field of size q, i.e., $q_v = q^t$, and the scalar linear solution has field size at least q_s (for the following given r),

1) if $h - \ell \leq \ell$ and $\epsilon = 0$, then $r = q^{\ell t}$ and $q_s = q^t$.
2) if $h - \ell \leq \ell$ and $\epsilon \neq 0$, then $r = q^{(\ell t)(\epsilon t+1)}$ and $q_s = q^{\epsilon t^2/(\epsilon+1)+o(t)}$.
3) if $h - \ell \geq \ell$ and $2\ell - h + \epsilon = 0$, then $r = q^{(h-\ell)t}$ and $q_s = q^t$.

4) if $h - \ell \geq \ell$ and $2\ell - h + \epsilon \neq 0$, then $r = q^{(h-\ell)t(2\ell t - ht + \epsilon t + 1)}$ and $q_s = q^{(2\ell - h + \epsilon)t^2/(2\ell - h + \epsilon + 1) + o(t)}$.

To obtain the largest possible gap between q_v and q_s using our methods, we have to optimize the order in the cases given in Theorem 7, which do not depend only on t, i.e., case 2 and case 4.

2) If $h - \ell \leq \ell$ and $\epsilon \neq 0$, then we have to maximize $q^{\epsilon t^2/(\epsilon+1)}$, i.e., for a given h, we must have the largest possible ϵ. Since $\ell + \epsilon < h$, it follows that we should have $\epsilon = h - \ell - 1$, and ℓ should be small as possible.

    a) If h is even, then the smallest ℓ is obtained when $h = 2\ell$ (since $h \leq 2\ell$), i.e., $\ell = \frac{h}{2}$. Hence, ϵ gets the maximum value when $\epsilon = \ell - 1 = \frac{h}{2} - 1$. Therefore, the largest gap occurs when $q_s = q^{(h-2)t^2/h+o(t)}$, and the network that achieves the largest gap is the $(\ell - 1, \ell)$-$\mathcal{N}_{2\ell, r, 3\ell-1}$ network.

    b) If h is odd, then the smallest ℓ is obtained when $h = 2\ell - 1$ (since $h \leq 2\ell$), i.e., $\ell = \frac{h+1}{2}$. Thus, ϵ has to be maximized, and the largest gap occurs when $q_s = q^{(h-3)t^2/(h-1)+o(t)}$. The network that achieves this largest gap is the $(\ell - 2, \ell)$-$\mathcal{N}_{2\ell-1, r, 3\ell-2}$ network.

4) If $h - \ell \geq \ell$ and $2\ell - h + \epsilon \neq 0$, then we have to maximize $q^{(2\ell - h + \epsilon)t^2/(2\ell - h + \epsilon + 1)}$, i.e., for a given h, we must have the largest possible value for $2\ell - h + \epsilon$. Since $\ell + \epsilon < h$, it follows that we should have $\epsilon = h - \ell - 1$, and hence we have to maximize $2\ell - h + \epsilon = 2\ell - h + h - \ell - 1 = \ell - 1$.

    a) If h is even, then the largest ℓ is obtained for $h = 2\ell$ (since $h \geq 2\ell$), i.e., $\ell = \frac{h}{2}$. Therefore, $2\ell - h + \epsilon$ is maximized for $2\ell - h + \epsilon = 2\frac{h}{2} - h + h - \frac{h}{2} - 1 = \frac{h}{2} - 1$. Thus, the largest gap occurs when $q_s = q^{(h-2)t^2/h+o(t)}$, and the network that achieve the largest gap is the $(\ell - 1, \ell)$-$\mathcal{N}_{2\ell, r, 3\ell-1}$ network (the same one as before, since the intersection of the two cases is when $h - \ell = \ell$).

    b) If h is odd, then the largest gap is obtained for $h = 2\ell + 1$ (since $h \geq 2\ell$), i.e., $\ell = \frac{h-1}{2}$. Hence, $2\ell - h + \epsilon$ is maximized for $2\ell - h + \epsilon = 2\frac{h-1}{2} - h + h - \frac{h-1}{2} - 1 = \frac{h-1}{2} - 1$. It implies that the largest gap occurs when $q_s = q^{(h-3)t^2/(h-1)+o(t)}$, and the network that achieves the largest gap is the $(\ell - 1, \ell)$-$\mathcal{N}_{2\ell+1, r, 3\ell-1}$ network.

