

On Vector Linear Solvability of Multicast Networks

Qifu Tyler Sun, *Member, IEEE*, Xiaolong Yang, *Member, IEEE*, Keping Long, *Senior Member, IEEE*,
Xunrui Yin, and Zongpeng Li, *Senior Member, IEEE*

Abstract—Vector linear network coding (LNC) is a generalization of the conventional scalar LNC, such that the data unit transmitted on every edge is an L -dimensional vector of data symbols over a base field $\text{GF}(q)$. Vector LNC enriches the choices of coding operations at intermediate nodes, and there is a popular conjecture on the benefit of vector LNC over scalar LNC in terms of alphabet size of data units: there exist (single-source) multicast networks that are vector linearly solvable of dimension L over $\text{GF}(q)$ but not scalar linearly solvable over any field of size $q' \leq q^L$. This paper introduces a systematic way to construct such multicast networks, and subsequently establish explicit instances to affirm the positive answer of this conjecture for infinitely many alphabet sizes p^L with respect to an arbitrary prime p . On the other hand, this paper also presents explicit instances with the special property that they do not have a vector linear solution of dimension L over $\text{GF}(2)$ but have scalar linear solutions over $\text{GF}(q')$ for some $q' < 2^L$, where q' can be odd or even. This discovery also unveils that over a given base field, a multicast network that has a vector linear solution of dimension L does not necessarily have a vector linear solution of dimension $L' > L$.

Index Terms—Vector network coding, scalar network coding, multicast networks, alphabet size, direct sum.

I. INTRODUCTION

IN THE conventional theory of linear network coding (LNC) [1], [2], the data unit transmitted along every edge of unit capacity in a network consists of a single data symbol belonging to a base field $\text{GF}(q)$. Every outgoing edge of a node v transmits a data symbol that is a $\text{GF}(q)$ -linear combination of the incoming data symbols to v . Such a coding mechanism is referred to as *scalar LNC*.

A generalization of scalar LNC is *vector LNC* [3] or *block LNC* [4], which models the data unit transmitted along every edge of unit capacity as an L -dimensional vector of data

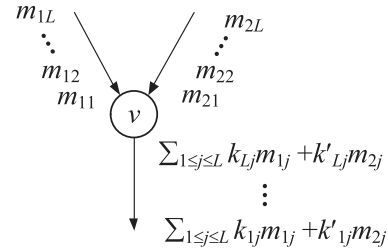


Fig. 1. Consider an intermediate node v with 1 outgoing edge and 2 incoming edges in a network. In vector LNC, v receives two vectors (m_{11}, \dots, m_{1L}) and (m_{21}, \dots, m_{2L}) of L data symbols belonging to a base field $\text{GF}(q)$. The data unit transmitted on the outgoing edge of v is also a vector of L data symbols over $\text{GF}(q)$, in which each data symbol is a $\text{GF}(q)$ -linear combination of all $2L$ incoming data symbols to v .

symbols over a base field $\text{GF}(q)$, and concomitantly defines the coding operations performed at every intermediate node as $\text{GF}(q)$ -linear combinations of all data symbols in incoming data unit vectors, as illustrated in Fig. 1.

The introduction of the concept of vector LNC stems from its potential to enrich the choices of coding operations at intermediate nodes in a network. The potential of vector LNC has been considered from several different aspects (See for example [3]–[13]). In particular, the work in [3] demonstrated a classic multi-source multicast network which has a simple vector linear solution of dimension 2 over $\text{GF}(2)$ but does not have a scalar linear solution over any base field. It was also noted in [3] that the network constructed in [14] which is not scalar linearly solvable over any field has a vector linear solution. There is another exemplifying network proposed in [5] which does not have a scalar linear solution over any field but has a vector linear solution of dimension 3 over $\text{GF}(2)$. These exemplifying networks manifest the superiority of vector LNC over scalar LNC in terms of enabling a linear solution.

Up to now, most studies on vector LNC have been in the context of general (non-multicast) networks. Specific to a (single-source) multicast network, though it is well known that there is a scalar linear solution over a field with size no smaller than the number of receivers [15], there are still benefits to consider vector LNC, as summarized in [11]. In particular, the alphabet size of data units is a key factor that affects the linear solvability of a multicast network. Under the same alphabet size q^L , vector LNC of dimension L over $\text{GF}(q)$ provides much more choices for coding operations than scalar LNC over $\text{GF}(q^L)$, and every scalar linear code over $\text{GF}(q^L)$ can be transformed into a vector linear code of dimension L

Manuscript received November 12, 2015; revised May 9, 2016 and September 13, 2016; accepted September 13, 2016. Date of publication September 23, 2016; date of current version December 15, 2016. This work was partially supported by the China 973 Program under grant 2012CB315905, the National Natural Science Foundation of China under Grant 61271227, Grant 61471034, and Grant 61571335, the Natural Sciences and Engineering Research Council of Canada under Grant RT733206. This work was partially presented at the 2015 IEEE International Conference on Communications and the 2015 IEEE International Symposium on Information Theory. The associate editor coordinating the review of this paper and approving it for publication was B. Liang.

Q. T. Sun, X. Yang, and K. Long are with the School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China (e-mail: qfsun@ustb.edu.cn; yangxl@ustb.edu.cn; longkeping@ustb.edu.cn).

X. Yin and Z. Li are with the Department of Computer Science, University of Calgary, Calgary, AB T2N 1N4, Canada, and also with the Department of Computer, Wuhan University, Wuhan 430072, China (e-mail: yinxunrui@gmail.com; zongpeng@ucalgary.ca).

Digital Object Identifier 10.1109/TCOMM.2016.2613085

over $\text{GF}(q)$, so that the scalar linear code is a solution if and only if its corresponding vector linear code is a solution too. Thus, a network has a scalar linear solution over $\text{GF}(q^L)$ *only if* it has a vector linear solution of dimension L over $\text{GF}(q)$. It would be natural to conceive the following benefit of vector LNC, as conjectured in [11]:

- There exists a multicast network that is vector linearly solvable of dimension L over $\text{GF}(q)$, but not scalar linearly solvable over $\text{GF}(q')$ for any $q' \leq q^L$.

If proven true, this conjecture will imply practical benefit of vector LNC in terms of reducing the alphabet size to yield a solution on a multicast network, which is a fundamental research topic in the network coding literature. Assume the base field is $\text{GF}(q)$. For a multicast network, in the case that there is not a linear solution over $\text{GF}(q)$, we need to extend the alphabet size from q to q^L for some $L > 1$ to guarantee the existence of a linear solution. For both a scalar linear code over $\text{GF}(q^L)$ and a vector linear code over $\text{GF}(q)$ of length L , every edge will transmit a block of L data symbols over $\text{GF}(q)$, and hence its transmission delay is theoretically L times the transmission delay of a scalar code over $\text{GF}(q)$. The correctness of the above conjecture will reveal that vector LNC may help reduce the edge transmission delay compared with vector LNC for some multicast networks. Even though the work in [11] indicated the possible correctness of this conjecture from the perspective of multivariate determinant polynomials of transfer matrices, it failed to provide explicit multicast networks to verify its correctness.

In the first part of the paper, we propose a systematic way to construct a multicast network vector linearly solvable over $\text{GF}(q)$ at dimension L but not scalar linearly solvable over $\text{GF}(q')$ for any $q' \leq q^L$. Explicit multicast networks are also subsequently constructed based on this method so that the aforementioned conjecture is proven to be correct for *infinitely many* alphabet sizes p^L with respect to an *arbitrary* prime p . Moreover, some of the illustrated multicast networks vector linearly solvable at dimension L over $\text{GF}(p)$ do not have a scalar linear solution over $\text{GF}(q')$, not only for all those $q' \leq p^L$, but also for some $q' > p^L$. This affirms that in some multicast networks, vector LNC can indeed be superior to scalar LNC, in a stronger sense than as conjectured, in terms of alphabet size of data units to yield a solution. The vector coding techniques we propose to beat scalar codes have several implications:

- Scalar linear solutions over respective alphabets $\text{GF}(q^{L_1}), \dots, \text{GF}(q^{L_m})$ do not necessarily imply another scalar linear solution over $\text{GF}(q^{L_1+\dots+L_m})$, but they guarantee a vector linear solution of dimension $L_1 + \dots + L_m$ over $\text{GF}(q)$.
- For scalar linear codes over respective alphabets $\text{GF}(q^{L_1}), \dots, \text{GF}(q^{L_m})$, even in the case that none of them has a solution, it is still possible to combine their corresponding vector linear codes, by direct sum, to form a vector linear solution of dimension $L_1 + \dots + L_m$ over $\text{GF}(q)$.

In the second part of the paper, we compare the alphabet size requirements for scalar and vector linear solvability of

multicast networks from another direction. Specifically, now that the non-existence of a vector linear solution of dimension L over $\text{GF}(q)$ implies the non-existence of a scalar linear solution over $\text{GF}(q^L)$, a natural question is whether it can further imply the non-existence of a scalar linear solution over every $\text{GF}(q')$ with $q' \leq q^L$. At a first glance, one might be inclined to believe its correctness. However, as we shall demonstrate, the answer to this question is *negative*. Another contribution of this paper is to show explicit multicast networks, for the first time in the literature, which do not have a vector linear solution of dimension L over $\text{GF}(2)$ but have a scalar linear solution over $\text{GF}(q')$ for some $q' < 2^L$, where q' can be odd or a power of 2. This discovery suggests that it is also possible for scalar LNC to outperform vector LNC (of dimension $L \geq 2$) in multicast networks, in terms of using a smaller alphabet to yield a solution. More importantly, it further discloses that

- over a given base field, a multicast network vector linearly solvable of dimension L is not necessarily vector linearly solvable of dimensions L' with $L' > L$.

This discovery is intriguing in the sense that it appears to contradict the folklore on multicast networks: the larger the alphabet block length, the more likely a linear solution exists.

Recently, a few multicast networks were discovered in [16] with the intriguing property that they are scalar linearly solvable over a small field but not necessarily scalar linearly solvable over a larger field. They share a common topological structure, and can thus be subsumed in a particular class of multicast networks, whose scalar linear solvability is completely characterized in [17]. One of the fundamental building blocks for the results obtained in this paper is the further analysis of the vector linear solvability of this special class of multicast networks, which was not dealt with in [16] and [17].

The remainder of this paper is organized as follows. In Section II, we establish the mathematical notations to be adopted and review some useful fundamental results of vector and scalar LNC. In Section III, we present a general way to construct multicast networks vector linearly solvable over $\text{GF}(q)$ of dimension L but not scalar linearly solvable over $\text{GF}(q')$ for any $q' \leq q^L$, and present instances for an arbitrary prime p and infinitely many alphabet sizes p^L . In Section IV, we verify that on multicast networks smaller alphabets can be better than larger ones for yielding a vector linear solution. Section V summarizes the paper.

II. PRELIMINARIES

A. Mathematical Model for Vector Linear Codes

This work focuses on a single-source multicast network, which is modeled as a finite directed acyclic multigraph, with a unique source node s and a set T of receivers. The source node s generates a data message consisting of ω data units chosen from an algebraic alphabet and multicasts it over the network through ω outgoing edges of s . For a node v in the network, denote by $In(v)$ and $Out(v)$, respectively, the set of its incoming and outgoing edges. Every edge has unit capacity, that is, it transmits one data unit per edge use. A topological

order is assumed on the set of edges led by ones in $Out(s)$. For every receiver $t \in T$, based on the $|In(t)|$ data units received from edges in $In(t)$, its goal is to recover the ω source data units generated from s , where $\omega = |Out(s)|$ will be referred to as the source dimension of the network. The maximum flow for every receiver $t \in T$, which is defined to be the maximum number of edge-disjoint paths leading from s to t , is assumed to be ω .

