Linear Network Coding: Effects of Varying the Message Dimension on the Set of Characteristics

Niladri Das and Brijesh Kumar Rai

Abstract

It is known a vector linear solution may exist if and only if the characteristic of the finite field belongs to a certain set of primes. But, can increasing the message dimension make a network vector linearly solvable over a larger set of characteristics? To the best of our knowledge, there exists no network in the literature which has a vector linear solution for some message dimension if and only if the characteristic of the finite field belongs to a set \( P \), for some other message dimension it has a vector linear solution over some finite field whose characteristic does not belong to \( P \). We have found that by increasing the message dimension just by 1, the set of characteristics over which a vector linear solution exists may get arbitrarily larger. However, somewhat surprisingly, we have also found that by decreasing the message dimension just by 1, the set of characteristics over which a vector linear solution exists may get arbitrarily larger.

As a consequence of these finding, we prove two more results: (i) rings may be superior to finite fields in terms of achieving a scalar linear solution over a lesser sized alphabet, (ii) existences of \( m_1 \) and \( m_2 \) dimensional vector linear solution guarantees the existence of an \((m_1 + m_2)\)-dimensional vector linear solution only if the \( m_1 \) and \( m_2 \) dimensional vector linear solutions exist over the same finite field.

Index Terms

Vector linear network coding, message dimension, M-network, non-multicast networks, characteristic set.

I. INTRODUCTION

Why is vector linear network coding needed? What advantage does it provide over scalar linear network coding? A multicast network has a scalar linear solution only if the size of the finite field is sufficiently large, but has a vector linear solution over any given finite field. This fact is presented as a theorem in [2], which shows that any network having a scalar linear solution over \( \mathbb{F}_q \) has an \( l \)-dimensional vector linear solution over \( \mathbb{F}_q \). So if over a given finite field a multicast network does not have a scalar linear solution because the size of the finite field is not large enough, for some message dimension the network would have a vector linear solution over the same finite field. Moreover, there are chances that a network will have an \( l \)-dimensional vector linear solution over \( \mathbb{F}_q \), even when it has no scalar linear solution over any finite field whose size is less than or equal to \( q^2 \) [12].

Linear solvability of a network may depend upon the terminals receiving sufficient number of independent linear equations of the demanded messages. A vector linear network code offers a higher ratio of: the number of coefficients available to encode/decode messages, to the number of possible source messages. For example, in an \( m \)-dimensional vector linear code over \( \mathbb{F}_q \), there are \( q^{m^2} \) coefficients (number of possible \( m \times m \) matrices) and \( q^m \) (number of possible \( m \)-length vectors) possible source messages. In a scalar linear network code over \( \mathbb{F}_q \), there are \( q \) coefficients and \( q \) messages. So the ratio of the number of available linear functions (that can be used to encode/decode messages) to number of possible source messages, increases by a factor of \( q^{m^2 - m} \). In reference [4], which gives an algorithm to design vector linear network codes for multicast networks, the authors Ebrahimi et al. – towards justifying the superiority of vector linear network coding over scalar linear network coding – wrote: “Thus, vector network coding offers a larger space of choices for optimizing cost parameters, such as the operational complexity, or the communication block length. Our work takes small steps in exploring this potential, using a subset of all possible matrices; we believe that the potential of vector coding is much beyond what this work achieves”.

It has been shown that, the existence of a scalar linear solution of a non-multicast network depends upon the characteristic of the finite field; a network may have a scalar linear solution if and only if the characteristic of the finite field belongs to a certain set of primes. Our question is: can such a network have a vector linear solution over a larger set of primes (characteristics)? To the best of our knowledge, for all networks presented in the literature, if the network has a scalar linear solution if and only if the characteristic of the finite field belongs to a set \( P \), then for any positive integer \( d \), it has a \( d \)-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( P \). (The quantity \( d \) is called as the message dimension.) We show that there exists a network which, for any given set of primes \( P \), has a scalar linear solution if and only if the characteristic of the finite field belongs to \( P \), but has a 2-dimensional vector linear solution over all finite fields. We show that similar trend may hold if a 2-dimensional vector linear network code is replaced by a 3-dimensional vector linear network code: for any two sets of primes \( P_1 \) and \( P_2 \), there exists a network which has a 2-dimensional vector linear solution if and
only if the characteristic of the finite field belongs to $P_1$, but has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to $\{P_1, P_2\}$.

Then, whether a higher message dimension is always superior to a lower message dimension in terms of achieving a linear solution over a larger set of characteristics? The answer is no: we show that for any two sets of primes $P_1$ and $P_2$, there exists a network which has a 2-dimensional vector linear solution if and only if the characteristic of the finite field belongs to $\{P_1, P_2\}$, but has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to $P_2$. We also show a network which has a 2-dimensional vector linear solution over all finite fields, but has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to a certain finite set of primes.

As a consequence of the property that the set of characteristics over which a linear solution exists may vary with the message dimension, we prove two more properties of linear network coding. Recently, linear network coding over finite ring alphabets has been studied. In three papers [5], [6], and [7], Connelly et al. answer many questions on whether linear network coding over ring alphabets offer any advantage over linear network coding over finite fields. The size of a finite ring could be any positive integer, where as the size of a finite field is always power of a prime; so it is natural to suspect that there could be some advantage at least in terms of achieving a linear solution over a lesser sized alphabet. In [5] it has been shown that if a network has a scalar linear solution over some finite commutative ring which is not a field, then the network also has a scalar linear solution over a finite field whose size is less than or equal to the size of the ring. We have found that, for any prime number $p$, there exists a network which has a scalar linear solution over a finite field if and only if the size of the finite field is a power of $p$, but has a scalar linear solution over a non-commutative ring of size $16$. Since, all networks that have a scalar linear solution over a finite field of size $q$ also have a scalar linear solution over a finite commutative ring of size $q$ (because a field is also a commutative ring), but all networks that have a scalar linear solution over a finite field of size $q$ does not have a scalar linear solution over a finite field whose size is less than or equal to $q$, we conclude that, in general, finite rings are superior to finite fields in terms of achieving a scalar linear solution over a lesser sized alphabet.

The second property of linear network coding that we prove is as follows. We show that for a network, the existence of an $m_1$-dimensional vector linear solution and an $m_2$-dimensional vector linear solution guarantees the existence of an $(m_1 + m_2)$-dimensional vector linear solution only if the respective $m_1$ and $m_2$ dimensional vector linear solutions exist over the same finite field. We prove this result by showing that, there exists a network which has a 2-dimensional vector linear solution and a 3-dimensional vector linear solution, but has no 5-dimensional vector linear solution.

A. Historical Background

Network coding was introduced by Ahlswede et al. in the pioneering work of [8]. They showed that the capacity of multicast networks (networks with a single source) is equal to the minimum of min-cut of the network, and that this capacity can be achieved by using network coding. Li et al. showed that, a restricted form of network coding called as scalar linear network coding (with encoding and decoding operations over a finite field) is sufficient to achieve the capacity of such networks [9]. Efficient algorithm to employ scalar linear network coding in multicast networks has been shown in [10].

For multicast networks, the size of the finite field and properties of the proper subgroups of the multiplicative group of the finite field can decide existence of a scalar linear solution. Riis et al. showed that for any positive integer $n$, there exists a multicast network (the combination network) which has a scalar linear solution if and only if the size of the finite field is greater than $n$ [11]. It was shown in [10] that for any multicast network there always exists a scalar linear solution if the size of the finite field is larger than the number of terminals. Sun et al. showed that the existence of a scalar linear solution over a certain finite field does not necessarily mean that a scalar linear solution exists over all larger finite fields [12]. In references [12] and [13] the authors show that not only the size, but also the order and the associated coset numbers of the proper subgroups of the multiplicative group of the finite field affects the existence of a scalar linear solution.

For multicast networks, the characteristic of the finite field does not play a significant role in the sense that there does not exist a multicast network that has a scalar linear solution if and only if the characteristic belongs to a certain set of primes.

Vector linear network coding is another restricted version of network coding that has been shown to have some advantage over scalar linear network coding [4]. Scalar and vector linear network coding differs by the fact that in the former, scalar quantities (i.e., elements of the finite field) are used to encode the outgoing messages, whereas in the latter, square matrices are used to encode outgoing messages. The size of these square matrices is described by a parameter called as the message dimension or vector dimension or simply dimension of a vector linear network code. Since, an $1 \times 1$ matrix is also a scalar, scalar linear network coding is vector linear network coding of message dimension 1. By using vector linear network coding of some message dimension if the terminals of a network can retrieve all of its demanded messages, then the network is said to have a vector linear solution. Ebrahimi et al. showed an efficient algorithm to design vector linear network codes that achieves a vector linear solution in multicast networks [4]. They also conjectured that there exists a multicast network which has a $L$-dimensional vector linear solution over a finite field $\mathbb{F}_q$, but has no scalar linear solution over any finite field whose size is less than or equal to $q^L$. This conjecture was settled by Sun et al. in [3] by showing an explicit instance of a network exhibiting such a property. In a recent publication [14], Etzion et al. showed that the gap between the minimum field size to achieve a scalar linear solution and the minimum field size to achieve a vector linear solution can be significantly large (the latter being
lesser). Sun et al. in [3] also showed that there exists a multicast network which has a 4-dimensional vector linear solution over $\mathbb{F}_2$, but has no 5-dimensional vector linear solution over the same finite field (the network also has a 5-dimensional vector linear solution over $\mathbb{F}_{2^5}$, so the solution is not characteristic dependent). This shows that over a fixed finite field, a multicast network may have a vector linear solution for a certain message dimension but not for a higher message dimension.

Non-multicast networks or multi-source multi-terminal networks, which could also be seen as multi-source multicast networks, act very differently to multicast networks. The capacity of such networks could be much lesser than the minimum of min-cut. Till now, no algorithm to find the capacity of such networks exists in the literature. Harvey et al. showed an algorithm to compute an upper-bound on the capacity in [15], which may be tighter than min-cut. Koetter et al. developed an algebraic framework to study both multicast and non-multicast networks [15]. Scalar linear network coding has been shown to be insufficient to achieve the capacity of non-multicast networks. Médard et al. showed that there exists a non-multicast network – the $M$-network – which has no scalar linear solution over any finite field, but has a 2-dimensional vector linear solution over all finite fields [17]. This result was generalized by Das et al. in [18] to show that for any positive integer $m$, there exists a network which has no vector linear solution if message dimension is less than $m$, but has a vector linear solution of $m$ message dimension. However, even vector linear network coding has been shown to be insufficient to achieve capacity [19]. Dougherty et al. showed that more general forms of linear network coding – defined over rings and modules – also fails to achieve the capacity [19]. Reference [19] presented an instance of a network in which the capacity is achieved by using non-linear network coding, but cannot be achieved by using any form of linear network coding. It has been also shown that capacity of non-multicast networks can be unachievable altogether – no form of network coding can achieve the capacity [20].