VIII. SCALAR AND VECTOR SOLUTIONS FOR GENERAL NETWORKS

In the previous sections, we have discussed specific sub-families of the generalized combination networks. The main goal was to find networks that, to our knowledge, achieve the largest gap in the alphabet size between a vector solution and the optimal scalar linear solution. In this section, we discuss the requirements needed for a scalar linear solution and the requirements needed for a vector solution for another subfamily of the generalized combination networks. As before, we aim to find the smallest alphabet size for which such a solution exists. Indeed, we will start with the most general network, the (ϵ, ℓ)-$\mathcal{N}_{h,r,\alpha\ell+\epsilon}$ network, to provide the requirements for its solution. However, the code required for such a solution cannot be constructed generally for a large set of parameters. Hence, also in this section, we will continue in a few steps from simpler subfamilies to more evolved ones. The reason is that a network coding problem for simple subfamilies might be feasible to solve, while it might be too difficult to provide the solution for the the most general networks. One of the highlights of this section is a network with three messages in which vector network coding outperforms scalar network coding. This is one of the parameters we could not obtain in our previous constructions. For two messages, unfortunately, this problem remains open. The vector solution for three messages raises an interesting open question on subspace codes.

The most general network is the (ϵ, ℓ)-$\mathcal{N}_{h,r,\alpha\ell+\epsilon}$ network, where $\epsilon \geq 0$ and $\ell \geq 1$. To avoid trivial solutions (i.e., routing), we must have that $\ell + \epsilon < h$, and to avoid unsolvable networks by the min-cut/max-flow condition, we must have that $\alpha\ell + \epsilon \geq h$. This is summarized in the following theorem.

Theorem 8: The (ϵ, ℓ)-$\mathcal{N}_{h,r,\alpha\ell+\epsilon}$ network has a trivial solution if $\ell + \epsilon \geq h$, and it has no solution if $\alpha\ell + \epsilon < h$.

We start with the scalar linear solution for the general network. Each set of parallel ℓ links carries ℓ vectors which span a subspace of dimension at most ℓ from the h-space $\mathbb{F}_{q_s}^h$. The subspaces on these ℓ parallel links define a subspace code in $\mathcal{P}_{q_s}(h)$ (the set of all subspaces from $\mathbb{F}_{q_s}^h$) such that any subset of α codewords spans a subspace of $\mathbb{F}_{q_s}^h$ whose dimension is at least $h - \epsilon$. We continue with the vector solution for the general network. Each set of parallel ℓ links carries a vector which spans a subspace of dimension at most ℓt from the (ht)-dimensional subspace $\mathbb{F}_q^{ht}$. The subspaces on these ℓ parallel links define a subspace code in $\mathcal{P}_q(ht)$ such that any subset of α codewords (subspaces) spans a subspace of $\mathbb{F}_q^{ht}$ whose dimension is at least $ht - \epsilon t$. The requirements on codes or subspace codes for the scalar linear solution and the subspace codes for the vector solution are too general. We suggest to split the problem into a few questions related to the different subfamilies of the generalized combination network.

A. Scalar Solution for the $(\epsilon, 1)$-$\mathcal{N}_{h,r,\alpha+\epsilon}$ Network

We start with the $(\epsilon, 1)$-$\mathcal{N}_{h,r,\alpha+\epsilon}$ network. This network is very similar to the $\mathcal{N}_{h,r,\alpha}$ combination network. The only difference between these two classes of networks are the ϵ direct links from the source to each receiver. For the optimal scalar linear solution, we need an $h \times r$ matrix over $\mathbb{F}_q$ such that any α columns span a subspace of $\mathbb{F}_{q_s}^h$ whose dimension is at least $h - \epsilon$. This is usually not a simple problem. For $\epsilon = 0$ this is equivalent to the error-correcting code problem as was defined in [37], i.e., constructing a code of length r with q_s^h codewords with minimum Hamming distance $r - \alpha + 1$ for a field of smallest possible size q_s. This can be generalized for any ϵ such that $0 \leq \epsilon \leq h - 2$. A scalar solution (linear or nonlinear) over $\mathbb{F}_{q_s}$ for the $(\epsilon, 1)$-$\mathcal{N}_{h,r,\alpha+\epsilon}$