In the conventional scalar LNC, the data unit transmitted along every edge e merely consists of a single data symbol belonging to an algebraic alphabet modeled as a finite field $GF(q)$. A *scalar linear code* is an assignment of a *local encoding kernel* $k_{d,e} \in GF(q)$ to every pair (d, e) of edges such that $k_{d,e} = 0$ when (d, e) is not an adjacent pair of edges. Every scalar linear code uniquely determines a global encoding kernel \mathbf{f}_e , which is an ω -dimensional column vector over $GF(q)$, for each edge e in the network. Based on the global encoding kernels, the data symbol m_e transmitted along every edge e can be computed by

$$m_e = [m_d]_{d \in Out(s)} \mathbf{f}_e.$$

On a multicast network, a scalar linear code is called a *scalar linear solution* if for every receiver $t \in T$, the juxtaposition $[\mathbf{f}_e]_{e \in In(t)}$ of the global encoding kernels for edges incoming to t has full rank ω . For a scalar linear solution, every receiver $t \in T$ can compute an $|In(t)| \times \omega$ matrix \mathbf{D}_t over $GF(q)$ such that $[\mathbf{f}_e]_{e \in In(t)} \mathbf{D}_t$ forms an $\omega \times \omega$ identity matrix. Based on \mathbf{D}_t , receiver t can successfully recover the ω source data symbols from the $|In(v)|$ received data symbols via

$$[m_e]_{e \in In(v)} \mathbf{D}_t = [m_d]_{d \in Out(s)} \mathbf{f}_e \mathbf{D}_t = [m_d]_{d \in Out(s)}.$$

As a generalization of scalar LNC, vector LNC models the data unit transmitted along every edge e to be an L -dimensional *row vector* \mathbf{m}_e of data symbols over a base field $GF(q)$. Thus, the mathematical model for the data unit alphabet in vector LNC is a vector space $GF(q)^L$ rather than a finite field. Under the new mathematical structure of data units, the model of scalar LNC can be naturally extended to vector LNC as follows.

A *vector linear code of dimension L over $GF(q)$* , or a *vector linear code over $GF(q)^L$* for short, is an assignment of a *local encoding kernel* $\mathbf{K}_{d,e}$, which is an $L \times L$ matrix over $GF(q)$, to every pair (d, e) of edges such that $\mathbf{K}_{d,e}$ is the zero matrix $\mathbf{0}$ when (d, e) is not an adjacent pair. Then, for every edge e outgoing from a non-source node v , the data unit vector of data symbols transmitted on e is

$$\mathbf{m}_e = \sum_{d \in In(v)} \mathbf{m}_d \mathbf{K}_{d,e}$$

Furthermore, every vector linear code uniquely determines a global encoding kernel \mathbf{F}_e , which is an $\omega L \times L$ matrix over $GF(q)$, for every edge e such that

- The columnwise juxtaposition $[\mathbf{F}_e]_{e \in Out(s)}$ of \mathbf{F}_e for $e \in Out(s)$ forms an $\omega L \times \omega L$ identity matrix \mathbf{I} ;
- For every outgoing edge e from a non-source node v , $\mathbf{F}_e = \sum_{d \in In(v)} \mathbf{F}_d \mathbf{K}_{d,e}$.

Correspondingly, the data unit vector transmitted along every edge e can also be represented as

$$\mathbf{m}_e = [\mathbf{m}_d]_{d \in Out(s)} \mathbf{F}_e.$$

A vector linear code over $GF(q)^L$ is called a *vector linear solution* if for every receiver $t \in T$, the juxtaposition $[\mathbf{F}_e]_{e \in In(t)}$ of the global encoding kernels for edges incoming to t has full rank ωL . Correspondingly, there is an $L|In(t)| \times L|Out(s)|$ decoding matrix \mathbf{D}_t over $GF(q)$ for every receiver t such that the source data units can be recovered at t via

$$\begin{aligned} [\mathbf{m}_e]_{e \in In(t)} \mathbf{D}_t &= ([\mathbf{m}_d]_{d \in Out(s)} [\mathbf{F}_e]_{e \in In(t)}) \mathbf{D}_t \\ &= [\mathbf{m}_d]_{d \in Out(s)} ([\mathbf{F}_e]_{e \in In(t)} \mathbf{D}_t) \\ &= [\mathbf{m}_d]_{d \in Out(s)} \mathbf{I} = [\mathbf{m}_d]_{d \in Out(s)}. \end{aligned}$$

A scalar linear code can be regarded as a vector linear code from two different facets. On one hand, it is straightforward to see that every scalar linear code over $GF(q^L)$ is naturally a vector linear code of dimension 1 over $GF(q^L)$. On the other hand, let Φ be a mapping from $GF(q^L)$ into the ring of $L \times L$ matrices over $GF(q)$ via

$$\Phi(0) = \mathbf{0}, \quad \Phi(\gamma^k) = \mathbf{C}_p^k, \quad 0 \leq k \leq q^L - 2, \quad (1)$$

where \mathbf{C}_p is the $L \times L$ companion matrix of a primitive polynomial $p(x)$ of degree L over $GF(q)$, and γ is a fixed root of $p(x)$, that is, a primitive element of $GF(q^L)$. As a consequence of the Cayley-Hamilton theorem, this mapping is a homomorphism, and $\{\mathbf{0}, \mathbf{C}_p^0, \dots, \mathbf{C}_p^{q^L-2}\}$ forms a matrix representation of the finite field $GF(q^L)$ (See, for example, [18]). Then, every scalar linear code over $GF(q^L)$ with local encoding kernels $(k_{d,e})$ corresponds to a vector linear code over $GF(q)^L$ with local encoding kernels prescribed as

$$\mathbf{K}_{d,e} = \Phi(k_{d,e}), \quad (2)$$

and moreover, based on the homomorphic property of Φ , we can derive the following result.

Proposition 1: Given a (not necessarily multicast) network, a scalar linear code over $GF(q^L)$ with local encoding kernels $(k_{d,e})$ is a solution if and only if the corresponding vector linear code over $GF(q)^L$ with local encoding kernels $\mathbf{K}_{d,e} = \Phi(k_{d,e})$ qualifies as a solution too. Moreover, if \mathbf{D}_t is a decoding matrix of the scalar linear solution for receiver t , then $\Phi(\mathbf{D}_t)$ is also a decoding matrix of the corresponding vector linear solution for t , where Φ is applied componentwise for the entries in \mathbf{D}_t .

In summary, Table I compares the mathematical structures of scalar and vector LNC.

B. A Special Class of Multicast Networks

Recently, the first few known multicast networks that are scalar linearly solvable over $GF(q)$ but not necessarily over a larger $GF(q')$ were discovered in [16]. They share a similar topology and can be generalized into a class of multicast networks $\mathcal{N}_{\omega, \mathbf{d}}$, as replotted in Fig. 2, with topological parameters ω and $\mathbf{d} = (d_1, d_2, \dots, d_\omega)$. The network $\mathcal{N}_{\omega, \mathbf{d}}$ has source dimension ω , and consists of nodes on five layers. The source s

TABLE I

COMPARISON OF SCALAR AND VECTOR LNC WHEN THE ALPHABET SIZE OF DATA UNITS IS FIXED TO q^L WITH q EQUAL TO A PRIME POWER

	Scalar LNC	Vector LNC
Data unit alphabet	Base field $\text{GF}(q^L)$	Vector space $\text{GF}(q)^L$
Local encoding kernel	Element in $\text{GF}(q^L)$	$L \times L$ matrix over $\text{GF}(q)$
# of candidates for local encoding kernels (for adjacent pairs of edges)	q^L	q^{L^2}

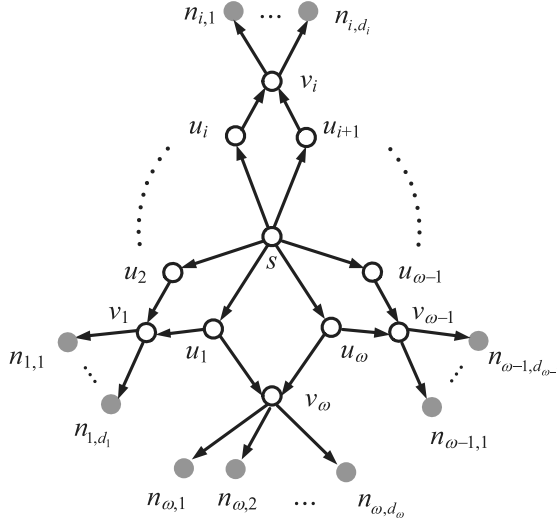


Fig. 2. The network $\mathcal{N}_{\omega, \mathbf{d}}$ consists of nodes on 5 layers. Layer-1 consists of the source node s only, and layer-4 nodes are depicted in grey. There is a non-depicted bottom-layer node connected from every set N of ω layer-4 nodes with $\maxflow(N) = \omega$. All bottom-layer nodes are receivers.

is the unique node in the first layer. There are ω layer-2 nodes u_j , $1 \leq j \leq \omega$, each of which is connected from s by an edge. There are ω layer-3 nodes v_j , $1 \leq j \leq \omega$, each of which is connected from two upstream layer-2 nodes u_j and u_{j+1} ($u_{\omega+1}$ represents u_1) by a respective edge. For each layer-3 node v_j , there are $d_j > 1$ outgoing edges, each of which leads to a different downstream layer-4 (grey) node. Thus, the ω -tuple $\mathbf{d} = (d_1, \dots, d_{\omega})$ controls the number of layer-4 nodes. There is a non-depicted bottom-layer node connected from every set N of ω layer-4 nodes with $\maxflow(N) = \omega$, that is, with ω edge-disjoint paths starting from s and ending at nodes in N . All bottom-layer nodes are receivers.

The following is a concise formula for the scalar linear solvability of $\mathcal{N}_{\omega, \mathbf{d}}$ derived in [17].

Theorem 2: Consider a network $\mathcal{N}_{\omega, \mathbf{d}}$ with parameters ω and $\mathbf{d} = (d_1, d_2, \dots, d_{\omega})$. It is linearly solvable over $\text{GF}(q)$ if and only if there is positive divisor d of $q - 1$ subject to

$$q \geq d \left(\left\lceil \frac{d_1}{d} \right\rceil + \dots + \left\lceil \frac{d_{\omega}}{d} \right\rceil - \omega + 1 \right) + 2 \quad (3)$$

Corollary 3: The network $\mathcal{N}_{\omega, \mathbf{d}}$ with parameters ω and $\mathbf{d} = (2, 2, \dots, 2)$ is called the *Swirl Network* [16]. As a consequence of Theorem 2, it is scalar linearly solvable over $\text{GF}(q)$ if and only if $q > \omega + 2$ or $q - 1$ is not a prime.

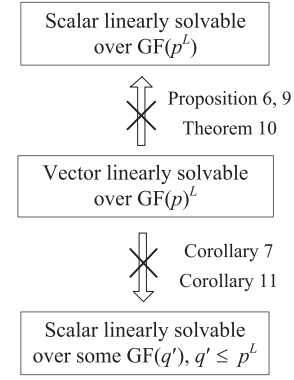


Fig. 3. The main results to be established in Section III. Herein p is an arbitrary prime.

The analysis of the vector linear solvability of $\mathcal{N}_{\omega, \mathbf{d}}$ will be one of the building blocks for the main discoveries of this paper.

III. MULTICAST NETWORKS WITH VECTOR LNC SUPERIOR TO SCALAR LNC

In this section, we shall first introduce a general method to construct multicast networks vector linearly solvable over $\text{GF}(q)^L$ but not scalar linearly solvable over any $\text{GF}(q')$ with $q' \leq q^L$. Then, we make use of this method to design infinitely many instances to verify that vector LNC can indeed outperform scalar LNC for multicast networks in terms of the required alphabet size to yield a solution. The main results to be established in this section are outlined in Fig. 3.