Since a multicast network can easily be converted into a non-multicast network (by adding a source and connecting a direct edge from this source to all the terminals), the fact that size of the finite field and properties of the proper subgroups of the multiplicative group of the finite field affects scalar linear solvability of multicast networks, holds for non-multicast networks as well. But along with, the characteristic of the finite field also plays an important role. It has been shown in [21] that for any set of polynomials with integer coefficients, there exists a network which has a scalar linear solution over a finite field if and only if the set of polynomials have a common root over the field. This showed that for any set of primes, there exists a network which has a scalar linear solution if and only if the characteristic of the finite field belongs to the given set of primes. This result was generalized in [22] to show that for any set of primes there exists a network which has a vector linear solution for any message dimension if and only if characteristic of the finite field belongs to the given set of primes. The result of Das et al. ( [18]) can be coupled with this result to show that for any set of primes $P$, and for any positive integer $m$, there exists a network which has a vector linear solution if and only if the message dimension is a multiple of $m$ and the characteristic of the finite field belongs to $P$.

Most works in the literature on linear network coding uses finite field as the source alphabet. Recently linear network coding over rings and modules has been studied extensively in three companion papers: [5], [6], and [7]. In [5] the authors have studied scalar linear network coding over commutative rings. They show that if a network has a scalar linear solution over a finite commutative ring which is not a field, then the network also has a scalar linear solution over a finite field whose size is less than or equal to the size of the commutative ring. So this indicates that, if the goal is to achieve a scalar linear solution over the least sized alphabet, there is no need to look for commutative rings. In the other paper [6], they showed that if a network has a vector linear solution but no scalar linear solution (over any finite field), then the network has a scalar linear solution over a non-commutative ring. This immediately shows that there exist networks which have no scalar linear solution over a finite field but have a scalar linear solution over a non-commutative ring. They also showed a network (named as the Dim-$k$ network) that behaves similar to the network of [18]. In [7] they showed that, for any network, linear coding capacity over finite fields is greater than or equal to the linear coding capacity over rings or modules.

B. Organization of the paper

In Section II we re-produce the standard definitions of network coding and linear network coding. In Section III we introduce the network constructions that will be used to prove the results in the paper. In Section IV we produce the main results of the paper. In Section V we conclude the paper. In the Appendix we prove some of the theorems and lemmas shown in Section III. Some of the proofs require polymatroid algebra, and hence in the appendix we also give an introduction to discrete polymatroids and its connection to linear solvability of networks.

II. Preliminaries

A network is represented by a graph $G(V, E)$ where $E \subseteq V \times V$. Three subsets of the set of nodes $V$ are defined: the set of sources $S$, the set of terminals $T$, and the set containing rest of the nodes $V'$. Without loss of generality (w.l.o.g) it is assumed that the sets $S, V'$, and $T$ are disjoint and partition $V$. Each source generates a $d$-length vector uniformly distributed over a finite field $\mathbb{F}_q^d$ (all $d$-length vectors over $\mathbb{F}_q$). Any vector generated by a source is independent of the other vectors generated by other sources. Each terminal wants to receive the vectors generated by a subset of the sources. W.l.o.g. it is assumed that the sources have no incoming edges, and the terminals have no outgoing edges. Each edge carries an element from $\mathbb{F}_q^d$. A vector carried by an edge is either a linear function of the messages generated by the tail node of the edge (if the tail node is
a source), or a linear function of the messages carried by the edges incoming to the tail node of the edge. A vector computed by a terminal is a linear function of the vectors carried by the edges incoming to the terminal.

To compute the linear functions, for each adjacent edge pair, for each source-edge pair where the source is the tail node of the edge, and for each edge-terminal pair where the terminal is the head node of the edge, a $d \times d$ matrix belonging to $\mathbb{F}_{q^d}$ is assigned. Each of these matrices is called local coding matrix, and their collection is called as a linear network code of $d$ message dimension.

For any edge $e \in E$, if the tail node of $e$ is a source $s$, then the vector carried by $e$ is equal to $A_{\{s,e\}}x_s$ where $A_{\{s,e\}}$ is the local coding matrix for the source-edge pair $(s,e)$, and $x_s$ is the vector generated by $s$. For any $e \in E$, if the tail node of $e$ is $v \in \mathcal{V}'$, then the vector carried by $e$ is equal to $\sum_{e' \in \text{In}(v)} A_{\{e',e\}}y_{e'}$ where $\text{In}(v)$ is the set of all edges whose head node is $v$. $A_{\{e',e\}}$ is the local coding matrix for the adjacent edge pair $(e',e)$, and $y_{e'}$ is the vector carried by the edge $e'$. If a terminal $t$ computes a vector $x_t$, then $x_t = \sum_{e \in \text{In}(t)} A_{\{e,t\}}x_e$ where $\text{In}(t)$ is the set of all edges whose head node is $t$. $A_{\{e,t\}}$ is a local coding matrix for the edge-terminal pair $(e,t)$, and $y_e$ is the vector carried by the edge $e$.

A network coding problem is a graph $G(V,E)$ along with a list of sources for each terminal – a terminal demands the vectors generated by the sources given in the list. If the terminals are successful in retrieving their demanded messages, then the network is said to have a $d$-dimensional vector linear solution over $\mathbb{F}_q$. The positive integer $d$ is also referred as message dimension or vector dimension or simply dimension of the vector linear network code. An 1-dimensional vector linear solution is called as a scalar linear solution. If a network has a vector linear solution for some message dimension over $\mathbb{F}_q$, then the network is said to have a linear solution over $\mathbb{F}_q$.

III. Constructing networks $\mathcal{N}_1$ and $\mathcal{N}_2$

In this section we present networks $\mathcal{N}_1$ and $\mathcal{N}_2$ which exhibit the property that the set of characteristics over which a linear solution exists varies with the dimension. These two networks are in turn constructed using three other intermediate networks: the M-network (shown in [17]), the generalized M-network for $m = 3$ (shown in [18]), and the Char-$q - s$ network (our contribution).

A. M-network

The M-network was first shown in [17]. It was shown that this network has no scalar linear solution over any finite field, but has a 2 dimensional vector linear solution over all finite field. For convenience, we have reproduced this network in Fig. 1b. We list the set of edges and vertices of this network below (the labelling is different from [17]).
Fig. 2. The Char-$q - s$ network for $q = 2$. The demands of each terminal is shown below the terminal’s label. Note that the source $s$ is not demanded by any of the terminals.

$$S = \{a, b, x, y\}, V' = \{u_1, u_2, v_1, v_2, v_3\}$$

$$T = \{t_i | 1 \leq i \leq 4\}$$

$$E = \{(a, u_1), (b, u_1), (x, u_2), (y, u_2), (u_1, v_1), (u_1, v_3), (u_2, v_2), (u_2, v_3)\} \cup \{(v_1, t_j) | i = 1, 2, 3, j = 1, 2, 3, 4\}$$

Each terminal demands messages from two sources. Out of these two sources, one is from $\{a, b\}$, and the other is from $\{x, y\}$. No two terminals can demand messages from the same set of sources. So there are 4 terminals. The demands of the terminals are shown in Fig. 1b (below the terminals).

B. Generalized $M$-network for $m = 3$

In reference [18] the M-network was generalized; this generalization constructs one new network for each positive integer $m \geq 3$ such that the network has a vector linear solution if and only if the dimension is a multiple of 3. We use the specific network that results when $m = 3$. For convenience we reproduce this network in Fig. 1b. The set of vertices and edges of this network is given below (the labelling is different from that of [18]).

$$S = \{\bar{a}, \bar{b}, \bar{c}, \bar{r}, \bar{s}, \bar{w}, \bar{x}, \bar{y}, \bar{z}\}, V' = \{\bar{u}_i | i = 1, 2, 3\} \cup \{\bar{v}_i | 1 \leq i \leq 5\}, T = \{\bar{t}_i | 1 \leq i \leq 27\}$$

$$E = \{(\bar{a}, \bar{u}_1), (\bar{b}, \bar{u}_1), (\bar{c}, \bar{u}_1), (\bar{r}, \bar{u}_2), (\bar{s}, \bar{u}_2), (\bar{w}, \bar{u}_2), (\bar{x}, \bar{u}_3), (\bar{y}, \bar{u}_3), (\bar{z}, \bar{u}_3)\} \cup \{(\bar{u}_i, \bar{v}_1), (\bar{u}_i, \bar{v}_4), (\bar{u}_i, \bar{v}_5) | i = 1, 2, 3\}

\cup \{(\bar{v}_i, \bar{t}_j) | 1 \leq i \leq 5, 1 \leq j \leq 27\}$$

Each terminal demands messages from three sources. Out of these three sources, one is from $\{a, b, c\}$, one from $\{r, s, w\}$, and one from $\{x, y, z\}$. No two terminals can demand messages from the same set of sources. So there are 27 terminals.

C. Char-$q - s$ network

In [7] Connelly et al. presented a network named as the Char-$q$ network. This network has a linear solution for any dimension if and only if the characteristics of the finite field divides $q$, where $q$ is any integer greater than or equal to 2. Inspired by the Char-$q$ network, we construct a network that we name as the Char-$q - s$ network, where $s$ is the label of a source node and not a number. The source labelled by $s$ is distinguished from the rest because no terminal demands $s$. We show that if the
middle edges (described below as $e_i$ for $1 \leq i \leq q + 3$) of the network do not transmit any information (i.e. any component of the vector) generated by the source $s$, then the Char-$q - s$ has a scalar linear solution over any finite field. But if the middle edges transmit any symbol (i.e. even one element of the vector) generated by $s$, then the Char-$q - s$ network has a vector linear solution if and only if the characteristic of the finite field divides $q$. The purpose of constructing such a network is that we will attach this network to other networks in such a way that if the other network does not receive any symbol (components of vector) from $s$ through one of the middle edges, then the other network would render linearly unsolvable for a particular message dimension (thereby forcing the characteristic of the finite field to be a divisor of $q$ for the network to have a linear solution for that particular message dimension). We describe the network below.