network exists if and only if there exists a code over $\mathbb{F}_{q_s}$ of length r with q_s^h codewords and minimum Hamming distance $r - \alpha - \epsilon + 1$. Hence, the addition of the direct edges from the source to the receivers enables us to use longer codes with smaller alphabet size for the scalar solution, but the type of the coding problem remains the same. Therefore, the question on a suitable construction is a standard problem in error-correcting codes.

B. Vector Solution for the $(\epsilon, 1)$-$\mathcal{N}_{h,r,\alpha+\epsilon}$ Network

For the vector solution, we need something different, stated in the following question.

Question 1: What is the largest set of r subspaces of dimension at most t of the space $\mathbb{F}_q^{ht}$ such that any subset of α subspaces spans a subspace of dimension at least $(h - \epsilon)t$?

While the scalar linear solution poses a classic coding problem for this network, the vector solution poses a completely new coding problem on subspace codes. In fact, while we have lot of knowledge on the solution for the coding problem posed by the scalar linear solution, we hardly know anything about an answer to Question 1. As described in previous sections, if $\alpha = 2$, then Question 1 reduces to the problem of designing error-correcting subspace codes. We discuss now a more specific subfamily of these networks.

The $(1, 1)$-$\mathcal{N}_{h,r,h+1}$ network, with $h \geq 3$, is the simplest known modification of the combination networks from all our new networks which exhibit the advantage of vector network coding on scalar network coding with respect to the alphabet size. The $(1, 1)$-$\mathcal{N}_{h,r,h+1}$ network consists of the unmodified combination network $\mathcal{N}_{h,r,h}$ with an additional direct link from the source to each receiver.

C. Scalar Solution for the $(1, 1)$-$\mathcal{N}_{3,r,4}$ Network

In this subsection, we discuss the case $h = 3$, i.e., the source has three messages (see also Fig. 3). Given a receiver R, it obtains its information from three nodes in the middle layer and from the direct link from the source. For the scalar linear solution, each such link has a coding vector of length three. The receiver is able to recover the three messages, if its four received vectors span a subspace of dimension three. This implies that the three links from the middle layer carry three vectors which span a subspace of $\mathbb{F}_{q_s}^4$ whose dimension is at least two. To ensure that each receiver will receive three vectors which span such a subspace, we have to guarantee that on the links between the source and the nodes of the middle layer, no three links will contain a vector which is contained in the same one-dimensional subspace (two such links can have such vectors). Thus, for a scalar linear solution, we must have that $r \leq 2\begin{bmatrix}3\\1\end{bmatrix}_{q_s} = 2\frac{q_s^3-1}{q_s-1} = 2(q_s^2 + q_s + 1)$. Fortunately, a related assignment of the coefficients for the coding vectors of the edges induces a scalar solution with $r = 2(q_s^2 + q_s + 1)$.

D. Vector Solution for the $(1, 1)$-$\mathcal{N}_{3,r,4}$ Network

We continue with a vector solution for this network. Assume now that the three messages are vectors of length t over $\mathbb{F}_q$. Now, the coefficients on each link are three $t \times t$ matrices over $\mathbb{F}_q$. Each such three coefficients on a link can be represented as a $t \times (3t)$ matrix. The receivers can recover the

three messages if any three such matrices on the links between the source and the nodes of the middle layer span a subspace of $\mathbb{F}_q^{3t}$ whose dimension is at least $2t$. Our problem is to find the largest possible r with this property, and it can be formulated by the following coding problem in the Grassmannian $\mathcal{G}_q(3t, t)$: Find the largest set of subspaces from $\mathcal{G}_q(3t, t)$ such that any three subspaces of the set span a subspace of dimension at least $2t$. If the size of this set r is greater than $2(q_s^2 + q_s + 1)$, then our vector solution outperforms the optimal scalar linear solution in the $(1, 1)$-$\mathcal{N}_{3,r,4}$ network.