A. A General Construction Method

Under the same alphabet size of data units, which is considered to be a prime power throughout the paper, the number of candidates to which the local encoding kernels can be assigned increases *exponentially* from q^L to q^{L^2} . Consequently, it is natural to conceive that vector LNC outperforms scalar LNC on a multicast network in the sense that the minimum alphabet size to yield a vector linear solution might be smaller than the minimum required in a scalar solution. However, to the best of our knowledge, no explicit demonstration of this advantage for vector LNC on multicast networks has ever been given, and this advantage was only partially confirmed in [11]. In the work of [11], an algebraic framework is established to characterize the vector linear solvability of a multicast network, which can be regarded as a generalization of the classic algebraic framework in [2] that concentrates on scalar linear solvability. Specifically, the framework associates every receiver in a multicast network with a transfer matrix whose entries are multivariate polynomials. Correspondingly, it associates a multicast network with a multivariate polynomial obtained by the product of the determinants of all transfer matrices. It is then shown that a multicast network is vector linearly solvable over $\text{GF}(q)^L$ if and only if there is an assignment of $L \times L$ matrices over $\text{GF}(q)$ to the variables in the associated polynomial under which the evaluation of this polynomial is an invertible matrix over $\text{GF}(q)$. Meanwhile,

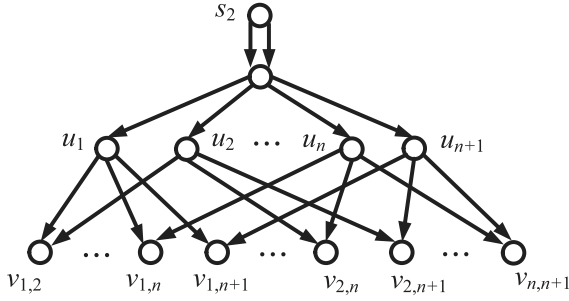


Fig. 4. An $(n+1, 2)$ -combination network \mathcal{N}_2 . It is well known to be scalar linearly solvable over $\text{GF}(q^L)$ if and only if $q^L \geq n$. It can also be shown to be vector linearly solvable over $\text{GF}(q^L)$ if and only if $q^L \geq n$.

a multivariate polynomial was discovered in [11] which does not have such an assignment over $\text{GF}(q)$ for any $q \leq 2^{10}$, but has a feasible assignment over $\text{GF}(2)^{10}$. However, that work did not show the existence of a multicast network that can be associated with this particular polynomial, and hence whether there exists a multicast network with the desired advantage of vector LNC remains elusive.

We next propose a general construction method, based on which the design of a multicast network vector linearly solvable over $\text{GF}(q)^L$ but not scalar linearly solvable over $\text{GF}(q')$ for every $q' \leq q^L$ reduces to the design of a multicast network vector linearly solvable over $\text{GF}(q)^L$ but not scalar linearly solvable over $\text{GF}(q^L)$.

Construction 1: Let \mathcal{N}_1 be a multicast network with source dimension ω that is vector linearly solvable over $\text{GF}(q)^L$ but not scalar linearly solvable over $\text{GF}(q^L)$. Set $n = q^L$. Construct a multicast network \mathcal{N} of source dimension ω as follows:

- Create the unique source node s' and another node s , as well as ω edges starting from s' and ending at s .
- Add \mathcal{N}_1 as a subnetwork of \mathcal{N} . Create ω edges from s to the original source node s_1 of \mathcal{N}_1 .
- Add an $(n+1, 2)$ -combination network \mathcal{N}_2 (See, e.g., [19] [20]), as depicted in Fig. 4, to be another subnetwork of \mathcal{N} . Create 2 edges from s to the original source node s_2 of \mathcal{N}_2 .
- For every original receiver t of \mathcal{N}_2 , create $\omega - 2$ edges from s to t .

In this way, every node that is originally a receiver in \mathcal{N}_1 or \mathcal{N}_2 is also a receiver in \mathcal{N} .

Theorem 4: Let \mathcal{N}_1 be a multicast network that is vector linearly solvable over $\text{GF}(q)^L$ but not scalar linearly solvable over $\text{GF}(q^L)$. The network \mathcal{N} constructed by Construction 1 with $n = q^L$ has a vector linear solution over $\text{GF}(q)^L$. However, it is not scalar linearly solvable over $\text{GF}(q')$ for any $q' \leq q^L$, and not vector linearly solvable over $\text{GF}(q')^{L'}$ for any $q'^{L'} < q^L$.

Proof: The network \mathcal{N} is vector linearly solvable over $\text{GF}(q')^{L'}$ or scalar linearly solvable over $\text{GF}(q')$ if and only if so are the subnetworks \mathcal{N}_1 and \mathcal{N}_2 .

It is well known that the $(n+1, 2)$ -combination network is scalar linearly solvable over $\text{GF}(q')$ if and only if $q' \geq n$. In a similar argument to characterize its scalar linear solvability, one can deduce that an $(n+1, 2)$ -combination network is

vector linear solvable over $\text{GF}(q')^{L'}$ if and only if there are $L' \times L'$ invertible matrices $\mathbf{A}_1, \dots, \mathbf{A}_{n-1}$ over $\text{GF}(q')$ such that

$$\text{rank}(\mathbf{A}_i - \mathbf{A}_j) = L', \quad \forall 1 \leq i < j \leq n-1, \quad (4)$$

Thus, $\{\mathbf{A}_1, \dots, \mathbf{A}_{n-1}\}$, together with $\mathbf{0}$ form an L' -dimensional rank-metric code of distance L' over $\text{GF}(q')$. According to the Singleton bound for the rank-metric codes (See [21] for example), there are at most $q'^{L'(L'-L'+1)} = q'^{L'}$ codewords for such a rank-metric code. Thus, if there are $L' \times L'$ invertible matrices $\mathbf{A}_1, \dots, \mathbf{A}_{n-1}$ over $\text{GF}(q')$ subject to (4), then $n-1 \leq q'^{L'} - 1$, i.e. $q'^{L'} \geq n$. On the other hand, when $q'^{L'} \geq n$, a scalar linear solution can be constructed for the $(n+1, 2)$ -combination network over $\text{GF}(q')^{L'}$, which in turn induces a vector linear solution over $\text{GF}(q')^{L'}$ according to Proposition 1. We can now conclude that an $(n+1, 2)$ -combination network is vector linearly solvable over $\text{GF}(q')^{L'}$ if and only if $q'^{L'} \geq n$.

In consequence, the subnetwork \mathcal{N}_2 of \mathcal{N} has a vector linear solution over $\text{GF}(q)^L$, but neither a scalar nor a vector linear solution when the alphabet size of data units is smaller than q^L . On the other hand, the subnetwork \mathcal{N}_1 of \mathcal{N} is vector linearly solvable over $\text{GF}(q)^L$ but not scalar linearly solvable over $\text{GF}(q^L)$. We can see when the alphabet size is no greater than q^L , the network \mathcal{N} does not have any scalar linear solution, and has a vector linear solution only over $\text{GF}(q)^L$. \square

B. The First Explicit Network Construction

In order to apply Construction 1 to construct a multicast network vector linearly solvable over $\text{GF}(q)^L$ but not scalar linearly solvable over $\text{GF}(q')$ for any $q' \leq q^L$, a key step that has not been explicated is to provide a multicast network that is vector linearly solvable over $\text{GF}(q)^L$ but not scalar linearly solvable over $\text{GF}(q^L)$. We next show that the Swirl Network with appropriate source dimension ω is actually the first known one with such a property.

Assume that the alphabet size of data units is 2^L . When $2^L - 1$ is a prime, the Swirl Network with dimension $\omega \geq 2^L - 2$ does not have a scalar linear solution over $\text{GF}(2^L)$. Recall that a prime in the form of $2^L - 1$ is called a Mersenne prime. After examining the list of all known 49 Mersenne primes in the ascending order [22], we found that the 5th one, $2^{13} - 1$, can be written as $2^4 \cdot 2^9 - 1$ but neither $2^4 - 1$ nor $2^9 - 1$ is a Mersenne prime. Thus, the Swirl Network turns out to be the first exemplifying multicast network scalar linearly solvable over both $\text{GF}(q^{L_1})$ and $\text{GF}(q^{L_2})$ but not over $\text{GF}(q^{L_1+L_2})$. This has been noticed in [16].

Now consider a (possibly non-multicast) network and a scalar linear solution of it, with local encoding kernels denoted by $(k_{d,e,j})$, over $\text{GF}(q^{L_j})$ for all $1 \leq j \leq m$. We can define a vector linear code of dimension $L := L_1 + L_2 + \dots + L_m$ over $\text{GF}(q)$ with local encoding kernels prescribed by

$$\mathbf{K}_{d,e} = \begin{bmatrix} \Phi(k_{d,e,1}) & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \Phi(k_{d,e,2}) & \dots & \dots \\ \dots & \dots & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \Phi(k_{d,e,m}) \end{bmatrix}, \quad (5)$$

where Φ is the homomorphism from $\text{GF}(q^L)$ into the ring of $L \times L$ matrix over $\text{GF}(q)$ defined in (1). In the same way as to prove Proposition 1, one can prove that this vector code over $\text{GF}(q)^L$ qualifies as a solution too. We thus obtained the following.

Proposition 5: If a (possibly non-multicast) network is scalar linearly solvable over $\text{GF}(q^{L_j})$ for all $1 \leq j \leq m$, then it is not necessarily scalar linearly solvable over $\text{GF}(q^L)$, but must be vector linearly solvable over $\text{GF}(q)^L$, where $L = L_1 + L_2 + \dots + L_m$.

As a consequence of the above analysis, the Swirl Network with source dimension $\omega \geq 2^{13} - 2$ has a vector linear solution over $\text{GF}(2)^{13}$ but no scalar linear solution over $\text{GF}(2^{13})$. This satisfies our desired property. Next result can be further obtained.

Proposition 6: Let $2^L - 1$ be an arbitrary Mersenne prime no smaller than $2^{13} - 1$. The Swirl Network with source dimension $\omega \geq 2^L - 2$ is vector linearly solvable over $\text{GF}(q')^{L'}$ for every $q'^{L'} \geq 2^L$, but not scalar linearly solvable over $\text{GF}(q')$ for any q' with $2^L \leq q' \leq \omega + 2$ and $q' - 1$ being a prime.

Proof: Corollary 3 characterizes the scalar linear solvability of the considered Swirl network. It remains to show its vector linear solvability. Assume q' is odd. The Swirl Network is scalar linearly solvable over $\text{GF}(q'^{L'})$ for every $L' \geq 1$, and hence vector linearly solvable over $\text{GF}(q')^{L'}$ by Proposition 1. Assume $q' = 2$. The case $L' = 13$ has been discussed in the analysis prior to the present proposition. Consider the case $L' > 13$. Since $2^L - 1$ a Mersenne prime, L is an (odd) prime too. Thus, $L' - 13$ is even and hence $2^{L'-13} - 1$ must be a composite. Consequently, the considered Swirl Network is scalar linearly solvable over $\text{GF}(2^4)$, $\text{GF}(2^9)$ and $\text{GF}(2^{L'-13})$ respectively. Consequently, it is vector linearly solvable over $\text{GF}(2)^{L'}$ according to Proposition 5. \square

Corollary 7: Let $2^L - 1$ be a Mersenne prime no smaller than $2^{13} - 1$, and \mathcal{N}_l represent the Swirl Network with source dimension $\omega \geq 2^L - 2$. The multicast network \mathcal{N} constructed by Construction 1 with $n = 2^L$ has a vector linear solution over $\text{GF}(2)^L$, but does not have a scalar linear solution over $\text{GF}(q')$ for any $q' \leq 2^L$. Moreover, it is vector linearly solvable over $\text{GF}(q')^{L'}$ for every $q'^{L'}$ larger than 2^L , but not scalar linearly solvable over $\text{GF}(q')$ for any q' with $2^L \leq q' \leq \omega + 2$ and $q' - 1$ being a prime.