The Char-$q - s$ network for $q = 2$ is shown in Fig. 2. The network has $q + 3$ source nodes: $x_1, x_2, \ldots, x_{q+2}$ and $s$; and $q + 3$ terminals: $r_1, r_2, \ldots, r_{q+3}$. The rest of the nodes are union of these two sets: $\{m_1, m_2, \ldots, m_{q+3}\}$ and $\{n_1, n_2, \ldots, n_{q+3}\}$. The edges are listed below:

$\{(x_1, m_i) | 1 \leq i \leq q + 1\} \cup \{(s, m_i) | i = 1, 4 \leq i \leq q + 3\} \cup \{(x_i, m_j) | 2 \leq i, j \leq q + 2, i \neq j\} \cup \{(x_i, m_{q+3}) | 1 \leq i \leq q + 2\}
\cup \{(n_i, r_1) | 1 \leq i \leq q + 2\} \cup \{(n_{q+3}, r_i), (n_i, r_{q+3}) | 1 \leq i \leq q + 2\}
\cup \{(x_i, r_1) | 2 \leq i \leq q + 1\} \cup \{(x_i, r_{q+2}),(s, r_2), (s, r_3)\}$

The demands of the terminals are: $r_1$ demands $x_{q+2}$, $r_i$ for $2 \leq i \leq q + 2$ demands $x_i$, and $r_{q+3}$ demands $x_1$. Let the message vector generated by $x_i$ be also denoted by $x_i$, and the message vector generated by $s$ be also denoted by $s$.

Lemma 1. Over a finite field whose characteristic does not divide $q$, for any positive integer $d$, the Char-$q - s$ network has a $d$-dimensional vector linear solution if and only if the middle edges i.e. $e_i$ for $1 \leq i \leq q + 3$ does not carry any component of the vector generated by $s$.

Proof: We prove the ‘if’ part over here. The proof of the ‘only if’ part is shown in Section A. To show the ‘if’ part, we present a scalar linear solution of the Char-$q - s$ network. In this case all the local coding matrices are (scalar) elements of the underlying finite field. Let the vector carried by the edge $e_i$ be denoted by $y_{e_i}$. Chose suitable coding coefficients such that the middle edges carry the following information.

\[ y_{e_1} = x_1 \]
\[ \text{for } 2 \leq j \leq q + 1 : \quad y_{e_j} = x_1 + \sum_{i=2,i\neq j}^{q+2} x_i \]
\[ y_{e_{q+2}} = \sum_{i=2}^{q+1} x_i \]
\[ y_{e_{q+3}} = \sum_{i=1}^{q+2} x_i \]

$r_1$ receives messages $x_i$ for $2 \leq i \leq q + 1$ through direct edges, $x_1$ from $e_1$, and hence it can retrieve $x_{q+2}$ from $y_{e_{q+2}}$, $r_i$ for $2 \leq i \leq q + 1$ receives $x_i$ by subtracting $y_{e_1}$ from $y_{e_{q+3}}$, $r_{q+2}$ receives $x_1$ from a direct edge, and hence it can computes $x_{q+2}$ by subtracting $y_{e_{q+2}}$ from $y_{e_{q+3}}$. And $r_{q+3}$ receives $x_1$ from $y_{e_1}$.

We now prove the following lemma.

Lemma 2. Over a finite field whose characteristic divides $q$, the Char-$q - s$ network has scalar linear solution even when the middle edges i.e. $e_i$ for $1 \leq i \leq q + 3$ carry information generated by $s$.

Proof: Chose suitable coding coefficients such that the middle edges carry the following information.

\[ y_{e_1} = x_1 + s \quad \text{(1)} \]
\[ y_{e_2} = x_1 + x_3 + \cdots + x_{q+2} \quad \text{(2)} \]
\[ y_{e_3} = x_1 + x_2 + x_4 + \cdots + x_{q+2} \quad \text{(3)} \]

for $4 \leq j \leq q + 1 : y_{e_j} = s + \sum_{i=1,i\neq j}^{q+2} x_i \quad \text{(4)}$
\[ y_{e_{q+2}} = s + \sum_{i=2}^{q+1} x_i \quad \text{(5)} \]
\[ y_{e_{q+3}} = s + \sum_{i=1}^{q+2} x_i \quad \text{(6)} \]
When for \( q \) form \([17]\), the Char-q – y network, and an edge \((r_1, t_4)\). The sources \( a \) and \( y \) are common to both of the M-network and the Char-q – y network. The demands of the terminals are written below the label of the terminals.

\( r_1 \) receives messages \( x_i \) for \( 2 \leq i \leq q + 1 \) through direct edges, \( x_1 + s \) from \( e_1 \), and hence it can retrieve \( x_{q+2} \) from \( y_{e_{q+3}} \). \( r_2 \) receives \( s \) from a direct edge, and hence it can subtract \( y_{e_2} \) from \( y_{e_{q+3}} \) to receive \( x_2 \). Similarly, \( r_3 \) receives \( x_3 \). \( r_i \) for \( 4 \leq i \leq q + 1 \) receives \( x_i \) by subtracting \( y_{e_i} \) from \( y_{e_{q+3}} \). \( r_{q+2} \) receives \( x_1 \) from a direct edge, and hence it can computes \( x_{q+2} \) by subtracting \( y_{e_{q+2}} \) from \( y_{e_{q+3}} \). And since \( q = 0 \) over the finite field, \( r_{q+3} \) receives \( x_1 \) by the operation: 

\[
\sum_{i=1}^{q+2} y_{e_i} = (q + 1)x_1 + q + \sum_{j=2}^{q+2} qx_j = x_1
\]

\([7]\)

\[\blacksquare\]

D. Network \( N_1' \)

In this subsection we show the network \( N_1' \). It is constructed by joining together the M-network (reproduced in Section III-A form \([17]\)), the Char-q – y network (shown in Section III-C), and a new edge. The network that results for the particular case when for \( q = 2 \), is shown in Fig. 3. The labelling of the Char-q – y network is different from the description of the Char-q – s network given Section III-C; the label \( s \) is changed to \( y \), and \( x_1 \) is changed to \( a \). The sources \( a \) and \( y \) are common to both networks. In addition to the M-network and the Char-q – y network, there is one additional edge: \((\text{head}(e_3), t_4)\).

The reason these two networks are connected as such is the following. We know that the M-network does not have a scalar linear solution; but we figured that if the terminal \( t_4 \) receives an extra symbol which is a function of \( a \) and \( y \), then the network does have a scalar linear solution. In \( N_1' \), the terminal \( t_4 \) can have this extra information if the information carried by \( e_1 \) is a function of both \( a \) and \( y \). But, from Lemma \([1]\) we know that if such is the case, then the characteristic of the finite field has to divide \( q \) for a scalar linear solution to exist, thus limiting the set of characteristics over which a scalar linear solution exists.

Lemma 3. For any odd number \( d \), the network \( N_1' \) has a \( d \)-dimensional vector linear solution if and only if the characteristic of the finite field divides \( q \).

The proof of this lemma is given in Appendix C.

E. Network \( N_2' \)

In this section we show the network \( N_2' \). It is constructed by joining together the generalized M-network for \( m = 3 \) (reproduced in Section III-B form \([18]\)), the Char-q’ – \( \bar{x} \) network (shown in Section III-C), and some additional edges. The network that results for the particular case when for \( q' = 2 \), is shown in Fig. 4. The labelling of the Char-q’ – \( \bar{x} \) network is different from the description of the Char-q – s network given Section III-C; the label \( s \) is changed to \( \bar{x} \), \( x_1 \) is changed to \( \bar{a} \),
Fig. 4. The network \( N_2 \) for \( q' = 2 \). For some of the terminals, there is a direct edge connecting a source to the terminal, and the complete edge has not been shown to maintain tidiness. For example, the terminal \( t_7 \) has a direct edge \((\bar{\omega}, t_7)\) connecting the source \( \bar{\omega} \) and \( t_7 \), but the complete edge has not been shown.

any other \( x_i \) where \( i \neq 1 \) is changed to \( \bar{x}_i \), edge \( e_i \) is changed to \( \bar{e}_i \), and terminals \( r_i \) is changed to \( \bar{r}_i \). The sources \( \bar{a} \) and \( \bar{x} \) are common to both networks. In addition to the generalized M-network for \( m = 3 \) and the \( \text{Char}-q' - \bar{x} \) network, the additional edges that are not part of these two networks, are given below:

\[
\{(w, \bar{r}_7), (\bar{w}, \bar{r}_8), (w, \bar{r}_9), (\bar{w}, \bar{r}_{18}), (w, \bar{r}_{17}), (\bar{c}, \bar{r}_{20}), (c, \bar{r}_{21}), (c, \bar{r}_{22}), (c, \bar{r}_{23}), (c, \bar{r}_{24}), (\bar{a}, \bar{r}_{25}), (\bar{y}, \bar{r}_{20})\}.
\]

We prove the following properties of \( N_2 \). The proofs of all of these lemmas are given in Appendix D.

**Lemma 4.** The network \( N_2 \) has no scalar linear solution over any finite field.

The proof is given in Appendix D-A.

**Lemma 5.** The network \( N_2 \) has a 2-dimensional vector linear solution if and only if the characteristic of the finite field divides \( q' \).

The proof is given in Appendix D-B.

**Lemma 6.** The network \( N_2 \) has a 5-dimensional vector linear solution if and only if the characteristic of the finite field divides \( q' \).

The proof is given in Appendix D-C.

**IV. MAIN RESULTS**

Let \( V_1 \) be the set of all nodes and \( E_1 \) be the set of all edges of \( N_1 \) (shown in Section III-D). Similarly, let \( V_2 \) be the set of all nodes and \( E_2 \) be the set of all edges of \( N_2 \) (shown in Section III-E).

**Definition 1.** The union of networks \( N_1 \) and \( N_2 \) is a network whose node set is \( V_1 \cup V_2 \), and edge set is \( E_1 \cup E_2 \). Let this union be named as \( N_{12} \).

**Lemma 7.** \( N_{12} \) has a \( d \)-dimensional vector linear solution if and only if both of the constituent sub-networks \( N_1 \) and \( N_2 \) has a \( d \)-dimensional vector linear solution.
Proof: If both \( \mathcal{N}_1 \) and \( \mathcal{N}_2 \) have a \( d \)-dimensional vector linear solution, then it \( \mathcal{N}_{12} \) also has a \( d \)-dimensional vector linear solution since the latter is an union of the former two. If \( \mathcal{N}_{12} \) has a \( d \)-dimensional vector linear solution, since there is not information exchange between \( \mathcal{N}_1 \) and \( \mathcal{N}_2 \) as \( \{V_1 \cup E_1\} \cap \{V_2 \cup E_2\} = \emptyset \), both of the sub-networks \( \mathcal{N}_1 \) and \( \mathcal{N}_2 \) must have a \( d \)-dimensional vector linear solution.

The first two theorems show that with increasing message dimension the set of characteristics over which a vector linear solution exists get larger.

**Theorem 8.** For any set of primes \( P \), there exists a network which has a scalar linear solution if and only if the characteristic of the finite field belongs to \( P \), but has a 2-dimensional vector linear solution over all finite fields.