We consider now a specific example which can be generalized. Assume $q_s = 4 = 2^2$, i.e., $r \leq 2 \cdot (4^2 + 4 + 1) = 42$, and consider the vector solution, where the messages are binary vectors of length $t = 2$. Hence, the edges will carry two-dimensional subspaces of $\mathbb{F}_2^6$. Vector network coding will outperform optimal scalar linear network coding if there exist more than 42 two-dimensional subspaces of $\mathbb{F}_2^6$ such that any three two-dimensional subspaces will span at least a four-dimensional subspace of $\mathbb{F}_2^6$, so they will be completed by the direct link from the source to the receiver.

Let β be a primitive element in $\mathbb{F}_{2^4}$ satisfying $\beta^4 = \beta + 1$. We form the following set of 51 two-dimensional subspaces of $\mathbb{F}_2^6$: $\{\langle 01\beta^i, 10\beta^{i+1}\rangle \; : \; 0 \leq i \leq 14\}$, $\{\langle 01\beta^i, 10\beta^{i+2}\rangle \; : \; 0 \leq i \leq 14\}$, $\{\langle\langle 01\beta^i, 10\beta^{i-1}\rangle \; : \; 0 \leq i \leq 14\}$, $\{\langle 00\beta^i, 00\beta^{i+5}\rangle \; : \; 0 \leq i \leq 4\}$, and $\{\langle 100000, 010000\rangle\}$. One can easily verify that any three of these 51 two-dimensional subspaces span at least a four-dimensional subspace and hence, our vector solution outperforms the optimal scalar linear solution in this case. Recently, 97 two-dimensional subspaces of $\mathbb{F}_2^6$, such that any three two-dimensional subspaces will span at least a four-dimensional subspace of $\mathbb{F}_2^6$, were found [13].

IX. CONCLUSIONS AND PROBLEMS FOR FUTURE RESEARCH

We have shown that our vector solutions outperform the optimal scalar linear solution in the alphabet size for several generalizations of the combination networks. The key is the use of subspace codes, particularly subspace codes derived from rank-metric codes. Our networks and codes imply a gap of size $q^{(h-2)t^2/h + o(t)}$ for even $h \geq 4$, and a gap of size $q^{(h-3)t^2/(h-1) + o(t)}$ for any odd $h \geq 5$, between the alphabet size of our vector solution and the optimal scalar linear solution for multicast networks, where h is the number of messages and t is the length of the vectors. Clearly, a vector solution can be translated to a scalar nonlinear solution. Therefore, our results also imply a gap of size $q^{(h-2)t^2/h + o(t)}$ for any even $h \geq 4$, and a gap of size $q^{(h-3)t^2/(h-1) + o(t)}$ for any odd $h \geq 5$, between the field size in *linear* and *nonlinear* scalar network coding for multicast networks. We have also proved the existence of a multicast network with three messages in which the vector solution outperforms the scalar linear solution.

There are many interesting questions which remain open after our discussion. Some of these open questions for future research are briefly outlined and discussed as follows.

1) Can the $\mathcal{N}_{h,r,h}$ combination network have a vector solution based on an $\mathcal{MRD}[t \times t, t]_q$ code which

outperforms the optimal scalar linear solution? We conjecture that the answer is NO. Clearly, if the MRD code consists of a companion matrix and its powers, then this is not possible since each power of the companion matrix can be translated to the related element in the finite field and the vector solution can be translated to a scalar linear solution. Are all the $\mathcal{MRD}[t \times t, t]_q$ codes equivalent in this sense? We conjecture that the answer is YES.