Proof: It follows from Theorem 4 together with Proposition 6. \square

We have now affirmed the correctness of the conjecture raised in [11] by explicit examples that vector linear coding can indeed be superior to scalar one in terms of the required alphabet size in a linear network coding solution. Furthermore, these first exemplifying networks suggest that there are cases where vector linear coding are superior to scalar linear coding in a stronger sense than as conjectured in [11]:

- It is possible for a multicast network vector linearly solvable over $\text{GF}(q')^{L'}$ for every prime power $q'^{L'} \geq q^L$, but not scalar linearly solvable not only over any $\text{GF}(q')$ with $q' \leq q^L$, but also over some $\text{GF}(q')$ with $q' > q^L$, which can be extremely large compared with q^L .

C. Construction of Infinitely Many Network Instances

In the previous subsection, the key to proving the Swirl Network to be vector linearly solvable over $\text{GF}(2)^L$ but not scalar linearly solvable over $\text{GF}(2^L)$ is the observation that scalar linear solutions over respective alphabets $\text{GF}(q^{L_1}), \dots, \text{GF}(q^{L_m})$ do not necessarily imply another scalar linear solution over $\text{GF}(q^{L_1+\dots+L_m})$, but they guarantee a vector linear solution over $\text{GF}(q)^{L_1+\dots+L_m}$. At this moment, it only brings us a few alphabet sizes 2^L with the property that there is a multicast network vector linearly solvable over $\text{GF}(2)^L$ but not scalar linearly solvable over $\text{GF}(2^L)$. In this subsection, we shall identify *infinitely many* alphabet sizes with this property. Towards this goal, we first characterize the vector linear solvability of the network $\mathcal{N}_{\omega, \mathbf{d}}$ described in Section II.B.

Lemma 8: The network $\mathcal{N}_{\omega, \mathbf{d}}$ with parameters ω and $\mathbf{d} = (d_1, \dots, d_\omega)$ has a vector linear solution over $\text{GF}(q)^L$ if and only if there exist invertible matrices $\mathbf{A}_{11}, \dots, \mathbf{A}_{1d_1}, \dots, \mathbf{A}_{\omega 1}, \dots, \mathbf{A}_{\omega d_\omega}$ of size $L \times L$ over $\text{GF}(q)$ such that

$$\text{rank}(\mathbf{A}_{jk_1} - \mathbf{A}_{jk_2}) = L \quad \forall 1 \leq j \leq \omega, 1 \leq k_1 < k_2 \leq d_j, \quad (6)$$

$$\text{rank}(\mathbf{I} + (-1)^{\omega-1} \mathbf{M}_\omega \mathbf{M}_{\omega-1} \dots \mathbf{M}_1) = L$$

$$\forall \mathbf{M}_j \in \{\mathbf{A}_{j1}, \dots, \mathbf{A}_{jd_j}\}, 1 \leq j \leq \omega. \quad (7)$$

The technical proof of this lemma is provided in Appendix A. It is worthwhile to note that when $L = 1$, the lemma degenerates to a scalar linear solvability characterization of $\mathcal{N}_{\omega, \mathbf{d}}$, which coincides with the one derived in [17] as a preliminary to further obtain Theorem 2.

Proposition 9: Let l be an arbitrary integer larger than 2. Set $\omega \geq 484$ and $\mathbf{d} = \left(\left\lceil \frac{2^{6l+1}-1}{22} \right\rceil, \left\lceil \frac{2^{6l+1}-1}{22} \right\rceil, \dots, \left\lceil \frac{2^{6l+1}-1}{22} \right\rceil\right)$. Then, $\mathcal{N}_{\omega, \mathbf{d}}$ is vector linearly solvable over $\text{GF}(2)^{6l+1}$ but not scalar linearly solvable over $\text{GF}(2^{6l+1})$.

Proof: We first show that the network $\mathcal{N}_{\omega, \mathbf{d}}$ is not scalar linearly solvable over $\text{GF}(2^{6l+1})$. Observe that the smallest n for $2^n \equiv 1 \pmod p$ for $p = 3, 5, 7, 11, 13, 17, 19$ is, respectively, 2, 4, 3, 10, 12, 8, 18. Thus, it can be seen that the smallest positive integer that possibly divides $2^{6l+1} - 1$ is 23, and for every proper divisor d of $2^{6l+1} - 1$, $d \leq \frac{2^{6l+1}-1}{23} < \frac{2^{6l+1}-1}{22}$. Consequently,

$$\begin{aligned} & d \left(\underbrace{\left\lceil \frac{2^{6l+1}-1}{22} \right\rceil + \dots + \left\lceil \frac{2^{6l+1}-1}{22} \right\rceil}_{\omega} - \omega + 1 \right) + 2 \\ & \geq d \left(\underbrace{\left\lceil \frac{2^{6l+1}-1}{22d} \right\rceil + \dots + \left\lceil \frac{2^{6l+1}-1}{22d} \right\rceil}_{\omega} - \omega + 1 \right) + 2 \\ & > \omega \left(\frac{2^{6l+1}-1}{22} - d \right) + d + 2 \\ & \geq 484 \frac{2^{6l+1}-1}{22} - 483 \frac{2^{6l+1}-1}{23} + 2 = 2^{6l+1} + 1, \end{aligned}$$

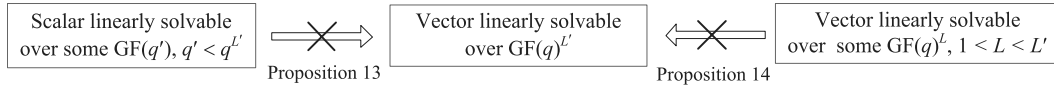


Fig. 5. The main results to be established in Section IV.

and hence condition (3) does not hold. Theorem 2 then affirms that $\mathcal{N}_{\omega, \mathbf{d}}$ is not scalar linearly solvable over $\text{GF}(2^{6l+1})$.

We next establish a vector linear solution for $\mathcal{N}_{\omega, \mathbf{d}}$ over $\text{GF}(2)^{6l+1}$. Write $d = \left\lceil \frac{2^{6l+1}-1}{22} \right\rceil$, $L = 6l + 1$, $L_1 = 9$ and $L_2 = 6l - 8$. Let \mathbf{G}_1 be the $L_1 \times L_1$ invertible matrix over $\text{GF}(2)$ representing a primitive element in $\text{GF}(2^{L_1})$, and \mathbf{G}_2 be the $L_2 \times L_2$ invertible matrix over $\text{GF}(2)$ representing a primitive element in $\text{GF}(2^{L_2})$ according to the homomorphism presented in (1) in Section II.A. Then, $\text{rank}(\mathbf{G}_1^{j_1} - \mathbf{G}_1^{j_2}) = L_1$ for all $1 \leq j_1 < j_2 \leq 2^{L_1} - 1$, and $\text{rank}(\mathbf{G}_2^{j_1} - \mathbf{G}_2^{j_2}) = L_2$ for all $1 \leq j_1 < j_2 \leq 2^{L_2} - 1$.

Write $m_1 = \frac{2^{L_1}-1}{7}$ and $m_2 = \frac{2^{L_2}-1}{3}$. Note that both m_1 and m_2 are integers. For $1 \leq j \leq m_1$, $1 \leq k \leq m_2$, define \mathbf{B}_{jk} to be the $L \times L$ matrix over $\text{GF}(2)$ as $\mathbf{B}_{jk} = \begin{bmatrix} \mathbf{G}_1^{7j} & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2^{3k} \end{bmatrix}$. Thus, $\text{rank}(\mathbf{B}_{j_1 k_1} - \mathbf{B}_{j_2 k_2}) = \text{rank}(\mathbf{G}_1^{7j_1} - \mathbf{G}_1^{7j_2}) + \text{rank}(\mathbf{G}_2^{3k_1} - \mathbf{G}_2^{3k_2}) = L$ for all $1 \leq j_1 < j_2 \leq m_1$, $1 \leq k_1 < k_2 \leq m_2$. Since

$$\begin{aligned} m_1 m_2 - d &= \frac{2^9 - 1}{7} \frac{2^{6l-8} - 1}{3} - \left\lceil \frac{2^{6l+1} - 1}{22} \right\rceil \\ &> \frac{2^{6l+1}}{21 \cdot 22} - \frac{2^9 + 2^{6l-8} - 1}{21} - 1 > 0, \end{aligned}$$

where the last inequality holds as l is assumed larger than 2, we can set $\mathbf{A}_{n1}, \dots, \mathbf{A}_{nd}$ to be arbitrary d distinct matrices in $\{\mathbf{B}_{jk} : 1 \leq j \leq m_1, 1 \leq k \leq m_2\}$ for $1 \leq n \leq \omega - 1$, and set $\mathbf{A}_{\omega 1} = \mathbf{A}_0 \mathbf{A}_{11}, \mathbf{A}_{\omega 2} = \mathbf{A}_0 \mathbf{A}_{12}, \dots, \mathbf{A}_{\omega d} = \mathbf{A}_0 \mathbf{A}_{1d}$, where $\mathbf{A}_0 = \begin{bmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2 \end{bmatrix}$. In this way, $\text{rank}(\mathbf{A}_{j k_1} - \mathbf{A}_{j k_2}) = L$ for all $1 \leq j \leq \omega$ and $1 \leq k_1 < k_2 \leq d$, and

$$\begin{aligned} \mathbf{I} &\notin \{\mathbf{A}_0 \mathbf{B}_{\omega} \cdots \mathbf{B}_2 \mathbf{B}_1 : \mathbf{B}_n \in \{\mathbf{B}_{jk}, 1 \leq j \leq m_1, 1 \leq k \leq m_2\}\} \\ &\supset \{\mathbf{M}_{\omega} \mathbf{M}_{\omega-1} \cdots \mathbf{M}_1 : \mathbf{M}_j \in \{\mathbf{A}_{j1}, \dots, \mathbf{A}_{jd}\}, 1 \leq j \leq \omega\}. \end{aligned}$$

This means that the designed \mathbf{A}_{jk} , where $1 \leq j \leq \omega$ and $1 \leq k \leq d$, satisfy (6) and (7), so $\mathcal{N}_{\omega, \mathbf{d}}$ is vector linearly solvable over $\text{GF}(2)^L$ according to Lemma 8. \square

In the proof of $\mathcal{N}_{\omega, \mathbf{d}}$ to be vector linearly solvable over $\text{GF}(2)^{6l+1}$ in Theorem 9, we essentially constructed a scalar linear code over $\text{GF}(2^9)$ and another scalar linear code $\text{GF}(2^{6l-8})$, none of which qualifies as a solution according to Theorem 2. Then, we combine their corresponding vector linear codes by direct sum and form a vector linear solution. This provides a new approach to design vector linear codes which scalar codes cannot substitute. By a similar but more elaborate argument, we are able to obtain the following generalization.

Theorem 10: Let p be an arbitrary prime. There exists a positive integer m such that for every p^{ml+1} , $l \geq 1$, an instance $\mathcal{N}_{\omega, \mathbf{d}}$ can be found to be vector linearly solvable over $\text{GF}(p)^{ml+1}$ but not scalar linearly solvable over $\text{GF}(p^{ml+1})$.

Proof: Please refer to Appendix B. \square

If we let \mathcal{N}_l represent the network $\mathcal{N}_{\omega, \mathbf{d}}$ established in Theorem 10, then the multicast network \mathcal{N} constructed by Construction 1 with $n = p^{ml+1}$ has a vector linear solution over $\text{GF}(p)^{ml+1}$, but does not have a scalar linear solution over $\text{GF}(q')$ for any $q' \leq p^{ml+1}$. The conjectured benefit of vector linear codes raised in [11] is thus proven in the following more general sense.

Corollary 11: For every prime p , there are infinitely many alphabet sizes p^L each of which corresponds to a multicast network vector linearly solvable over $\text{GF}(p)^L$ but not scalar linearly solvable over any $\text{GF}(q')$ with $q' \leq p^L$.