Proof: Let \( P = \{p_1, p_2, \ldots, p_l\} \). The network \( \mathcal{N}_1 \) shown in Section III-D for \( q = p_1 \times p_2 \times \cdots \times p_l \) is such a network. Lemma 3 shows that the network has a scalar linear solution if and only if the characteristic of the finite field divides \( q \). But for that to happen, the characteristic must be one of \( \{p_1, p_2, \ldots, p_l\} \).

The M-network part of \( \mathcal{N}_1 \) already has a 2-dimensional vector linear solution over all finite fields \( [17] \). The Char-\( q - y \) part of \( \mathcal{N}_1 \) was shown to have a scalar linear solution over all finite fields when its middle edges do not carry any information from \( y \) (see proof for the ‘if’ part of Lemma 1), and hence it also has a 2-dimensional vector linear solution over all finite fields. Since the M-network part and the Char-\( q - y \) part both have a 2-dimensional vector linear solution over all finite fields, the whole network also has a 2-dimensional vector linear solution over all finite fields.

**Theorem 9.** For any two sets of prime numbers \( P_1 = \{p_1, p_2, \ldots, p_l\} \) and \( P_2 = \{p_1', p_2', \ldots, p_{l'}\} \), there exists a network which has a 2-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( P_1 \), but has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( \{P_1, P_2\} \).

Proof: Consider the network \( \mathcal{N}_{12} \) for \( q = p_1 \times p_2 \times \cdots \times p_l \times p_1' \times p_2' \times \cdots \times p_{l'} \) and \( q' = p_1 \times p_2 \times \cdots \times p_l \). As explained in the proof of Theorem 8, \( \mathcal{N}_1 \) has a 2-dimensional vector linear solution over all finite fields. Lemma 3 shows that \( \mathcal{N}_2 \) has 2-dimensional vector linear solution if and only if the characteristic of the finite field divides \( q' \). But for the characteristic to divide \( q' \), it must be one of \( \{p_1, p_2, \ldots, p_l\} \). Hence, \( \mathcal{N}_{12} \) has a 2-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( P_1 \).

As per Lemma 1, \( \mathcal{N}_1 \) has a 3-dimensional vector linear solution if and only if the characteristic of the finite field divides \( q \). But the characteristic divides \( q \) if and only if it belongs to \( \{P_1, P_2\} \). The generalized M-network for \( m = 3 \) (part of \( \mathcal{N}_2 \)) has a 3-dimensional vector linear solution over all finite fields (proved in [18]). The Char-\( q' - x \) part of \( \mathcal{N}_2 \) has a scalar linear solution over all finite fields if its middle edges do not carry any information about \( x \) (see if part of Lemma 1), and hence it also has a 3-dimensional vector linear solution. Since, the generalized M-network for \( m = 3 \) part already has a 3-dimensional vector linear solution, the middle edges of the Char-\( q' - x \) need not carry any information about \( x \). Hence, the whole network \( \mathcal{N}_2 \) has a 3-dimensional vector linear solution over all finite fields. Since both \( \mathcal{N}_1 \) and \( \mathcal{N}_2 \) has a 3-dimensional vector linear solution if the characteristic of the finite field belongs to \( \{P_1, P_2\} \), and since \( \mathcal{N}_1 \) has a 3-dimensional vector linear solution only if the characteristic of the finite field belongs to \( \{P_1, P_2\} \), the network \( \mathcal{N}_{12} \) has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( \{P_1, P_2\} \).

**Note:** For any given positive integer \( n \), if \( l_2 > l_1 + n \), then \( \mathcal{N}_{12} \) has that property that the set of characteristics over which it has a 3-dimensional vector linear solution is arbitrarily larger than the set of characteristics over which it has a 2-dimensional vector linear solution.

Next, we show two classes of network in which with increasing message dimension the set of characteristics over which a vector linear solution exists get smaller.

**Theorem 10.** For any set of primes \( P \), there exists a network which has a 2-dimensional vector linear solution over all finite fields, but has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( P \).

Proof: Let \( P = \{p_1, p_2, \ldots, p_l\} \). In \( \mathcal{N}_1 \) take \( q = p_1 \times p_2 \times \cdots \times p_l \). Proof of Theorem 8 already describes that \( \mathcal{N}_1 \) has a 2-dimensional vector linear solution over all finite fields. Lemma 1 shows that \( \mathcal{N}_1 \) has a 3-dimensional vector linear solution if and only if the characteristic divides \( q \), which can only happen if the characteristic belongs to \( P \).

**Theorem 11.** For any two sets of prime numbers \( P_1 = \{p_1, p_2, \ldots, p_l\} \) and \( P_2 = \{p_1', p_2', \ldots, p_{l'}\} \), there exists a network which has a 2-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( \{P_1, P_2\} \), but has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( P_2 \).

Proof: Consider the network \( \mathcal{N}_{12} \) for \( q = p_1 \times p_2 \times \cdots \times p_l \times p_1' \times p_2' \times \cdots \times p_{l'} \) and \( q' = p_1 \times p_2 \times \cdots \times p_l \times p_1' \times p_2' \times \cdots \times p_{l'} \). As explained in the proof of Theorem 8, \( \mathcal{N}_1 \) has a 2-dimensional vector linear solution over all finite fields. Lemma 5 shows that \( \mathcal{N}_2 \) has 2-dimensional vector linear solution if and only if the characteristic of the finite field divides \( q' \), and that can only happen if and only if the characteristic belongs to \( \{P_1, P_2\} \). Hence, \( \mathcal{N}_{12} \) has a 2-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( \{P_1, P_2\} \).
As per Lemma 1 and our value of \( q \), \( N_1 \) has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( P_2 \). And as argued in Theorem 10, \( N_2 \) has a vector linear solution over all finite fields. Hence, \( N_{12} \) has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( P_2 \).

**Note:** For any given positive integer \( n \), if \( l_1 \) is such that \( l_1 > l_2 + n \), then \( N_{12} \) has that property that the set of characteristics over which it has a 2-dimensional vector linear solution is arbitrarily larger than the set of characteristics over which it has a 3-dimensional vector linear solution.

**Theorem 12.** There exists a network which has a 2-dimensional vector linear solution and a 3-dimensional vector linear solution, but has no 5-dimensional vector linear solution.

**Proof:** We show a whole class of such networks. Let \( P_1 = \{ p_1, p_2, \ldots, p_{l_1} \} \) and \( P_2 = \{ q_1, q_2, \ldots, q_{l_2} \} \) be two sets of primes such that \( P_1 \cap P_2 = \emptyset \). Consider the network \( N_{12} \) for \( q = p_1 \times p_2 \times \cdots \times p_{l_1} \) and \( q' = q_1 \times q_2 \times \cdots \times q_{l_2} \). Similar to the proofs of Theorems 9 and 11, it can be shown that \( N_{12} \) has a 2-dimensional vector linear solution over if and only if the characteristic belongs to \( P_2 \), and has a 3-dimensional vector linear solution over if and only if the characteristic belongs to \( P_1 \).

Lemma 1 shows that \( N_1 \) has a 5-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( P_1 \) (because for our choice of \( q \) the characteristic divides \( q \) if and only if it belongs to \( P_1 \)). Lemma 6 shows that \( N_2 \) has a 5-dimensional vector linear solution if and only if the characteristic of the finite field belongs to \( P_2 \) (because for our choice of \( q' \) the characteristic divides \( q' \) if and only if it belongs to \( P_2 \)). Since, \( P_1 \cap P_2 = \emptyset \), \( N_{12} \) does not have a 5-dimensional vector linear solution over any finite field.

This shows that, in general, the following theorem holds.

**Theorem 13.** For a network, existences of an \( m_1 \)-dimensional vector linear solution and an \( m_2 \)-dimensional vector linear solution implies the existence of an \( (m_1 + m_2) \)-dimensional vector linear solution if and only if the \( m_1 \) and \( m_2 \) dimensional vector linear solutions exists over the same finite field.

**Theorem 14.** For any prime number \( p \), there exists a network which has a scalar linear solution over a finite field if and only if the size of the finite field is a power of \( p \), but has a scalar linear solution over a non-commutative ring of size 16.

**Proof:** We show that the network \( N_1 \) for \( q = p \) (shown in Section III-D) is such a network. Lemma 1 shows that \( N_1 \) has a scalar linear solution if and only if the characteristic of the finite field divides \( p \).

Linear network coding over rings has been defined in [5] and [6]. In [6], it has been shown that all networks that has a vector linear solution over a finite field, also has a scalar linear solution over some ring. The authors also showed that the M-network has a scalar linear solution over a non-commutative ring of size 16. On the other hand, from the proof of the ‘if’ part of Lemma 1 it can be seen that only addition and subtraction operations required to achieve a scalar linear solution of the Char-\( q - s \). Hence the same solution would also work over any ring. Since both the M-network and the Char-\( q - s \) network have a scalar linear solution over the non-commutative ring of size 16, \( N_1 \) also has a scalar linear solution over the same ring.

**Note:** For any given positive integer \( n \), if \( p \) is selected such that \( p > n \), then for \( q = p \) the network \( N_1 \) has that property that the size of the alphabet required to achieve a scalar linear solution over a finite field is arbitrarily larger than the size of the alphabet required to achieve a scalar linear solution over a non-commutative ring.

**V. Conclusion**

Our research shows that the answer to these two questions: (i) for what message dimensions a vector linear solution exists, and (ii) for what values of the characteristic of the finite field a vector linear solution exists, in general cannot be answered separately. Recently it has been shown in [7] that linear coding capacity is dependent only on the characteristic of the finite field. This paper shows that for different message dimensions, the rate prescribed by the linear coding capacity may be achieved over different sets of characteristics. For example, the linear coding capacity of the network \( N_1 \) is 1 and it can be achieved over all finite fields. But we now know that the rate 1 can be achieved over all finite fields if and only if message dimension is even.

We also show that rings are superior to finite fields when the objective is to achieve a scalar linear solution over the least sized alphabet. We leave it an open problem that whether rings are also superior when the objective is to achieve a vector linear solution. That is, whether there exists a network which for any positive integer \( d \), has a \( d \)-dimensional vector linear solution over a finite field only if the size of the finite field is greater than or equal to \( n \), but has \( d \)-dimensional vector linear solution over a non-commutative ring whose size is strictly less than \( n \).