2) Can the $\mathcal{N}_{h,r,h}$ combination network have a vector solution based on subspace codes which outperforms the optimal scalar linear solution? If such a code $\mathbb{C}$ with r codewords exists, then any h t-dimensional subspaces of $\mathbb{C}$ have to span the ambient space $\mathbb{F}_q^{ht}$. We have shown that the answer is negative for $h = 2$ and we conjecture it is negative for all h.

3) Can any $\mathcal{N}_{h,r,s}$ combination network have a vector solution which outperforms the optimal scalar linear solution? Since the scalar solution of the $\mathcal{N}_{h,r,s}$ combination network uses an error-correcting code, this question is of a great interest. The scalar solution for the $\mathcal{N}_{h,r,h}$ combination network uses an MDS code. A vector solution which outperforms the scalar solution implies subspace codes which go beyond the MDS bound. For some codes, we can prove that a vector solution cannot outperform the optimal scalar linear solution.

4) Does any $(0, \ell)$-$\mathcal{N}_{h,r,s}$ network, $\ell > 1$, have a vector solution which outperforms the scalar solution? If $s = 2\ell$ this is related to some interesting questions on subspace codes, where the most interesting case is related to spreads and partial spreads in projective geometry.

5) Does there exist a multicast network with *two* messages in which a vector solution outperforms the optimal scalar linear solution?

6) For multicast networks with $h = 3$ messages which have a vector solution of dimension t over $\mathbb{F}_q$, what is the largest alphabet size required for a solution with scalar linear network coding? It was pointed out by Roth [39] that by a probabilistic argument, there exists a set with at least $q^{t^2/3}$ t-dimensional subspace of $\mathbb{F}_q^{3t}$ for which any three subspaces span a subspace of dimension at least $2t$. This probabilistic argument can be generalized for any h. Is this an optimal solution? It is a future task to find a construction of such a code and possibly a larger one.

7) For multicast networks which have a vector solution of dimension t over $\mathbb{F}_q$, is there an algorithm which transforms the vector solution into a scalar linear solution? What is the alphabet size required by this transformation? We believe that the minimum alphabet size for scalar network coding is at most $q^{(h-2)t^2/h+o(t)}$ for even $h \geq 4$ and at most $q^{(h-3)t^2/(h-1)+o(t)}$ for odd $h \geq 5$, but an algorithm for any larger alphabet might be interesting to begin with, e.g., an alphabet of size q^{t^2} seems to be an excellent achievement.

8) Is there a network with h messages in which exactly h edge disjoint paths are used (for network coding) from the source to each receiver, and on which vector network coding outperforms scalar linear network coding? Note that our constructions use more than h paths. In other words, can vector network coding outperform scalar linear network coding in a network in which the deletion of any edge will destroy the multicast property?

9) What is the largest possible gap between the field size in scalar nonlinear network coding and scalar linear network coding for multicast networks? This gap is at least the size of the gap between the vector solution and the optimal scalar linear solution. However, is it possible to obtain a larger gap between nonlinear and linear scalar network coding? Dougherty *et al.* [9] proved that for any integer $h \geq 3$, there exists a multicast network with h messages that has a binary solution but does not have a binary linear solution. This result implies that there is no vector solution with vectors of length one over $\mathbb{F}_2$. Can this result be generalized to any non-binary alphabet? Can it be also generalized to vectors of length greater than one? What is the largest possible gap in the alphabet size between nonlinear scalar network coding and vector network coding?

10) For given $h \geq 3$, $\alpha \geq 3$, and $1 \leq \epsilon \leq h - 2$, what is the size of the largest code in $\mathcal{G}_q(ht, \ell t)$ such that any α codewords span a subspace of dimension at least $(h - \epsilon)t$? This question has an immediate application for $h = 3$, $\alpha = 3$, and $\epsilon = 1$ in constructing networks with three messages for which vector network coding outperforms scalar coding. Also, it is interesting to see the related results in the performance of vector network coding for $h > 3$. This is a generalization of the standard coding problem for subspace codes. For $\alpha = 2$, such a code is a subspace code with minimum subspace distance $2(h - \ell - \epsilon)$. This problem was considered recently in [19].