IV. VECTOR LNC WITH SMALLER ALPHABETS BETTER THAN LARGER ONES

In this section, we shall investigate the vector linear solvability of multicast networks from another direction, in which the main results to be established are outlined in Fig. 5. According to Proposition 1, we have known that if a multicast network is not vector linearly solvable over $\text{GF}(q)^L$, then it is not scalar linearly solvable over $\text{GF}(q^L)$ either. A natural subsequent question is: when a multicast network is not vector linearly solvable over $\text{GF}(q)^L$, is it scalar linearly unsolvable over $\text{GF}(q')$ for any $q' \leq q^L$? It is tempting to think of a ‘yes’ answer, since vector LNC offers a much larger set for local encoding kernel choices. However, we next prove the *negative* answer to this question, through further study of the Swirl Network.

Consider the Swirl Network $\mathcal{N}_{\omega, \mathbf{d}}$ with $\omega \geq 6$ and $\mathbf{d} = (2, \dots, 2)$ again. As a consequence of Corollary 3, it is scalar linearly solvable over both $\text{GF}(5)$ and $\text{GF}(7)$, no matter how large ω is selected. We shall next investigate its vector linear solvability.

Our first goal is to check whether the Swirl Network has a vector linear solution over $\text{GF}(2)^3$ when $\omega = 6$. Based on Lemma 8, a straightforward way to do so is to exhaustively enumerate all invertible 3×3 matrices over $\text{GF}(2)$ for $\mathbf{A}_{11}, \mathbf{A}_{12}, \dots, \mathbf{A}_{61}, \mathbf{A}_{62}$ to see whether conditions (6) and (7) hold. However, because there are total $(2^3 - 2^0)(2^3 - 2^1)(2^3 - 2^2) = 168$ invertible 3×3 matrices over $\text{GF}(2)$, the raw exhaustive enumeration will involve 168^{12} combinations, and such computational complexity is too high to realize. In order to reduce the computational complexity in exhaustive enumeration, we are able to further refine the equivalent conditions in Lemma 8 for the Swirl Network as follows. Similar refinement can also be conducted for a general $\mathcal{N}_{\omega, \mathbf{d}}$ but we shall not address it in this paper.

Lemma 12: The Swirl Network has a vector linear solution over $\text{GF}(q)^L$ if and only if there exist invertible matrices $\mathbf{B}_1, \dots, \mathbf{B}_{\omega}, \mathbf{B}_{\omega+1}$ of size $L \times L$ over $\text{GF}(q)$ such that

$$\text{rank}(\mathbf{I} - \mathbf{B}_j) = L \quad \forall 1 \leq j \leq \omega, \quad (8)$$

$$\begin{aligned} \text{rank}(\mathbf{B}_{\omega+1} + \mathbf{M}_{\omega} \mathbf{M}_{\omega-1} \cdots \mathbf{M}_1) &= L \\ \forall \mathbf{M}_j &\in \{\mathbf{I}, \mathbf{B}_j\}, 1 \leq j \leq \omega. \end{aligned} \quad (9)$$

Proof: Please refer to Appendix C. \square

Consider the case that $q = 2$ and $L = 3$. There are total 48 invertible matrices \mathbf{B} over $\text{GF}(2)$ of size 3×3 satisfying $\text{rank}(\mathbf{I} - \mathbf{B}) = 3$ by computer search. Thus, the number of combinations to search for invertible matrices $\mathbf{B}_1, \dots, \mathbf{B}_7$ subject to (8) and (9), when ω is set to 6, is 48^7 , which becomes more manipulable. By a divide-and-conquer method on ω , we first find that there are 2304 sets of invertible matrices $\mathbf{B}_1, \dots, \mathbf{B}_4$ subject to (8) and (9) when ω is set to 3. Based on this finding, further exhaustive enumeration verifies that no invertible matrices $\mathbf{B}_1, \dots, \mathbf{B}_7$ can be found to make (8) and (9) hold. It can also be readily verified that there are not invertible matrices $\mathbf{B}_1, \dots, \mathbf{B}_7$ over $\text{GF}(2)$ of size 2×2 to make conditions (8) and (9) hold, so the Swirl Network is not vector linearly solvable over $\text{GF}(2)^2$ either. In addition, the Swirl Network is not scalar (and thus not vector) linearly solvable over $\text{GF}(2)$. Since the Swirl Network with $\omega > 6$ has a vector linear solution over $\text{GF}(q)^L$ only if so is the Swirl Network with $\omega = 6$, we conclude the following.

Proposition 13: For $\omega \geq 6$, the Swirl Network is scalar linearly solvable over $\text{GF}(5)$ and $\text{GF}(7)$, but does not have a vector linear solution over $\text{GF}(2)^L$ for any $L \leq 3$.

The Swirl Network affirms that even though the choice of local encoding kernels in scalar LNC is more restricted than in vector LNC, scalar LNC can still outperform vector LNC (of dimension larger than 1) in terms of enabling a linear solution using a smaller alphabet. Since every scalar solution can be regarded as a vector solution of dimension 1, this finding suggests that the alphabet size for vector LNC is not always the larger the better for yielding a solution on a multicast network.

Next, we present a more surprising result that over the same base field, a higher dimension of vector LNC is *not* always more likely to enable a linear multicast solution.

Proposition 14: The Swirl Network, which has a scalar linear solution over $\text{GF}(2^4)$ and thus a vector linear solution over $\text{GF}(2)^4$, is *not* vector linearly solvable over $\text{GF}(2)^5$ when source dimension ω is large enough.

Proof: According to Corollary 3 and Proposition 1, it is straightforward to see that the Swirl Network is scalar linearly solvable over $\text{GF}(2^4)$ and then vector linearly solvable over $\text{GF}(2)^4$. In order to show that the Swirl Network is not vector linearly solvable over $\text{GF}(2)^5$, by Lemma 12, it is equivalent to show the non-existence of invertible matrices $\mathbf{B}_1, \dots, \mathbf{B}_{\omega+1}$ of size 5×5 over $\text{GF}(2)$ to make conditions (8) and (9) hold. However, as ω is large and there are $(2^5 - 1)(2^5 - 2) \dots (2^5 - 2^4) = 9999360$ invertible matrices of size 5×5 over $\text{GF}(2)$, which form the general linear group $GL_5(2)$, it is hard to directly check this by exhaustive enumeration. By analyzing the group structure of $GL_5(2)$, which is provided in [23], we shall first greatly reduce the cases to the degree that exhaustively enumeration is manipulable.

Assume that there is a vector linear solution for the Swirl Network over $\text{GF}(2)^5$, and let $\mathbf{B}_1, \dots, \mathbf{B}_{\omega+1}$ be 5×5 matrices over $\text{GF}(2)$ satisfying conditions (8) and (9).

Recall that the conjugacy class of an element a in a group G refers to the set $\{gag^{-1} : g \in G\}$. The elements in a group can be partitioned into conjugacy classes and elements in the same conjugacy class have the same order. Since $\text{rank}(\mathbf{I} - \mathbf{ABA}^{-1}) = \text{rank}(\mathbf{A}(\mathbf{I} - \mathbf{B})\mathbf{A}^{-1})$ for every $\mathbf{A} \in GL_5(2)$, $\text{rank}(\mathbf{I} - \mathbf{B}) = 5$ for a matrix $\mathbf{B} \in GL_5(2)$ if and only if $\text{rank}(\mathbf{I} - \mathbf{B}') = L$ for every matrix \mathbf{B}' in the conjugacy class of \mathbf{B} in $GL_5(2)$. After examining the representative of every conjugacy class in $GL_5(2)$, as listed in [23], we found that there are only 8 conjugacy classes in $GL_5(2)$ in which the matrices \mathbf{B} satisfy $\text{rank}(\mathbf{I} - \mathbf{B}) = 5$. Two of the 8 conjugacy classes comprise matrices of order 21 in $GL_2(5)$, and the other 6 conjugacy classes comprise matrices of order 31 in $GL_2(5)$. Thus, $\mathbf{B}_1, \dots, \mathbf{B}_{\omega+1}$ are contained in the union of these 8 conjugacy classes.

Next, as ω is assumed to be large enough,

$$\{\mathbf{I}, \mathbf{B}_1, \dots, \mathbf{B}_1^{31}\} \\ \subseteq \{\mathbf{M}_\omega \mathbf{M}_{\omega-1} \dots \mathbf{M}_1 : \mathbf{M}_j \in \{\mathbf{I}, \mathbf{B}_j\}, 1 \leq j \leq \omega\},$$

and thus $\text{rank}(\mathbf{B}_{\omega+1} + \mathbf{B}_1^j) = 5$ for all $1 \leq j \leq 31$. Let \mathbf{B}'_1 be the representative listed in [23] for the conjugacy class which \mathbf{B}_1 belongs to. Then, \mathbf{B}'_1 can be written as $\mathbf{AB}_1\mathbf{A}^{-1}$ for some $\mathbf{A} \in GL_5(2)$. Also write $\mathbf{B}'_{\omega+1} = \mathbf{AB}_{\omega+1}\mathbf{A}^{-1}$. Then, for all $1 \leq j \leq 31$,

$$\text{rank}(\mathbf{B}'_{\omega+1} - \mathbf{B}_1^j) = \text{rank}(\mathbf{A}(\mathbf{B}_{\omega+1} - \mathbf{B}_1^j)\mathbf{A}^{-1}) = 5.$$

It can be observed that the set $\{\mathbf{B}'_1, \mathbf{B}_1^2, \dots, \mathbf{B}_1^{31}\}$ is identical no matter which conjugacy class of order 31 matrices \mathbf{B}'_1 is in. It can further be checked that $\text{rank}(\mathbf{B}_1^j - \mathbf{B}_1^k) = 5$ for all $1 \leq j < k \leq 31$. Thus, the 33 matrices $\mathbf{0}, \mathbf{B}_1, \dots, \mathbf{B}_1^{31}, \mathbf{B}_{\omega+1}$ form a 5-dimensional rank-metric code of distance 5 over $\text{GF}(2)$. However, this contradicts the fact that the number of codewords of such a code is at most 32 according to the Singleton bound of rank-metric codes.

Consequently, \mathbf{B}'_1 can only be the representative for either of the two conjugacy classes of order 21 matrices. It can be observed that the set $\{\mathbf{B}'_1, \dots, \mathbf{B}_1^{21}\}$ is identical for both cases. Then, exhaustive enumeration can be readily conducted on all possible $\mathbf{B}'_{\omega+1} \in GL_5(2)$ with $\text{rank}(\mathbf{I} - \mathbf{B}'_{\omega+1}) = 5$ to verify that there does not exist $\mathbf{B}'_{\omega+1}$ such that $\text{rank}(\mathbf{B}'_{\omega+1} - \mathbf{B}_1^j) = 5$ for all $1 \leq j \leq 21$. We can now conclude that there does not exist a vector linear solution over $\text{GF}(2)^5$ when ω is large enough. \square

Remark: It has been proven in [24] that the classical network proposed in [3] which is not scalar linearly solvable over any field has a vector linear solution over $\text{GF}(q)^L$ if and only if L is even. However, the discovery in Proposition 14 is more surprising in the sense that a multicast network is considered, which always has a linear solution over a sufficiently large alphabet. In comparison, a general solvable network may not even be vector linearly solvable over any $\text{GF}(q)^L$ [25].