**Appendix A**

**Proof of the ‘only if’ part of Lemma 1**

**Proof:** Let the message carried by the edge \( e_i \) be denoted by \( y_{e_i} \) for \( 1 \leq i \leq q + 3 \). First consider the ‘only if’ part. Then, there exist \( d \times d \) matrices: \( A_i \) for \( 1 \leq i \leq q + 3 \); \( M_i \) for \( 1 \leq i \leq q + 1 \), \( i = q + 3 \), \( W_{(j,i)} \) for \( 2 \leq j \leq q + 3 \), for the following network.
2 \leq i \leq q+2, j \neq i, \text{ such that }
\begin{align*}
y_{e_1} &= M_1 x_1 + A_1 s \\
y_{e_2} &= M_2 x_1 + \sum_{i=3}^{q+2} W_{(2,i)} x_i \\
y_{e_3} &= M_3 x_1 + W_{(3,2)} x_2 + \sum_{i=4}^{q+2} W_{(3,i)} x_i \\
\text{for } 4 \leq j \leq q+1: \quad y_{e_j} &= M_j x_1 + A_j s + \sum_{i=2, i \neq j}^{q+2} W_{(j,i)} x_i \\
y_{e_{q+2}} &= (A_{q+2}) s + \sum_{i=2}^{q+1} W_{(q+2,i)} x_i \\
y_{e_{q+3}} &= M_{q+3} x_1 + A_{q+3} s + \sum_{i=2}^{q+2} W_{(q+3,i)} x_i
\end{align*}

Due to the demands of the terminal $r_1$, from equations (8) and (15), there exists $d \times d$ matrices $T_{11}$ and $T_{12}$ such that
\[(T_{11}) y_{e_1} + (T_{12}) y_{e_{q+3}} + \sum_{j=2}^{q+1} (T'_{1j}) x_j = x_{q+2}\]

So we must have:
\begin{align*}
T_{11} M_1 + T_{12} M_{q+3} &= 0 \\
T_{11} A_1 + T_{12} A_{q+3} &= 0 \\
T_{12} W_{(q+3,q+2)} &= I
\end{align*}

Due to the demands of terminal $r_2$, from equations (9) and (13), there exists $d \times d$ matrices $T_{21}$ and $T_{22}$ such that
\[(T_{21}) y_{e_2} + (T_{22}) y_{e_{q+3}} + (T'_{2}) s = x_2\]

So we must have:
\begin{align*}
T_{21} M_2 + T_{22} M_{q+3} &= 0 \\
T_{22} W_{(q+3,2)} &= I \\
\text{for } 3 \leq i \leq q + 2: \quad T_{21} W_{(2,i)} + T_{22} W_{(q+3,i)} &= 0
\end{align*}

Due to the demands of terminal $r_3$, from equations (10) and (13) there exists $d \times d$ matrices $T_{31}$ and $T_{32}$ such that
\[(T_{31}) y_{e_3} + (T_{32}) y_{e_{q+3}} + (T'_{3}) s = x_3\]

So we must have:
\begin{align*}
T_{31} M_3 + T_{32} M_{q+3} &= 0 \\
T_{31} W_{(3,2)} + T_{32} W_{(q+3,2)} &= 0 \\
T_{32} W_{(q+3,3)} &= I \\
\text{for } 4 \leq i \leq q + 2: \quad T_{31} W_{(3,i)} + T_{32} W_{(q+3,i)} &= 0
\end{align*}

Due to the demands of the terminal $r_j$ for $4 \leq j \leq q+1$, from equations (11) and (13), there exists $d \times d$ matrices $T_{j1}$ and $T_{j2}$ such that
\[(T_{j1}) y_{e_j} + (T_{j2}) y_{e_{q+3}} = x_j\]

So we must have:
\begin{align*}
T_{j1} M_j + T_{j2} M_{q+3} &= 0 \\
T_{j1} A_j + T_{j2} A_{q+3} &= 0 \\
T_{j2} W_{(q+3,j)} &= I \\
\text{for } 2 \leq i \leq q + 2, i \neq j: \quad T_{j1} W_{(j,i)} + T_{j2} W_{(q+3,i)} &= 0
\end{align*}
Due to the demands of the terminal \( r_{q+2} \), from equations (12) and (13), there exists \( d \times d \) matrices \( T_{(q+2)1} \) and \( T_{(q+2)2} \) such that
\[
(T_{(q+2)1})y_{e_{q+2}} + (T_{(q+2)2})y_{e_{q+3}} + (T'_{q+2})x_1 = x_{q+2}
\] (32)
So we must have:
\[
T_{(q+2)1}A_{q+2} + T_{(q+2)2}A_{q+3} = 0
\] (33)
for \( 2 \leq i \leq q + 1 : \ T_{(q+2)1}W_{(q+2,i)} + T_{(q+2)2}W_{(q+3,i)} = 0
\] (34)
\[
T_{(q+2)2}W_{(q+3,q+2)} = I
\] (35)
Due to the demands of the terminal \( r_{q+3} \), from equations (19), (22), there exists \( d \times d \) matrices \( Z_i \) for \( 1 \leq i \leq q + 2 \) such that
\[
(Z_1)y_{e_1} + (Z_2)y_{e_2} + \cdots + (Z_{q+1})y_{e_{q+1}} = x_1
\] (36)
So we must have:
\[
Z_1M_1 + Z_2M_2 + \cdots + Z_{q+1}M_{q+1} = I
\] (37)
\[
Z_1A_1 + Z_2A_2 + \cdots + Z_{q+2}A_{q+2} = 0
\] (38)
for \( 2 \leq i \leq q + 2 : \ \sum_{j=2,j\neq i}^{q+2} Z_jW_{(j,i)} = 0
\] (39)
From equations (17), (20), (25), (30) and (35) we get: \( T_{i2} \) is invertible for \( 1 \leq i \leq q + 2 \, , \, \) and \( W_{(q+3,i)} \) is invertible for \( 2 \leq i \leq q + 2 \). Then, from equations (21), (24), (26), (31) and (34): \( T_{i1} \) is invertible for \( 1 \leq i \leq q + 2 \, , \) and \( W_{(j,i)} \) is invertible for \( 2 \leq j, i \leq q + 2 \, , \, j \neq i \).

From equations (15), (19), (23) and (28) we have:
\[
\text{for } 1 \leq i \leq q + 1 \, : \, M_i = -T_{i1}^{-1}T_{i2}M_{q+3}
\] (40)
Substituting equation (40) in equation (37) we get:
\[
(Z_1T_{i1}^{-1}T_{12} + Z_2T_{21}^{-1}T_{22} + \cdots + Z_{q+1}T_{(q+1)1}^{-1}T_{(q+1)2})M_{q+3} = -I
\] (41)
From equations (16), (29), and (33) we have:
\[
\text{for } i = 1 \, \text{and } 4 \leq i \leq q + 2 \, : \, A_i = -T_{i1}^{-1}T_{i2}A_{q+3}
\] (42)
Substituting equation (42) in equation (38) we get:
\[
(Z_1T_{i1}^{-1}T_{12} + Z_2T_{31}^{-1}T_{32} + \cdots + Z_{q+2}T_{(q+2)1}^{-1}T_{(q+2)2})A_{q+3} = 0
\] (43)
From equations (21), (24), (26), (31) and (34) we have:
\[
\text{for } 2 \leq j \leq q + 2 \, , \, 2 \leq i \leq q + 2 \, , \, j \neq i \, : \, W_{(j,i)} = -T_{j1}^{-1}T_{j2}W_{(q+3,i)}
\] (44)
Substituting equation (44) in equation (39), for \( 2 \leq i \leq q + 2 \) we have:
\[
\sum_{j=2,j\neq i}^{q+2} Z_jT_{j1}^{-1}T_{j2}W_{(q+3,i)} = 0
\] (45)
Since \( W_{(q+3,i)} \) for \( 2 \leq i \leq q + 2 \) has been already shown to be invertible, for \( 2 \leq i \leq q + 2 \) we must have:
\[
\sum_{j=2,j\neq i}^{q+2} Z_jT_{j1}^{-1}T_{j2} = 0
\] (46)
Expanding equation (46) for each value of \( 2 \leq i \leq q + 2 \) we have:
\[
Z_3T_{31}^{-1}T_{32} + Z_4T_{41}^{-1}T_{42} + \cdots + Z_{q+2}T_{(q+2)1}^{-1}T_{(q+2)2} = 0
\] (47)
\[
Z_2T_{21}^{-1}T_{22} + Z_4T_{41}^{-1}T_{42} + \cdots + Z_{q+2}T_{(q+2)1}^{-1}T_{(q+2)2} = 0
\] (48)
\[
\vdots
\]
\[
Z_2T_{21}^{-1}T_{22} + Z_3T_{31}^{-1}T_{32} + Z_4T_{41}^{-1}T_{42} + \cdots + Z_{q+1}T_{(q+1)1}^{-1}T_{(q+1)2} = 0
\] (50)
Adding the above \( q + 1 \) equations shown in equations (47)-(50), i.e. by the operation \( \sum_{i=2}^{q+2} \sum_{j=2,j\neq i}^{q+2} Z_jT_{j1}^{-1}T_{j2} \) we have:
\[
q(Z_2T_{21}^{-1}T_{22} + Z_3T_{31}^{-1}T_{32} + Z_4T_{41}^{-1}T_{42} + \cdots + Z_{q+2}T_{(q+2)1}^{-1}T_{(q+2)2}) = 0
\] (51)
Since the characteristic of the finite field does not divide $q$, we must have $q \neq 0$ in the finite field. Then, from equation (51) we must have:

$$Z_2T_{21}^{-1}T_{22} + Z_3T_{31}^{-1}T_{32} + Z_4T_{41}^{-1}T_{42} + \cdots + Z_{q+2}T_{(q+2)1}^{-1}T_{(q+2)2} = 0$$  \hspace{1cm} (52)

For each value of $2 \leq i \leq q + 2$, subtracting equation (46) from (52) we get:

$$Z_jT_{jj}^{-1}T_{j2} = 0$$  \hspace{1cm} (53)

Substituting the values set by equation (53) in equation (41) we get:

For each value of $i$, we must have:

$$\rho_P^{3}$$

the components of $v$ that delineates this connection. Extensively used this connection to establish some of the theorems. So, next we reproduce some preliminaries from linear solution if and only if a discrete polymatroid with certain properties can be constructed from the network [24]. We have the set of sources be $S$, the set of non-source nodes be $V$, and the set of edges be $E$. The network $N$ has a $d$-dimensional vector linear solution over $\mathbb{F}_q$ if and only if there exists a discrete polymatroid $D$ with rank function $\rho$ and ground set $G$, such that $D$ representable over $\mathbb{F}_q$, and there exists a map $f : \{S \cup E\} \rightarrow G$ that satisfies the following conditions:

**Definition 2** (Definition 2, [24]). Let $\rho : 2^G \rightarrow \mathbb{Z}_{\geq 0}$ such that

- $P_1 \rho(\emptyset) = 0$
- $P_2 \rho(A) \leq \rho(B)$ if $A \subseteq B$
- $P_3 \rho(A) + \rho(B) \geq \rho(A \cup B) + \rho(A \cap B)$

Let $D = \{x \in \mathbb{Z}_{\geq 0}^n \mid \rho(A), \forall A \subseteq G\}$. Then $D$ is a discrete polymatroid with rank function $\rho$ and ground set $G$.