REFERENCES

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

[2] J. Cannons, R. Dougherty, C. Freiling, and K. Zeger, "Network routing capacity," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 777–788, Mar. 2006.

[3] J. Connelly and K. Zeger, "Linear network coding over rings—Part I: Scalar codes and commutative alphabets," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 274–291, Jan. 2018. [Online]. Available: https://arxiv.org/abs/1608.01738

[4] J. Connelly and K. Zeger, "Linear network coding over rings—Part II: Vector codes and non-commutative alphabets," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 292–308, Jan. 2018. [Online]. Available: https://arxiv.org/abs/1608.01737

[5] N. Das and B. K. Rai, "On the message dimensions of vector linearly solvable networks," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1701–1704, Sep. 2016.

[6] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *J. Combinat. Theory A*, vol. 25, no. 3, pp. 226–241, Nov. 1978.

[7] F. Didier. (Jan. 2009). "Efficient erasure decoding of Reed–Solomon codes." [Online]. Available: https://arxiv.org/abs/0901.1886

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

[9] R. Dougherty, C. Freiling, and K. Zeger, "Linearity and solvability in multicast networks," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2243–2256, Oct. 2004.

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

[11] J. B. Ebrahimi and C. Fragouli, "Algebraic algorithms for vector network coding," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 996–1007, Feb. 2011.

[12] T. Etzion, E. Gorla, A. Ravagnani, and A. Wachter-Zeh, "Optimal Ferrers diagram rank-metric codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 1616–1630, Apr. 2016.

[13] T. Etzion, S. Kurz, K. Otal, and F. Özbudak, in preparation.

[14] T. Etzion and N. Silberstein, "Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 2909–2919, Jul. 2009.

[15] T. Etzion and N. Silberstein, "Codes and designs related to lifted MRD codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1004–1017, Feb. 2013.

[16] T. Etzion and L. Storme, "Galois geometries and coding theory," *Designs, Codes Cryptogr.*, vol. 78, no. 1, pp. 311–350, Jan. 2016.

[17] T. Etzion and A. Vardy, "Error-correcting codes in projective space," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1165–1173, Feb. 2011.

[18] T. Etzion and A. Wachter-Zeh, "Vector network coding based on subspace codes outperforms scalar linear network coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 1949–1953.

[19] T. Etzion and H. Zhang. (2018). "Grassmannian codes with new distance measures for network coding." [Online]. Available: https://arxiv.org/abs/1801.02329

[20] C. Fragouli and E. Soljanin, "(Secure) linear network coding multicast," *Designs, Codes Cryptogr.*, vol. 78, no. 1, pp. 269–310, Jan. 2016.

[21] È. M. Gabidulin, "Theory of codes with maximum rank distance," *Problemy Peredachi Informatsii*, vol. 21, no. 1, pp. 3–16, 1985.

[22] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[23] I. Gohberg and V. Olshevsky, "Fast algorithms with preprocessing for matrix-vector multiplication problems," *Common Divisors Matrix Polynomials, I. Spectral Method, Indiana J. Math.*, vol. 30, pp. 321–1981, 1994.

[24] S. Jaggi, Y. Cassuto, and M. Effros, "Low complexity encoding for network codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2006, pp. 40–44.

[25] S. Jaggi *et al.*, "Polynomial time algorithms for multicast network code construction," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 1973–1982, Jun. 2005.

[26] R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.

[27] R. Kötter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[28] M. Langberg, A. Sprintson, and J. Bruck, "Network coding: A computational perspective," *IEEE Trans. Inf. Theory*, vol. 55, no. 1, pp. 147–157, Jan. 2009.

[29] M. Langberg and A. Sprintson, "Recent results on the algorithmic complexity of network coding," in *Proc. Workshop Netw. Coding, Theory, Appl. (NetCod)*, 2009, pp. 1–3.

[30] M. Langberg and A. Sprintson, "On the hardness of approximating the network coding capacity," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, Jul. 2008, pp. 315–319.