V. SUMMARY

In this paper, several new results are established for vector linear network coding (LNC) on multicast networks. A systematic way is first introduced to construct a multicast network

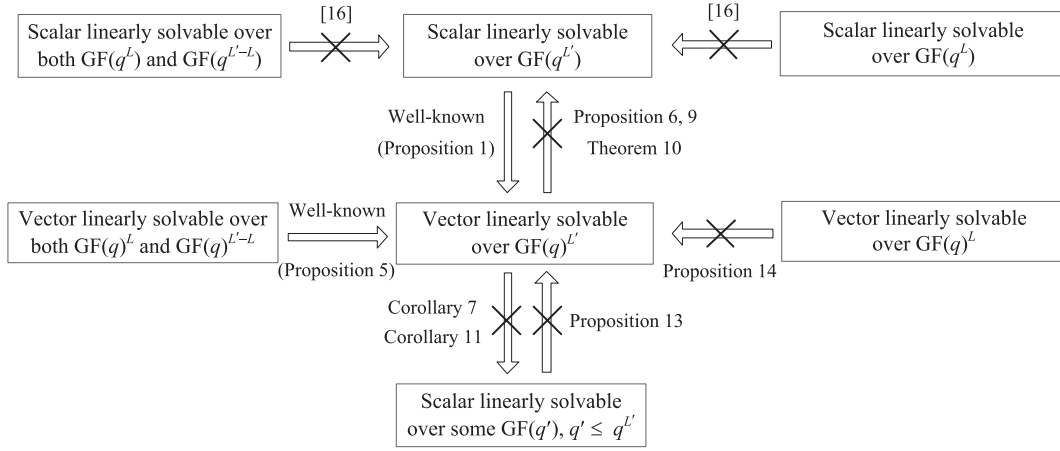


Fig. 6. The relationship established between scalar and vector linear solvability on a multicast network. Herein, $1 < hL < L'$.

that has a vector linear solution over $\text{GF}(p)^L$, but does not have a scalar linear solution over any $\text{GF}(q')$ with $q' \leq p^L$, for an arbitrary prime p and infinitely many alphabet sizes p^L . This affirms a conjectured benefit of vector LNC over scalar one in [11]. In addition, the technique to construct a vector linear solution is based on an interesting observation: a vector linear solution over $\text{GF}(q)^L$ can be constructed by direct sum of different scalar linear codes, which are *not necessarily* scalar linear solutions, over $\text{GF}(q^{L_1})$, \dots , $\text{GF}(q^{L_m})$ with $L_1 + \dots + L_m = L$. This is demonstrated to be useful and cannot be substituted by scalar LNC because a multicast network which has scalar linear solutions over $\text{GF}(q^{L_1})$, \dots , $\text{GF}(q^{L_m})$ may not even be scalar linearly solvable over $\text{GF}(q^{L_1+\dots+L_m})$. In the second part of the paper, explicit multicast networks are presented and proven to have the special property that they do not have a vector linear solution of dimension L over $\text{GF}(2)$ but have scalar linear solutions over $\text{GF}(q')$ for some $q' < 2^L$, where q' can be odd or even. This discovery unveils a surprising result for vector LNC on multicast networks: the existence of a vector linear solution over $\text{GF}(2)^L$ does not imply the existence of a vector linear solution over $\text{GF}(2)^{L'}$ with $L' > L$. Fig. 6 summarizes the relationship between scalar and vector LNC on a multicast network established so far in the literature.

APPENDIX

A. Proof of Lemma 8

Denote by e_{j1}, \dots, e_{jd_j} the d_j outgoing edges of layer-3 node v_j for each $1 \leq j \leq \omega$. Consider a vector linear code over $\text{GF}(q)^L$. For $1 \leq j \leq \omega$, denote by $\mathbf{U}_{j1}, \dots, \mathbf{U}_{jd_j}$ the local encoding kernels for adjacent pairs (d_j, e) with $e \in \text{In}(v_j)$ and $e \in \text{In}(v_{j-1})$, respectively, where v_0 stands for v_ω . Note that by left multiplying \mathbf{U}_{j1} to the local encoding kernels for downstream adjacent pairs $(e, e_{j1}), \dots, (e, e_{jd_j})$, and resetting \mathbf{U}_{j1} to be the $L \times L$ identity matrix \mathbf{I} , the global encoding kernels for edges e_{j1}, \dots, e_{jd_j} remain unchanged. Hence, without loss of generality, for all $1 \leq j \leq \omega$ and $1 \leq k \leq d_j$, we can assume $\mathbf{U}_{jk} = \mathbf{I}$ and let $\mathbf{K}_{jk}, \mathbf{K}'_{jk}$ denote the local encoding kernels for (e, e_{jk}) , $e \in \text{In}(v_j)$. Then, the

juxtaposition of global encoding kernels for edges e_{jk} is equal to

$$[\mathbf{F}_{e_{j1}} \cdots \mathbf{F}_{e_{jd_j}}]_{1 \leq j \leq \omega} = \begin{bmatrix} \mathbf{K}_{11} & \mathbf{K}_{1d_1} & \mathbf{0} & \mathbf{0} & \mathbf{K}_{\omega d_1} & \mathbf{K}_{\omega d_\omega} \\ \mathbf{K}'_{11} & \mathbf{K}'_{1d_1} & \vdots & \vdots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & \cdots & \mathbf{0} & \vdots \\ \vdots & \vdots & \mathbf{K}_{(\omega-1)1} & \mathbf{K}_{(\omega-1)d_{\omega-1}} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{K}'_{(\omega-1)1} & \mathbf{K}'_{(\omega-1)d_{\omega-1}} & \mathbf{K}'_{\omega 1} & \mathbf{K}'_{\omega d_\omega} \end{bmatrix}.$$

Since there is a receiver connected from every set N of ω grey nodes with $\text{maxflow}(N)$ and each e_{jk} is the unique incoming edge to a grey node, the vector linear code is a solution if and only if for every set E of ω edges in $\{e_{jk} : 1 \leq j \leq \omega, 1 \leq k \leq d_j\}$ with $\text{maxflow}(E) = \omega$, where $\text{maxflow}(E)$ means the number edge-disjoint paths starting from the source and ending at edges in E , the matrix $[\mathbf{F}_e]_{e \in E}$ is of full rank ωL .

To prove the necessity part of the lemma, assume that the considered code is a vector linear solution. First observe that $\text{maxflow}(E) = \omega$ when $E = \{e_{1k_1}, \dots, e_{(\omega-2)k_{\omega-2}}, e_{(\omega-1)1}, e_{(\omega-1)2}\}$, where $1 \leq k_j \leq d_j$.

$$\text{Then the matrix } [\mathbf{F}_e]_{e \in E} = \begin{bmatrix} \mathbf{K}_{1k_1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{K}'_{1k_1} & \cdots & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{K}_{(\omega-2)k_{\omega-2}} & \mathbf{0} \\ \cdots & \mathbf{K}'_{(\omega-2)k_{\omega-2}} & \mathbf{K}_{(\omega-1)1} & \mathbf{K}_{(\omega-1)2} \\ \mathbf{0} & \mathbf{0} & \mathbf{K}'_{(\omega-1)1} & \mathbf{K}'_{(\omega-1)2} \end{bmatrix}$$

has full rank ωL . Because

$$\begin{aligned} 0 &\neq \det([\mathbf{F}_e]_{e \in E}) \\ &= \det \left(\begin{bmatrix} \mathbf{K}_{1k_1} & \mathbf{0} & \mathbf{0} \\ \mathbf{K}'_{1k_1} & \cdots & \cdots \\ \mathbf{0} & \cdots & \mathbf{K}_{(\omega-2)k_{\omega-2}} \\ \mathbf{0} & \mathbf{K}'_{(\omega-2)k_{\omega-2}} & \mathbf{K}_{(\omega-1)1} \end{bmatrix} \right) \\ &\quad \det \left(\begin{bmatrix} \mathbf{K}_{(\omega-1)1} & \mathbf{K}_{(\omega-1)2} \\ \mathbf{K}'_{(\omega-1)1} & \mathbf{K}'_{(\omega-1)2} \end{bmatrix} \right) \\ &= \det(\mathbf{K}_{1k_1}) \cdots \det(\mathbf{K}_{(\omega-2)k_{\omega-2}}) \det \left(\begin{bmatrix} \mathbf{K}_{(\omega-1)1} & \mathbf{K}_{(\omega-1)2} \\ \mathbf{K}'_{(\omega-1)1} & \mathbf{K}'_{(\omega-1)2} \end{bmatrix} \right), \end{aligned}$$

the local encoding kernels $\mathbf{K}_{1k_1}, \dots, \mathbf{K}_{(\omega-2)k_{\omega-2}}$ are invertible matrices. By similar arguments on the set

$\{e_{1k_1}, \dots, e_{(\omega-2)k_{\omega-2}}, e_{\omega 1}, e_{\omega 2}\}, \{e_{11}, e_{12}, e_{3k_3}, \dots, e_{\omega k_\omega}\}$, and $\{e_{21}, e_{22}, e_{3k_3}, \dots, e_{\omega k_\omega}\}$, where $1 \leq k_j \leq d_j$, we can deduce that all local encoding kernels \mathbf{K}_{jk} and \mathbf{K}'_{jk} for $1 \leq j \leq \omega$, $1 \leq k \leq d_j$, are invertible matrices.

Write $\mathbf{A}_{jk} = \mathbf{K}'_{jk} \mathbf{K}_{jk}^{-1}$ for $1 \leq j \leq \omega - 1$, $1 \leq k \leq d_j$, and $\mathbf{A}_{\omega k} = \mathbf{K}_{\omega k} \mathbf{K}_{\omega k}^{-1}$ for $1 \leq k \leq d_\omega$. We need show these invertible matrices satisfy conditions (6) and (7). Define another vector linear code of dimension L over $\text{GF}(q)$ prescribed by the following global encoding kernels

$$[\mathbf{F}'_{e_{j1}} \cdots \mathbf{F}'_{e_{jd_j}}]_{1 \leq j \leq \omega} = \begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{A}_{\omega 1} & \mathbf{A}_{\omega d_\omega} \\ \mathbf{A}_{11} & \mathbf{A}_{1d_1} & \vdots & \vdots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & \ddots & \mathbf{0} & \cdots \\ \vdots & \vdots & \mathbf{I} & \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{A}_{(\omega-1)1} & \mathbf{A}_{(\omega-1)d_{\omega-1}} & \mathbf{I} & \mathbf{I} \end{bmatrix} \quad (10)$$

Since $[\mathbf{F}'_{e_{j1}} \cdots \mathbf{F}'_{e_{jd_j}}]_{1 \leq j \leq \omega} = [\mathbf{F}_{e_{j1}} \cdots \mathbf{F}_{e_{jd_j}}]_{1 \leq j \leq \omega} \mathbf{D}(*),$ where $\mathbf{D}(*)$ stands for the square block diagonal matrix with diagonal blocks equal to $\mathbf{K}_{11}^{-1}, \dots, \mathbf{K}_{1d_1}^{-1}, \dots, \mathbf{K}_{(\omega-1)1}^{-1}, \mathbf{K}_{(\omega-1)d_{\omega-1}}^{-1}, \mathbf{K}_{\omega 1}^{-1}, \mathbf{K}_{\omega d_\omega}^{-1}$, we have, for any set E of ω edges with $\maxflow(E) = \omega$,

$$\text{rank}([\mathbf{F}_e]_{e \in E}) = \text{rank}([\mathbf{F}'_e]_{e \in E}).$$

Consider $E = \{e_{1k_1}, e_{1k_2}, e_{21}, \dots, e_{(\omega-1)1}\}$ subject to $\maxflow(E) = \omega$, where $1 \leq k_1 < k_2 \leq d_1$. Then,

$$\begin{aligned} 0 &\neq \det([\mathbf{F}'_e]_{e \in E}) \\ &= \det \left(\begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{A}_{1k_1} & \mathbf{A}_{1k_2} & \mathbf{I} & \cdots \\ \mathbf{0} & \mathbf{0} & \mathbf{A}_{21} & \cdots \\ \cdots & \cdots & \cdots & \mathbf{I} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{A}_{(\omega-1)1} \end{bmatrix} \right) \\ &= \det \left(\begin{bmatrix} \mathbf{I} & \mathbf{I} \\ \mathbf{A}_{1k_1} & \mathbf{A}_{1k_2} \end{bmatrix} \right) \\ &\quad \times \det \left(\begin{bmatrix} \mathbf{A}_{21} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \cdots & \cdots \\ \cdots & \mathbf{A}_{(\omega-2)1} & \mathbf{I} \\ \mathbf{0} & \mathbf{0} & \mathbf{A}_{(\omega-1)1} \end{bmatrix} \right). \end{aligned}$$

This implies that

$$0 \neq \det \left(\begin{bmatrix} \mathbf{I} & \mathbf{I} \\ \mathbf{A}_{1k_1} & \mathbf{A}_{1k_2} \end{bmatrix} \right) = \det \left(\begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{A}_{1k_1} & \mathbf{A}_{1k_2} - \mathbf{A}_{1k_1} \end{bmatrix} \right),$$

i.e., $\text{rank}(\mathbf{A}_{1k_1} - \mathbf{A}_{1k_2}) = L$. By similar arguments on $E = \{e_{jk_1}, e_{jk_2}, e_{(j+1)1}, \dots, e_{(j+\omega-1)1}\}$, where $1 \leq j \leq \omega$, $1 \leq k_1 < k_2 \leq d_j$, and e_{l1} refers to $e_{(l-\omega)1}$ whenever $l > \omega$, we can verify that condition (6) holds for the considered \mathbf{A}_{jk} .