**Definition 3** (Definition 3, [24]). A discrete polymatroid $D$ with rank function $\rho$ and ground set $G$ is said to be representable over $\mathbb{F}_q$ if for each element $i$ of $G$, there exists a vector subspace $V_i$ of a vector space $V$ over $\mathbb{F}_q$ such that $\dim(\sum_{i \in X} V_i) = \rho(X)$ for all $X \subseteq G$.

Let $e_{in}$ be a $n$ length vector whose $i^{th}$ component is one and all other components are zero. For any node $v$, let $In(v)$ denote the set of edges whose head node is $v$, and $Out(v)$ denote the set of edges whose tail node is $v$. The following theorem combines Definition 7 and Theorem 1 of [24].

**Theorem 15.** [Definition 7 and Theorem 1, [24]] For a network $N$ let the set of sources be $S$, the set of non-source nodes be $V$, and the set of edges be $E$. The network $N$ has a $d$-dimensional vector linear solution over $\mathbb{F}_q$ if and only if there exists a discrete polymatroid $D$ with rank function $\rho$ and ground set $G$, such that $D$ representable over $\mathbb{F}_q$, and there exists a map $f : \{S \cup E\} \rightarrow G$ that satisfies the following conditions:

- **D1** $f$ is one-to-one on $S$.
- **D2** $\sum_{i \in f(S)} d_{i\in} \in D$.
- **D3** $\forall s \in S, \rho(f(s)) = d$, and $\forall e \in E, \rho(f(e)) \leq d$.
- **D4** $\rho(f(In(v))) = \rho(f(In(v)) \cup Out(v)))$, $\forall v \in V$.

Let $S$ be the set of sources of a network which has a $d$-dimensional vector linear solution, and let $D$ be the corresponding discrete polymatroid as per Theorem 15. Say $S_1$ and $S_2$ are two subsets of $S$. Let $f$ be the function that maps the sources and edges of the network to the ground set of $D$, and $\rho$ be the rank function of $D$. Define $g = \rho \circ f$. 

**APPENDIX B**

**Discrete Polymatroids**

A Discrete Polymatroid is an abstract mathematical structure. It has been shown that a network has a $d$-dimensional vector linear solution if and only if a discrete polymatroid with certain properties can be constructed from the network [24]. We have extensively used this connection to establish some of the theorems. So, next we reproduce some preliminaries from [24] that delineates this connection.

Define $G = \{1, 2, \ldots, n\}$, $\mathbb{Z}_{\geq 0}$ as the set of non-negative integers, and $\mathbb{Z}_{\geq 0}^n$ as the set of all $n$ length vectors over $\mathbb{Z}_{\geq 0}$. For a vector $v$, let $v(A)$ be the vector having only the components indexed by the elements of $A$, and $|v(A)|$ denote the sum of the components of $v(A)$.
Lemma 16. \( g(S_1, S_2) = g(S_1) + g(S_2) \).

Proof: For simplicity, we prove for the particular case when \( S_1 = \{s_1, s_2\} \) and \( S_2 = \{s_3, s_4\} \), and the other possibilities can be proved similarly. Note that according [D1] of Theorem [15] all sources are mapped to different elements. Now, if the ground set of \( \mathbb{D} \) is \( \{1, 2, \ldots, n\} \), then according to [D2] of Theorem [15] the vector \( v = \sum_{i \in f(S)} d_{i,n} \) is in \( \mathbb{D} \). Hence, from Definition [2] we have \(|v(\{f(s_1), f(s_2), f(s_3), f(s_4)\})| \leq \rho(\{f(s_1), f(s_2), f(s_3), f(s_4)\}) \). Since \(|v(\{f(s_1), f(s_2)\})| = 4d \), this implies: \( 4d \leq \rho(\{f(s_1), f(s_2), f(s_3), f(s_4)\}) \). Also, from [D3] of Theorem [15] we have: \( \rho(f(s_1)) = \rho(f(s_2)) = \rho(f(s_3)) = \rho(f(s_4)) = d \). So, \( \rho(f(s_1)) + \rho(f(s_2)) + \rho(f(s_3)) + \rho(f(s_4)) \leq \rho(\{f(s_1), f(s_2), f(s_3), f(s_4)\}) \).

Lemma 17. If \( C \subseteq B \), then \( g(A, B) - g(A, C) \leq g(B) - g(C) \).

Proof:

\[
g(A, C) + g(B) \geq g(A, B, C) + g(C) \quad \text{[from [P4] of Definition [2]]}
\]

or, \( g(A, C) + g(B) \geq g(A, B) + g(C) \) [as \( C \subseteq B \)]

or, \( g(B) - g(C) \geq g(A, B) - g(A, C) \)

Lemma 18. Let \( E_1 \) and \( E_2 \) be set of edges such that \( g(S_1, E_1) = g(S_1) \) and \( g(S_2, E_2) = g(S_2) \). If \( \tilde{S}_1 \) is a subset of \( S_1 \) and \( \tilde{S}_2 \) is a subset of \( S_2 \), then \( g(S_1, E_1) + g(\tilde{S}_2, E_2) = g(\tilde{S}_1, E_1, \tilde{S}_2, E_2) \).

Proof: Note that, due to Lemma [16] we have:

\[
g(S_1, E_1) + g(S_2, E_2) = g(S_1, S_2, E_2) \quad (58)
\]

\[
g(S_2, E_2) - g(\tilde{S}_2, E_2)
= g(S_1, E_1, S_2, E_2) - g(S_1, E_1) - g(\tilde{S}_2, E_2) \quad \text{[using equation (58)]}
\leq g(S_1, E_1, S_2, E_2) - g(S_1, E_1, \tilde{S}_2, E_2)
\leq g(S_2, E_2) - g(\tilde{S}_2, E_2) \quad \text{[taking} \ A = \{S_1 \cup E_1\} \text{in Lemma [17]}\)

From equation [59] we have:

\[
g(S_1, E_1, S_2, E_2) - g(S_1, E_1, \tilde{S}_2, E_2) = g(S_2, E_2) - g(\tilde{S}_2, E_2) \quad (60)
\]

\[
g(S_1, E_1) - g(S_1, E_1)
= g(S_1, E_1, S_2, E_2) - g(S_2, E_2) - g(S_1, E_1) \quad \text{[using equation (58)]}
\leq g(S_1, E_1, S_2, E_2) - g(S_1, E_1, \tilde{S}_2, E_2) \quad \text{[applying [P3] of Definition [2]]}
\leq g(S_1, E_1, \tilde{S}_2, E_2) - g(S_1, E_1, \tilde{S}_2, E_2) \quad \text{[taking} \ A = S_2 \setminus \tilde{S}_2 \text{in Lemma [17]}\)
\leq g(S_1, E_1) - g(S_1, E_1) \quad \text{[taking} \ A = \tilde{S}_2 \cup E_2 \text{in Lemma [17]}\)

From equation [61] we have:

\[
g(S_1, E_1, \tilde{S}_2, E_2) - g(S_1, E_1, S_2, E_2) = g(S_1, E_1) - g(S_1, E_1) \quad (62)
\]

Adding equations [60] and [62] we get:

\[
g(S_1, E_1, S_2, E_2) - g(S_1, E_1, \tilde{S}_2, E_2) + g(S_1, E_1, \tilde{S}_2, E_2) - g(S_1, E_1, \tilde{S}_2, E_2)
= g(S_2, E_2) - g(\tilde{S}_2, E_2) + g(S_1, E_1) - g(S_1, E_1)
\]

or, \( g(S_1, E_1, S_2, E_2) - g(S_1, E_1, \tilde{S}_2, E_2) = g(S_1, E_1, S_2, E_2) - g(\tilde{S}_2, E_2) - g(S_1, E_1) \)

or, \( g(S_1, E_1, \tilde{S}_2, E_2) = g(\tilde{S}_2, E_2) + g(S_1, E_1) \)

\]
Appendix C
Proof of Lemma 3

Proof: Let \( f \) be the function that maps the network \( \mathcal{N}_1 \) to a discrete polymatroid \( D_1 \) conforming to the conditions given in Theorem 15. Let \( \rho \) be the rank function of \( D_1 \), and let \( g = \rho \circ f \). Consider the ‘only if’ part. We show that if the characteristic of the finite field does not divide \( q \), then \( \mathcal{N}_1 \) has no odd dimensional vector linear solution. Since the characteristic either divides \( q \) or does not divide \( q \), proving the this statement would prove the ‘only if’ part. Let’s assume that over a finite field whose characteristic does not divide \( q \), \( \mathcal{N}_1 \) has a \( d \)-dimensional vector linear solution for some odd number \( d \). Let the edges \( (u_i, v_j) \) be denoted by \( e_{ij} \) for \( i = 1, 2 \) and \( j = 1, 2, 3 \). The demands of the terminals are shown in Fig. 3. Due to the demands of terminal \( t_1 \) we get the following:

\[
g(e_{11}, a) + g(e_{22}, x) = g(e_{11}, a, e_{22}, x) \quad \text{[from Lemma 18]}
\]

\[
ge(e_{11}, a, e_{22}, x, (v_3, t_1)) = g(e_{11}, e_{22}, (v_3, t_1)) \quad \text{[due to demands of \( t_1 \)]}
\]

\[
ge(e_{11}) + g(e_{22}) + g((v_3, t_1)) \leq 3d \quad \text{[using [P3] of Definition 2 and [D3] of Theorem 15]} \tag{63}
\]

Similar to equation (63), due to the demands of \( t_2 \) and \( t_3 \) we have the following equations.

\[
g(e_{11}, a) + g(e_{22}, y) \leq 3d \tag{64}
\]

\[
g(e_{11}, b) + g(e_{22}, x) \leq 3d \tag{65}
\]

Since the characteristic of the finite field does not divide \( q \), from Lemma 1 we know that the message carried by \( e_1 \) is not a function of \( y \).

\[
g(e_{11}, a) + d + d \geq g(e_{11}, a) + g(e_{22}) + g((v_3, t_4))
\]

\[
\geq g(e_{11}, a, e_{22}, (v_3, t_4))
\]

\[
= g(e_{11}, a, e_{22}, (v_3, t_4), e_1) \quad \text{[since information carried by \( e_1 \) is function of only \( a \)]}
\]

\[
= g(e_{11}, a, e_{22}, (v_3, t_4), e_1, b, y) \quad \text{[due to demands of \( t_4 \)]}
\]

\[
\geq g(e_{11}, a, e_{22}, b, y)
\]

\[
= g(e_{11}, a, b) + g(e_{22}, y) \quad \text{[from Lemma 18]}
\]

\[
= 2d + g(e_{22}, y) \tag{66}
\]

From equation (66), we get that

\[
g(e_{11}, a) \geq g(e_{22}, y) \tag{67}
\]