[31] A. R. Lehman and E. Lehman, "Complexity classification of network information flow problems," in *Proc. 15th ACM-SIAM Symp. Discrete Algorithms (SODA)*, 2004, pp. 142–150.

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

[33] P. Lusina, E. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2757–2760, Oct. 2003.

[34] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1988.

[35] M. Médard, M. Effros, D. Karger, and T. Ho, "On coding for non-multicast networks," in *Proc. 41st Allerton Conf. Commun., Control Comput.*, Monticello, IL, USA, Oct. 2003, pp. 1–9.

[36] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, *Applications of Finite Fields*. Berlin, Germany: Springer, 1993.

[37] S. Riis and R. Ahlswede, "Problems in network coding and error correcting codes," in *General Theory of Information Transfer and Combinatorics* (Lecture Notes in Computer Science), vol. 4123. Berlin, Germany: Springer, 2006, pp. 861–897.

[38] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 328–336, Mar. 1991.

[39] R. M. Roth, personal communication, Apr. 2016.

[40] D. Silva, F. R. Kschischang, and R. Kötter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.

[41] Q. Sun, X. Yang, K. Long, and Z. Li, "Constructing multicast networks where vector linear coding outperforms scalar linear coding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 2633–2637.

[42] Q. Sun, X. Yang, K. Long, X. Yin, and Z. Li, "On vector linear solvability of multicast networks," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5096–5107, Dec. 2016.

[43] Q. Sun, X. Yin, Z. Li, and K. Long, "Multicast network coding and field sizes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun./Jul. 2014, pp. 2157–2161.

[44] L. R. Turner, "Inverse of the Vandermonde matrix with applications," NASA, Washington, DC, USA, Tech. Note D-3547, Aug. 1966.

Tuvi Etzion (M'89–SM'94–F'04) was born in Tel Aviv, Israel, in 1956. He received the B.A., M.Sc., and D.Sc. degrees from the Technion - Israel Institute of Technology, Haifa, Israel, in 1980, 1982, and 1984, respectively. From 1984 he held a position in the Department of Computer Science at the Technion, where he now holds the Bernard Elkin Chair in Computer Science. During the years 1985-1987 he was Visiting Research Professor with the Department of Electrical Engineering - Systems at the University of Southern California, Los Angeles. During the summers of 1990 and 1991 he was visiting Bellcore in Morristown, New Jersey. During the years 1994-1996 he was a Visiting Research Fellow in the Computer Science Department at Royal Holloway University of London, Egham, England. He also had several visits to the Coordinated Science Laboratory at University of Illinois in Urbana-Champaign during the years 1995-1998, two visits to HP Bristol during the summers of 1996, 2000, a few visits to the Department of Electrical Engineering, University of California at San Diego during the years 2000-2017, and several visits to the Mathematics Department at Royal Holloway University of London, during the years 2007-2017.

His research interests include applications of discrete mathematics to problems in computer science and information theory, coding theory, network coding, and combinatorial designs.

Dr. Etzion was an Associate Editor for Coding Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY from 2006 till 2009. From 2004 to 2009, he was an Editor for the *Journal of Combinatorial Designs*. From 2011 he is an Editor for Designs, Codes, and Cryptography. and from 2013 an Editor for Advances of Mathematics in Communications.

Antonia Wachter-Zeh (S'10–M'14) is an Assistant Professor at the Technical University of Munich (TUM), Munich Germany. She received an equivalent of the B.S. degree in electrical engineering in 2007 from the University of Applied Science Ravensburg, Germany, and the M.S. degree in communications technology in 2009 from Ulm University, Germany. She obtained her Ph.D. degree in 2013 at the Institute of Communications Engineering, University of Ulm, Germany and at the Institut de recherche mathmatique de Rennes (IRMAR), Universit de Rennes 1, Rennes, France. From 2013 to 2016, she was a postdoctoral researcher at the Technion—Israel Institute of Technology, Haifa, Israel. Her research interests are coding and information theory and their application to storage, communications, and security.