Consider $E = \{e_{1k_1}, e_{2k_2}, \dots, e_{\omega k_\omega}\}$ subject to $\maxflow(E) = \omega$, where $1 \leq k_j \leq d_j$. Then,

$$[\mathbf{F}'_e]_{e \in E} = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{A}_{\omega k_\omega} \\ \mathbf{A}_{1k_1} & \mathbf{I} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{A}_{2k_2} & \cdots & \mathbf{0} \\ \cdots & \cdots & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{A}_{(\omega-1)k_{\omega-1}} & \mathbf{I} \end{bmatrix} \text{ has full rank}$$

ωL . Set

$$\begin{aligned} \mathbf{M}_\omega &= \begin{bmatrix} \mathbf{I} & \mathbf{0} & -\mathbf{A}_{\omega k_\omega} \\ \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \mathbf{0} \\ \cdots & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix}, \\ \mathbf{M}_{\omega-1} &= \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{A}_{\omega k_\omega} \mathbf{A}_{(\omega-1)k_{\omega-1}} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \cdots & \mathbf{0} \\ \cdots & \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix}, \dots, \\ \mathbf{M}_2 &= \begin{bmatrix} \mathbf{I} & (-1)^{\omega-1} \mathbf{A}_{\omega k_\omega} \mathbf{A}_{(\omega-1)k_{\omega-1}} \cdots \mathbf{A}_{2k_2} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \cdots & \cdots \\ \cdots & \mathbf{0} & \cdots & \mathbf{0} \\ \cdots & \cdots & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix}. \end{aligned}$$

Obviously $\det(\mathbf{M}_2) = \cdots = \det(\mathbf{M}_{\omega-1}) = \det(\mathbf{M}_\omega) = 1$. A careful calculation yields

$$\begin{aligned} &\mathbf{M}_2 \cdots \mathbf{M}_\omega [\mathbf{F}'_e]_{e \in E} \\ &= \begin{bmatrix} \mathbf{I} + (-1)^{\omega-1} \mathbf{A}_{\omega k_\omega} \cdots \mathbf{A}_{1k_1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{A}_{1k_1} & \mathbf{I} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{A}_{2k_2} \cdots & \mathbf{0} & \cdots \\ \cdots & \cdots & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{A}_{(\omega-1)k_{\omega-1}} & \mathbf{I} \end{bmatrix}. \end{aligned}$$

This implies

$$\det(\mathbf{I} + (-1)^{\omega-1} \mathbf{A}_{\omega k_\omega} \cdots \mathbf{A}_{1k_1}) = \det([\mathbf{F}'_e]_{e \in E}) \neq 0,$$

and hence $\text{rank}(\mathbf{I} + (-1)^{\omega-1} \mathbf{A}_{\omega k_\omega} \cdots \mathbf{A}_{1k_1}) = L$. Condition (7) thus holds for the considered \mathbf{A}_{jk} . The necessity part of the lemma is proved.

For the sufficiency part, let \mathbf{A}_{jk} , $1 \leq j \leq \omega$, $1 \leq k \leq d_j$, be $L \times L$ invertible matrices over $\text{GF}(q)$ subject to (6) and (7). Assume that the considered vector linear code has local encoding kernels $\mathbf{K}_{jk} = \mathbf{I}$ and $\mathbf{K}'_{jk} = \mathbf{A}_{jk}$ when $1 \leq j \leq \omega - 1$, and $\mathbf{K}'_{jk} = \mathbf{I}$, $\mathbf{K}_{jk} = \mathbf{A}_{jk}$ when $j = \omega$, where $1 \leq k \leq d_j$. In this way, the juxtaposition $[\mathbf{F}_{e_{j1}} \cdots \mathbf{F}_{e_{jd_j}}]_{1 \leq j \leq \omega}$ of global encoding kernels for edges $\{e_{jk} : 1 \leq j \leq \omega, 1 \leq k \leq d_j\}$ is identical to (10). It can then be shown, by similar classified discussion following (10), that for every set E of ω edges in $\{e_{jk} : 1 \leq j \leq \omega, 1 \leq k \leq d_j\}$ with $\maxflow(E) = \omega$, the $\omega L \times \omega L$ matrix $[\mathbf{F}_e]_{e \in E}$ is of full rank ωL . The considered code thus qualifies as a solution for $\mathcal{N}_{\omega, \mathbf{d}}$.

B. Proof of Theorem 10

The case $p = 2$ has been considered in Proposition 9.

Assume that p is odd and l is an arbitrary positive integer. Write $a = p^2 + p + 1$ and $b = 2(p - 1)$. Note that a divides $p^{3l} - 1$ but does not divide $p^{3l+1} - 1$, and b divides $p^{2l} - 1$ but does not divide $p^{2l+1} - 1$. Label all odd primes smaller than ab as p_1, \dots, p_n for some n . For each $1 \leq j \leq n$, denote by q_j the smallest power of p_j that does not divide $p - 1$, and by m_j the smallest positive integer subject to $p^{m_j} \equiv 1 \pmod{q_j}$. Define m to be the least common multiplier of 12 and m_1, \dots, m_n . In this manner, each of a, b, q_1, \dots, q_n divides

$p^{ml} - 1$, but none of them divides $p^{ml+1} - 1$. Moreover, as $\frac{q_1 \cdots q_n}{p_1 \cdots p_n} < p - 1$, the largest divisor of $p^{ml+1} - 1$ that is smaller than ab is $b/2 = p - 1$.

Write $L = ml + 1$, which is no smaller than 13. Denote $\frac{(p^9-1)(p^{L-9}-1)}{ab}$ by d_0 , which is always an integer as a divides $p^9 - 1$ and b divides $p^{L-9} - 1$. Consider the network $\mathcal{N}_{\omega, \mathbf{d}}$ with ω sufficiently large and $\mathbf{d} = (d_0, d_0, \dots, d_0, (a-1)(b-1)d_0)$. It suffices to show that it is not scalar linearly solvable over $\text{GF}(p^L)$ but vector linearly solvable over $\text{GF}(p)^L$.

Let d be a proper divisor of $p^L - 1$. In the case $d < d_0$, it is obvious to observe that condition (3) does not hold for the ω -tuple \mathbf{d} when ω is sufficiently large. Consider the case $d \geq d_0$. As $L \geq 13$ and $ab = 2(p^3 - 1)$, it can be readily checked that $\frac{(p^9-1)(p^{L-9}-1)}{ab} > \frac{p^{L-1}}{ab+1}$, so $d > \frac{p^{L-1}}{ab+1}$ and can be written as $(p^L - 1)/d'$ for some divisor d' of $p^L - 1$ that is smaller than ab . As argued previously, $d' \leq b/2 = p - 1$, so

$$\begin{aligned} & (a-1)(b-1)d_0 - (d' - 1)\frac{p^L - 1}{d'} \\ & \geq (a-1)(b-1)\frac{(p^9-1)(p^{L-9}-1)}{ab} - \frac{b-2}{b}(p^L - 1) \\ & = \frac{a-b+1}{ab}p^L - \frac{ab-a-b+1}{ab}(p^9 + p^{L-9} - 1) + \frac{b-2}{b} \\ & > \frac{2}{ab}p^L - p^9 - p^{L-9} > 0. \end{aligned}$$

This implies $\left\lceil \frac{(a-1)(b-1)d_0}{d} \right\rceil = d'$. Consequently,

$$\begin{aligned} & d \left(\underbrace{\left\lceil \frac{d_0}{d} \right\rceil + \cdots + \left\lceil \frac{d_0}{d} \right\rceil}_{\omega-1} + \left\lceil \frac{(a-1)(b-1)d_0}{d} \right\rceil - \omega + 1 \right) + 2 \\ & = \frac{p^L - 1}{d'} d' + 2 > p^L, \end{aligned}$$

so condition (3) does not hold for the case $d \geq d_0$ either. Theorem 2 then asserts that the considered network $\mathcal{N}_{\omega, \mathbf{d}}$ is not scalar linearly solvable over $\text{GF}(p^L)$.

We next establish a vector linear solution for $\mathcal{N}_{\omega, \mathbf{d}}$ over $\text{GF}(p)^L$. Let \mathbf{G}_1 be the 9×9 invertible matrix over $\text{GF}(p)$ representing a primitive element in $\text{GF}(p^9)$, and \mathbf{G}_2 be the $(L-9) \times (L-9)$ invertible matrix over $\text{GF}(p)$ representing a primitive element in $\text{GF}(p^{L-9})$ according to the homomorphism presented in (1) in Section II.A. Then, $\text{rank}(\mathbf{G}_1^{j_1} - \mathbf{G}_1^{j_2}) = 9$ for all $1 \leq j_1 < j_2 \leq p^9 - 1$, and $\text{rank}(\mathbf{G}_2^{j_1} - \mathbf{G}_2^{j_2}) = L - 9$ for all $1 \leq j_1 < j_2 \leq p^{L-9} - 1$. For $1 \leq j \leq \frac{p^9-1}{a}$, $1 \leq k \leq \frac{p^{L-9}-1}{b}$, define \mathbf{B}_{jk} to be the $L \times L$ matrix G over $\text{GF}(q)$ as $\mathbf{B}_{jk} = \begin{bmatrix} \mathbf{G}_1^{aj} & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2^{bk} \end{bmatrix}$. Then, $\text{rank}(\mathbf{B}_{j_1 k_1} - \mathbf{B}_{j_2 k_2}) = \text{rank}(\mathbf{G}_1^{aj_1} - \mathbf{G}_1^{aj_2}) + \text{rank}(\mathbf{G}_2^{bk_1} - \mathbf{G}_2^{bk_2}) = L$ for all $1 \leq j_1 < j_2 \leq \frac{p^9-1}{a}$, $1 \leq k_1 < k_2 \leq \frac{p^{L-9}-1}{b}$. Set $\mathbf{A}_{n1}, \dots, \mathbf{A}_{nd_0}$ to be the d_0 distinct matrices in $\{\mathbf{B}_{jk} : 1 \leq j \leq \frac{p^9-1}{a}, 1 \leq k \leq \frac{p^{L-9}-1}{b}\}$ for all $1 \leq n \leq \omega - 1$, and set $\mathbf{A}_{\omega 1}, \dots, \mathbf{A}_{\omega((a-1)(b-1)d_0)}$ to be the

$(a-1)(b-1)d_0$ distinct matrices in

$$\left\{ (-1)^\omega \begin{bmatrix} \mathbf{G}_1^{a'} & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2^{b'} \end{bmatrix} \mathbf{B}_{jk} : 1 \leq a' < a, 1 \leq b' < b, \right. \\ \left. 1 \leq j \leq \frac{p^9-1}{a}, 1 \leq k \leq \frac{p^{L-9}-1}{b} \right\}.$$

Condition (6) naturally holds for thus defined \mathbf{A}_{jk} . Moreover, as $\mathbf{G}_1^{aj+a'} \neq \mathbf{I}$ and $\mathbf{G}_2^{bj+b'} \neq \mathbf{I}$, $\text{rank}(\mathbf{I} - \mathbf{G}_1^{aj+a'}) = 9$ and $\text{rank}(\mathbf{I} - \mathbf{G}_2^{bj+b'}) = L - 9$ for all $j \geq 0$, $1 \leq a' < a$ and $1 \leq b' < b$. Consequently, condition (7) holds for \mathbf{A}_{jk} too. By Lemma 8, $\mathcal{N}_{\omega, \mathbf{d}}$ is vector linearly solvable over $\text{GF}(p)^L$.