We know:

\[
4d = g(a, b, x, y)
\]

\[
= g(a, b, x, y, e_{11}, e_{13}, e_{22}, e_{23})
\]

\[
= g(e_{11}, e_{13}, e_{22}, e_{23})
\]

\[
\leq g(e_{11}) + g(e_{13}) + g(e_{22}) + g(e_{23})
\]

\[
\leq 4d \quad \text{[[D3] of Theorem 15]} \tag{68}
\]

From equation (68) we get:

\[
g(e_{11}) = g(e_{13}) = g(e_{22}) = g(e_{23}) = d \tag{69}
\]

We also have:

\[
g(e_{11}, a) + g(e_{11}, b)
\]

\[
\geq g(e_{11}, a, b) + g(e_{11}) \quad \text{[using [P3] of Definition 2]}
\]

\[
= g(a, b) + g(e_{11})
\]

\[
= 3d \quad \text{[we used equation 69]} \tag{70}
\]

Similar to equation (70), we have:

\[
g(e_{22}, x) + g(e_{22}, y) \geq 3d \tag{71}
\]

Adding equations (63) and (64) we get:

\[
2g(e_{11}, a) + g(e_{22}, x) + g(e_{22}, y) \leq 6d
\]

or, \( 2g(e_{11}, a) \leq 3d \) \quad \text{[substituting equation 71]} \tag{72}

or, \( g(e_{11}, a) \leq \frac{3d}{2} \)
Adding equations (63) and (65) we get:
\[ g(e_{11}, a) + g(e_{11}, b) + 2g(e_{22}, x) \leq 6d \]
or, \[ 2g(e_{22}, x) \leq 3d \] \[ \text{[substituting equation (70)]} \]
or, \[ g(e_{22}, x) \leq \frac{3d}{2} \] \[ \text{(73)} \]
From equation (67) we have:
\[ g(e_{22}, y) \leq \frac{3d}{2} \] \[ \text{(74)} \]
Since \( d \) is an odd positive integer, let \( d = 2n - 1 \) where \( n \) is a positive integer. Then, from equations (73) and (74) we have:
\[ g(e_{22}, x) \leq \frac{3(2n - 1) - 2}{2} = 3n - \frac{3}{2} = 3n - 2 + \frac{1}{2} \] \[ \text{(75)} \]
\[ g(e_{22}, y) \leq \frac{3(2n - 1) - 2}{2} = 3n - \frac{3}{2} = 3n - 2 + \frac{1}{2} \] \[ \text{(76)} \]
Since the rank function \( g() \) is integer valued by Definition 2, from equations (75) and (76) we have:
\[ g(e_{22}, x) \leq 3n - 2 \] \[ \text{(77)} \]
\[ g(e_{22}, y) \leq 3n - 2 \] \[ \text{(78)} \]
Substituting values from equation (77) and (78) in equation (71) we get:
\[ 6n - 4 \geq 3d = 3(2n - 1) = 6n - 3 \] \[ \text{(79)} \]
Equation (79) results in \( 3 \geq 4 \), which is a contradiction.

We now show the ‘if’ part of the proof. We show that \( N_1 \) has a scalar linear solution (thereby having a vector linear solution for any message dimension) if the characteristic of the finite field divides \( q \). Let the message vector generated by a source be denoted by the same label as the source. In our solution, the edges \( e_i \) for \( 1 \leq i \leq q + 3 \) carry the messages as indicated by equations (1)-(6) with \( x_1 \) replaced by \( a \) and \( s \) replaced by \( y \). Then, the terminals \( r_1 \) to \( r_{q+3} \) can retrieve its desired information (as described in Lemma 2). Now, in the M-network part, let \( e_{11} \) carry \( a \), \( e_{13} \) carry \( b \), \( e_{22} \) carry \( x \), and \( e_{23} \) carry \( y \). Then, it can be easily seen that terminals \( t_1, t_2 \) and \( t_3 \) can retrieve its desired information. The terminal \( t_4 \) receives \( a \) from \( e_{11}, b \) from \( (v_3, t_4) \), \( a + y \) from \( e_1 \), and as a result it can deduce \( y \) as well (by subtracting \( a \) from \( a + y \)).

**APPENDIX D**

**PROOF OF LEMMAS 4, 5, AND 6**

We first develop some general equations that hold for the network \( N_2 \). Let \( f \) be the function that maps the sources and edges of the network \( N_2 \) to the ground set \( G \) of a discrete polymatroid \( D_2 \) with rank function \( \rho \) such that \( N_2 \) has a \( d \)-dimensional vector linear solution over \( F_q \) if and only if \( D_2 \) is representable over \( F_q \) and \( f \) follows the conditions given in Theorem 15. Now let \( g = \rho \circ f \). Let the edge \((\bar{u}_i, \bar{v}_j)\) for \( 1 \leq i \leq 3 \) and \( 1 \leq j \leq 5 \) be denoted by \( \bar{e}_{ij} \). The demands of the terminals are shown in Fig. 4.

\[
g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{33}, \bar{x})
= g(\bar{e}_{11}, \bar{a}, \bar{e}_{22}, \bar{r}, \bar{e}_{33}, \bar{x}) \quad \text{[from Lemma 18]}
\leq g(\bar{e}_{11}, \bar{a}, \bar{e}_{22}, \bar{r}, \bar{e}_{33}, \bar{x}, (\bar{v}_4, \bar{t}_1), (\bar{v}_5, \bar{t}_1))
= g(\bar{e}_{11}, \bar{e}_{22}, \bar{e}_{33}, (\bar{v}_4, \bar{t}_1), (\bar{v}_5, \bar{t}_1)) \quad \text{[due to demands of \( \bar{t}_1 \)]}
\leq 5d \quad \text{[from [D3] of Theorem 15]} \quad \text{(80)}
\]
Similar to equation (80), we have the following equations:

\[ g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{33}, \bar{y}) \leq 5d \quad \text{[due to } \bar{t}_2]\] (81)

\[ g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{33}, \bar{z}) \leq 5d \quad \text{[due to } \bar{t}_3]\] (82)

\[ g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{33}, \bar{x}) \leq 5d \quad \text{[due to } \bar{t}_4]\] (83)

\[ g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{33}, \bar{y}) \leq 5d \quad \text{[due to } \bar{t}_5]\] (84)

\[ g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{33}, \bar{z}) \leq 5d \quad \text{[due to } \bar{t}_6]\] (85)

\[ g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{33}, \bar{x}) \leq 5d \quad \text{[due to } \bar{t}_{10}]\] (86)

\[ g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{33}, \bar{y}) \leq 5d \quad \text{[due to } \bar{t}_{11}]\] (87)

\[ g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{33}, \bar{z}) \leq 5d \quad \text{[due to } \bar{t}_{12}]\] (88)

\[ g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{33}, \bar{x}) \leq 5d \quad \text{[due to } \bar{t}_{13}]\] (89)

\[ g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{33}, \bar{y}) \leq 5d \quad \text{[due to } \bar{t}_{14}]\] (90)

\[ g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{33}, \bar{z}) \leq 5d \quad \text{[due to } \bar{t}_{15}]\] (91)

\[ g(\bar{e}_{11}, \bar{c}) + g(\bar{e}_{22}, \bar{w}) + g(\bar{e}_{33}, \bar{z}) \leq 5d \quad \text{[due to } \bar{t}_{27}]\] (92)

It can be seen that due to terminals \( \bar{t}_1, \bar{t}_{14}, \) and \( \bar{t}_{27}, \) all of the source messages are to be retrieved from

\[ 9d = g(\bar{a}, \bar{b}, \bar{c}, \bar{r}, \bar{s}, \bar{w}, \bar{x}, \bar{y}, \bar{z}) \quad \text{[from Lemma [16] and [D3] of Thm. [15]}\]

\[ = g(\bar{a}, \bar{b}, \bar{c}, \bar{r}, \bar{s}, \bar{w}, \bar{x}, \bar{y}, \bar{z}, \bar{f}_{11}, \bar{f}_{14}, \bar{f}_{22}, \bar{f}_{24}, \bar{f}_{25}, \bar{f}_{33}, \bar{f}_{34}, \bar{f}_{35})\]

\[ = g(\bar{e}_{11}, \bar{e}_{14}, \bar{e}_{15}, \bar{e}_{22}, \bar{e}_{24}, \bar{e}_{25}, \bar{e}_{33}, \bar{e}_{34}, \bar{e}_{35}) \quad \text{[due to demands of } \bar{t}_1, \bar{t}_{14}, \text{ and } \bar{t}_{27}]\]

\[ \leq \sum_{i=1,2,3,j=4,5} g(\bar{e}_{ij}) \quad \text{[from [P3] of Definition [2]}\]

\[ \leq 9d \quad \text{[from [D3] of Theorem [15]}\]

\[ g(\bar{e}_{ij}) = d \text{ for } i = 1, 2, 3 \text{ and } j = i, 4, 5 \quad \text{(93)}\]

\[ g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{11}, \bar{c}) \geq g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{11}) + g(\bar{e}_{11}, \bar{c}) \quad \text{[applying [P3] of Definition [2]}\]

\[ g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{11}, \bar{b}), \bar{c}, \bar{c}) + 2g(\bar{e}_{11}) \quad \text{[applying [P3] of Definition [2]}\]

\[ = g(\bar{a}, \bar{b}, \bar{c}) + 2g(\bar{e}_{11}) \]

\[ = 5d \quad \text{[using equation [93]}\]

We also have the following inequalities:

\[ g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{22}, \bar{w}) \geq 5d \quad \text{(94)}\]

\[ g(\bar{e}_{33}, \bar{x}) + g(\bar{e}_{33}, \bar{y}) + g(\bar{e}_{33}, \bar{z}) \geq 5d \quad \text{(95)}\]

We prove one of equations (94)-(95) and the rest can be proved similarly.