C. Proof of Lemma 12

Given invertible matrices $\mathbf{A}_{11}, \mathbf{A}_{12}, \dots, \mathbf{A}_{\omega 1}, \mathbf{A}_{\omega 2}$ over $\text{GF}(q)$ of size $L \times L$, define invertible $L \times L$ matrices \mathbf{B}_j , $1 \leq j \leq \omega + 1$ in the following way:

$$\begin{aligned} \mathbf{B}_1 &= (\mathbf{A}_{11}^{-1}) \mathbf{A}_{12}, \\ \mathbf{B}_2 &= (\mathbf{A}_{11}^{-1} \mathbf{A}_{21}^{-1}) \mathbf{A}_{22} (\mathbf{A}_{11}), \\ &\vdots \\ \mathbf{B}_\omega &= (\mathbf{A}_{11}^{-1} \cdots \mathbf{A}_{\omega 1}^{-1}) \mathbf{A}_{\omega 2} (\mathbf{A}_{(\omega-1)1} \cdots \mathbf{A}_{11}), \\ \mathbf{B}_{\omega+1} &= (-1)^{\omega-1} \mathbf{A}_{11}^{-1} \cdots \mathbf{A}_{\omega 1}^{-1}. \end{aligned} \quad (11)$$

Conversely, given invertible $L \times L$ matrices \mathbf{B}_j , $1 \leq j \leq \omega + 1$, define $\mathbf{A}_{11}, \mathbf{A}_{12}, \dots, \mathbf{A}_{\omega 1}, \mathbf{A}_{\omega 2}$ to be arbitrary matrices satisfying (11). Such a selection always exists because we can set $\mathbf{A}_{11}, \dots, \mathbf{A}_{(\omega-1)1} = \mathbf{I}$, $\mathbf{A}_{\omega 1} = (-1)^{\omega-1} \mathbf{B}_{\omega+1}^{-1}$, and $\mathbf{A}_{j2} = (\mathbf{A}_{j1} \cdots \mathbf{A}_{11}) \mathbf{B}_j (\mathbf{A}_{11}^{-1} \cdots \mathbf{A}_{(j-1)1}^{-1})$ for $1 \leq j \leq \omega$.

It can be readily checked that the two sets of matrices $\{\mathbf{M}_\omega \mathbf{M}_{\omega-1} \cdots \mathbf{M}_1 : \mathbf{M}_j \in \{\mathbf{A}_{j1}, \mathbf{A}_{j2}\}, 1 \leq j \leq \omega\}$ and $\{\mathbf{A}_{\omega 1} \cdots \mathbf{A}_{11} \mathbf{M}_\omega \mathbf{M}_{\omega-1} \cdots \mathbf{M}_1 : \mathbf{M}_j \in \{\mathbf{I}, \mathbf{B}_j\}, 1 \leq j \leq \omega\}$ are identical. Then,

$$\begin{aligned} & \{\mathbf{I} + (-1)^{\omega-1} \mathbf{M}_\omega \cdots \mathbf{M}_1 : \mathbf{M}_j \in \{\mathbf{A}_{j1}, \mathbf{A}_{j2}\}, 1 \leq j \leq \omega\} \\ &= \{\mathbf{B}_{\omega+1}^{-1} (\mathbf{B}_{\omega+1} + \mathbf{M}_\omega \cdots \mathbf{M}_1) : \mathbf{M}_j \in \{\mathbf{I}, \mathbf{B}_j\}, 1 \leq j \leq \omega\} \end{aligned}$$

Hence, condition (7) holds for $\mathbf{A}_{11}, \mathbf{A}_{12}, \dots, \mathbf{A}_{\omega 1}, \mathbf{A}_{\omega 2}$ if and only if condition (9) holds for $\mathbf{B}_1, \dots, \mathbf{B}_\omega, \mathbf{B}_{\omega+1}$. Moreover, because for every $1 \leq j \leq \omega$,

$$\begin{aligned} & \text{rank}(\mathbf{I} - \mathbf{B}_j) \\ &= \text{rank}(\mathbf{A}_{11}^{-1} \cdots \mathbf{A}_{j1}^{-1} (\mathbf{A}_{j1} \cdots \mathbf{A}_{11} - \mathbf{A}_{j2} \mathbf{A}_{(j-1)1} \cdots \mathbf{A}_{11})) \\ &= \text{rank}(\mathbf{A}_{11}^{-1} \cdots \mathbf{A}_{j1}^{-1} (\mathbf{A}_{j1} - \mathbf{A}_{j2}) \mathbf{A}_{(j-1)1} \cdots \mathbf{A}_{11}) \\ &= \text{rank}(\mathbf{A}_{j1} - \mathbf{A}_{j2}), \end{aligned}$$

condition (8) holds for $\mathbf{B}_1, \dots, \mathbf{B}_\omega, \mathbf{B}_{\omega+1}$ if and only if condition (6) holds for $\mathbf{A}_{11}, \mathbf{A}_{12}, \dots, \mathbf{A}_{\omega 1}, \mathbf{A}_{\omega 2}$.

ACKNOWLEDGMENT

The authors would appreciate the helpful suggestions by the editor as well as anonymous reviewers to help improve the presentation of the paper.

REFERENCES

- [1] 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.
- [2] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.
- [3] M. Médard, M. Effros, D. Karger, and T. Ho, "On coding for non-multicast networks," in *Proc. Annu. Allerton Conf.*, 2003.
- [4] S. Jaggi, M. Effros, and T. Ho, "On linear network coding," in *Proc. Annu. Allerton Conf.*, 2004.
- [5] S. Riis, "Linear versus nonlinear boolean functions in network flow," in *Proc. Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2004.
- [6] C. Fragouli and E. Soljanin, "A connection between network coding and convolutional codes," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2004, pp. 661–666.
- [7] A. R. Lehman and E. Lehman, "Network coding: Does the model need tuning?" in *Proc. Annu. ACM SIAM Symp. Discrete Algorithms*, 2005, pp. 499–504.
- [8] S. Jaggi, Y. Cassuto, and M. Effros, "Low complexity encoding for network codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 40–44.
- [9] M. Khojastepour and A. K. Haddad, "Rotational coding achieves multicast capacity of deterministic wireless networks," in *Proc. Annu. Allerton Conf.*, 2009, pp. 1330–1337.
- [10] S. El Rouayheb, A. Sprintson, and C. Georgiades, "On the index coding problem and its relation to network coding and matroid theory," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3187–3195, Jul. 2010.
- [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] K. Prasad and B. S. Rajan, "Network-error correcting codes using small fields," *IEEE Trans. Commun.*, vol. 62, no. 2, pp. 423–433, Feb. 2014.
- [13] J. Guo, T. Yang, J. Yuan, and J. A. Zhang, "Linear vector physical-layer network coding for MIMO two-way relay channels: Design and performance analysis," *IEEE Trans. Commun.*, vol. 63, no. 7, pp. 2591–2604, Jul. 2015.
- [14] A. R. Lehman and E. Lehman, "Complexity classification of network information flow problems," in *Proc. Annu. Allerton Conf.*, 2003, pp. 142–150.
- [15] 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.
- [16] Q. T. Sun, X. Yin, Z. Li, and K. Long, "Multicast network coding and field sizes," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6182–6191, Nov. 2015.
- [17] Q. T. Sun, S.-Y. R. Li, and Z. Li, "On base field of linear network coding," *IEEE Trans. Inf. Theory*, doi: 10.1109/TIT.2016.2613988.
- [18] W. P. Wardlaw, "Matrix representation of finite fields," *Math. Mag.*, vol. 67, no. 4, pp. 289–293, Oct. 1994.
- [19] C. K. Ngai and R. W. Yeung, "Network coding gain of combination networks," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Oct. 2004, pp. 283–287.
- [20] M. Xiao, M. Médard, and T. Aulin, "A binary coding approach for combination networks and general erasure networks," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2007, pp. 786–790.
- [21] È. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems Inf. Trans.*, vol. 21, no. 1, pp. 1–12, 1985.
- [22] *Great Internet Mersenne Prime Search (GIMPS) Project*, accessed on Sep. 16, 2016. [Online]. Available: <http://www.mersenne.org/default.php>
- [23] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*. Oxford, U.K.: Clarendon, 1985.
- [24] 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.
- [25] 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.



Beijing, China. His research interests include network coding, algebraic study of communication networks, and discrete algorithm design.



generation Internet, data center networking, and network security. He has fulfilled over 30 research projects, including the National Natural Science Foundation of China, the National High-Tech Research and Development Program (863 Program), and the National Key Basic Research Program (973 Program).



with the University of Science and Technology Beijing, Beijing, China. His research interests include the theory and technology of communication networks. He was elected to the Chang Jiang Scholars Program, Ministry of Education, China, in 2009.



Qifu Tyler Sun received the B.Eng. degree (Hons.) and the Ph.D. degree from the Department of Information Engineering, The Chinese University of Hong Kong, Shatin, NT, Hong Kong, in 2005 and 2009, respectively. He has been a Post-Doctoral Fellow with the Institute of Network Coding, The Chinese University of Hong Kong, and a Visiting Research Fellow with the University of New South Wales. He is currently an Associate Professor with the School of Computer and Communication Engineering, University of Science and Technology

Xiaolong Yang received the B.Eng., M.S., and Ph.D. degrees from the University of Electronic Science and Technology of China, Chengdu, China, in 1993, 1996, and 2004, respectively, all in communication and information system. He is currently a Professor with the School of Computer and Communication Engineering, Institute of Advanced Networking Technologies and Services, University of Science and Technology Beijing, Beijing, China. In his research field, he has authored over 80 papers. He holds 16 patents. His research focuses on the next-

Keping Long received the Ph.D. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 1997. From 1998 to 2000, he was a Post-Doctoral Research Fellow with the National Laboratory of Switching Technology and Telecommunication Networks, Beijing University of Posts and Telecommunications, Beijing. From 2001 to 2002, he was a Research Fellow with the ARC Special Research Center for Ultra Broadband Information Networks, The University of Melbourne, Australia. He is currently a Professor with the University of Science and Technology Beijing, Beijing, China. His research interests include the theory and technology of communication networks. He was elected to the Chang Jiang Scholars Program, Ministry of Education, China, in 2009.

Xunrui Yin received the B.S. and Ph.D. degrees in computer science from Fudan University in 2007 and 2013, respectively. He is currently with the Department of Computer Science, University of Calgary, Canada, and the Department of Computer, Wuhan University, China. His research interests include network coding, network topology design, and coding theory.



coding, cloud computing, and energy networks.

Zongpeng Li received the B.E. degree in computer science and technology from Tsinghua University, Beijing, in 1999, and the M.S. degree in computer science and the Ph.D. degree in electrical and computer engineering from the University of Toronto in 2001 and 2005, respectively. From 2011 to 2012, he was with the Institute of Network Coding, The Chinese University of Hong Kong. Since 2005, he has been with the University of Calgary, where he is currently a Professor of computer science. His research interests are in computer networks, network