Adding equations (94)-(95) we have:

\[ g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{11}, \bar{c}) + g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{22}, \bar{w}) + g(\bar{e}_{33}, \bar{x}) \]

\[ + g(\bar{e}_{33}, \bar{y}) + g(\bar{e}_{33}, \bar{z}) \geq 15d \quad \text{(96)}\]

or,

\[ (g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{33}, \bar{x})) + (g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{33}, \bar{y}) + g(\bar{e}_{11}, \bar{c}) \]

\[ + g(\bar{e}_{22}, \bar{w}) + g(\bar{e}_{33}, \bar{z}) \geq 15d \quad \text{(96)}\]

But as equations (80), (90) and (92) holds, from equation (96) we have:

\[ g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{33}, \bar{x}) = 5d \quad \text{(97)}\]

\[ g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{33}, \bar{y}) = 5d \quad \text{(98)}\]

\[ g(\bar{e}_{11}, \bar{c}) + g(\bar{e}_{22}, \bar{w}) + g(\bar{e}_{33}, \bar{z}) = 5d \quad \text{(99)}\]

Rearranging equation (96) and then using equations (81), (89), and (92) we have:

\[ g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{33}, \bar{y}) = 5d \quad \text{(100)}\]

\[ g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{33}, \bar{x}) = 5d \quad \text{(101)}\]
Rearranging equation (96) and then using equations (83), (87), and (92) we have:

\[ g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{33}, \bar{x}) = 5d \]  
(102)

\[ g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{33}, \bar{y}) = 5d \]  
(103)

Subtracting equations (97) from (102) we get:

\[ g(\bar{e}_{11}, \bar{a}) = g(\bar{e}_{11}, \bar{b}) \]  
(108)

Subtracting equations (97) from (102) we get:

\[ g(\bar{e}_{22}, \bar{r}) = g(\bar{e}_{22}, \bar{s}) \]  
(109)

Subtracting equations (97) from (100) we get:

\[ g(\bar{e}_{33}, \bar{x}) = g(\bar{e}_{33}, \bar{y}) \]  
(110)

Adding equations (97), (98), and (99) we have:

\[ \ldots + g(\bar{e}_{33}, \bar{z}) \) = 15d \]  
(111)

As equations (94)–(95) holds, we must have:

\[ g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{11}, \bar{b}) + g(\bar{e}_{11}, \bar{c}) = 5d \]  
(112)

\[ g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{22}, \bar{s}) + g(\bar{e}_{22}, \bar{w}) = 5d \]  
(113)

\[ g(\bar{e}_{33}, \bar{x}) + g(\bar{e}_{33}, \bar{y}) + g(\bar{e}_{33}, \bar{z}) = 5d \]  
(114)

Applying equations (108)–(110) to equations (112)–(114) we have:

\[ 2g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{11}, \bar{c}) = 5d \]  
(115)

\[ 2g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{22}, \bar{w}) = 5d \]  
(116)

\[ 2g(\bar{e}_{33}, \bar{x}) + g(\bar{e}_{33}, \bar{z}) = 5d \]  
(117)

Multiplying equation (82) by 2 and then adding to equation (99) we have:

\[ 2(g(\bar{e}_{11}, \bar{a}) + g(\bar{e}_{22}, \bar{r}) + g(\bar{e}_{33}, \bar{z}) = 15d \]  
or, \( 5d + 5d + 5g(\bar{e}_{33}, \bar{z}) \leq 15d \)  
[substituting equations (115) and (116)]

or, \( 3g(\bar{e}_{33}, \bar{z}) \leq \frac{5d}{3} \)

or, \( g(\bar{e}_{33}, \bar{z}) \leq \frac{5d}{3} \)  
(118)

We now derive one more equation that must hold if the characteristic of the finite field does not divide \( q' \). Note that in such a case the information carried by \( \bar{e}_1 \) in the Char-\( q' \) – \( \bar{x} \) network is independent of \( \bar{x} \) (from Lemma 1), and is a function of only \( \bar{a} \). Hence \( g(\bar{a}) = g(\bar{a}, \bar{e}_1) \). So due to the demands of terminal \( \bar{t}_{25} \) we have:

\[ g(\bar{e}_{11}, \bar{a}, \bar{c}) + g(\bar{e}_{22}, \bar{w}) + g(\bar{e}_{33}, \bar{x}) \]  
[from Lemma 18]

\[ g(\bar{e}_{11}, \bar{c}, \bar{w}, \bar{x}) \]  
[due to demands of \( \bar{t}_{25} \)]

\[ g(\bar{e}_{11}, \bar{c}, \bar{w}, \bar{x}) \]  
[due to demands of \( \bar{t}_{25} \)]

\[ g(\bar{e}_{11}, \bar{a}) \]  
(119)
Then we have
\[ g(\bar{e}_{11}, \bar{a}, \bar{c}) \geq 4d - g(\bar{e}_{11}, \bar{a}) \] (120)

Substituting equation (120) in equation (119) we have:
\[ g(\bar{e}_{11}, \bar{w}) + g(\bar{e}_{33}, \bar{x}) \leq 2g(\bar{e}_{11}, \bar{a}) \] (121)

A. Proof of Lemma 4

Proof: Note that equations (119)-(121) cannot be used as they hold only if the characteristic of the finite field divides \( q' \); and this lemma is to be shown to be true over all finite fields. Let us assume that the network has a scalar linear solution.

Since \( d = 1 \), and the rank function of a discrete polymatroid is always an integer, from equation (118) we have: \( g(\bar{e}_{33}, \bar{z}) \leq 1 \). Then from [P2] of Definition 2 and [D3] of Theorem 15 we have:
\[ g(\bar{e}_{33}, \bar{z}) = 1 \] (122)

Substituting equation (122) in equation (99) we have:
\[ g(\bar{e}_{11}, \bar{c}) + g(\bar{e}_{22}, \bar{w}) = 4 \] (123)

Since rank of any element is less than or equal to 1, we have \( g(\bar{e}_{11}, \bar{c}) \leq 2 \) and \( g(\bar{e}_{22}, \bar{w}) \leq 2 \). Then equation (123) implies:
\[ g(\bar{e}_{11}, \bar{c}) = 2 \] (124)

Substituting equation (124) in equation (115) we have:
\[ g(\bar{e}_{33}, \bar{x}) \geq 4 \] (125)

Equation (125) is a contradiction as by Definition 2 the rank function always outputs an integer.

B. Proof of Lemma 5

Proof:

Consider the ‘only if’ part. We show that if the characteristic of the finite field does not divide \( q' \) then network \( N_2 \) has no 2-dimensional vector linear solution. We prove this result by contradiction. Assume that \( N_2 \) has a 2-dimensional vector linear solution even when the characteristic of the finite field does not divide \( q' \).

Since the rank function of a discrete polymatroid is integer valued, from equation (118) we have:
\[ g(\bar{e}_{33}, \bar{z}) \leq 3 \] (126)

Substituting equation (126) in equation (117) we have:
\[ g(\bar{e}_{33}, \bar{x}) \geq 3.5 \] (127)

Then it must that
\[ g(\bar{e}_{33}, \bar{x}) \geq 4 \] (128)

Since rank of an element is less than or equal to 2 ([D3] of Theorem 15), we must have:
\[ g(\bar{e}_{33}, \bar{x}) = 4 \] (129)

Substituting equation (129) in equation (117) we have:
\[ g(\bar{e}_{33}, \bar{z}) = 2 \] (130)

Substituting equation (130) in equation (99) we have:
\[ g(\bar{e}_{11}, \bar{c}) + g(\bar{e}_{22}, \bar{w}) = 8 \] (131)
Since rank of an element is less than or equal to 2, we must have:
\[ g(\bar{e}_{11}, \bar{c}) = 4 \]  \hspace{1cm} (132)
\[ g(\bar{e}_{22}, \bar{w}) = 4 \]  \hspace{1cm} (133)

Substituting equation (132) in equation (115) we have:
\[ g(\bar{e}_{11}, \bar{a}) = 3 \]  \hspace{1cm} (134)

Substituting equations (129), (133), and (134) in equation (121) we have: \( 8 \leq 6 \), which is a contradiction.

To prove the ‘only if’ part we present a 2-dimensional vector linear solution over a finite field whose characteristic divides \( q' \). Let the message vector generated by a source be denoted by the same label as the source. In fig. 5 we show a 2-dimensional vector linear solution of \( \mathcal{N}_2 \) when \( q' = 2 \) (see Lemma 2 for the decoding operations at the terminals of the Char-\( q' - \bar{x} \) sub-network). This solution can easily be extended for any value of \( q' \). (For a different value of \( q' \), only a decoding matrix in the Char-\( q' - \bar{x} \) network changes (see equation 4.)

C. Proof of Lemma 6

Proof: Consider the ‘only if’ part. We show that if the characteristic of the finite field does not divide \( q' \) then network \( \mathcal{N}_2 \) has no 5-dimensional vector linear solution. We prove this result by contradiction. Assume that \( \mathcal{N}_2 \) has a 5-dimensional vector linear solution when the characteristic of the finite field does not divide \( q' \).

Since the rank function of a discrete polymatroid is integer valued, from equation (118) we have:
\[ g(\bar{e}_{33}, \bar{z}) \leq 8 \]  \hspace{1cm} (135)

From equation (117) we get that \( 25 - g(\bar{e}_{33}, \bar{z}) \) must be divisible by 2 (otherwise \( g(\bar{e}_{33}, \bar{x}) \) would not be an integer). Hence \( g(\bar{e}_{33}, \bar{z}) \) must be an odd number. For similar reasoning, from equations (115) and (116) we get that \( g(\bar{e}_{11}, \bar{c}) \) and \( g(\bar{e}_{22}, \bar{w}) \) must be odd numbers.

Then, since \( 5 = g(\bar{z}) \leq g(\bar{e}_{33}, \bar{z}) \), either \( g(\bar{e}_{33}, \bar{z}) = 5 \) or \( g(\bar{e}_{33}, \bar{z}) = 7 \).

Case I: \( g(\bar{e}_{33}, \bar{z}) = 5 \).
Substituting \( g(\vec{c}_{33}, \vec{x}) = 5 \) in equation (99) we get:
\[
g(\vec{c}_{11}, \vec{c}) + g(\vec{c}_{22}, \vec{w}) = 20
\]
(136)
Since rank of any union of two elements is less than or equal to 10, we must have
\[
g(\vec{c}_{11}, \vec{c}) = g(\vec{c}_{22}, \vec{w}) = 10
\]
(137)
But equation (137) is a contradiction because as we have argued, \( g(\vec{c}_{11}, \vec{c}) \) and \( g(\vec{c}_{22}, \vec{w}) \) must be odd numbers.

Case II: \( g(\vec{c}_{33}, \vec{x}) = 7 \).

Substituting \( g(\vec{c}_{33}, \vec{x}) = 7 \) in equation (117) we have:
\[
g(\vec{c}_{33}, \vec{x}) = 9
\]
(138)
Substituting \( g(\vec{c}_{33}, \vec{x}) = 7 \) in equation (99) we get:
\[
g(\vec{c}_{11}, \vec{c}) + g(\vec{c}_{22}, \vec{w}) = 18
\]
(139)
Since neither of \( g(\vec{c}_{11}, \vec{c}) \) and \( g(\vec{c}_{22}, \vec{w}) \) can be equal to 10 (as 10 is an even number), and as both of them must be less than 10, we must have:
\[
g(\vec{c}_{11}, \vec{c}) = 9
\]
(140)
\[
g(\vec{c}_{22}, \vec{w}) = 9
\]
(141)
Substituting equation (140) in equation (115) we have:
\[
g(\vec{c}_{11}, \vec{a}) = 8
\]
(142)
Substituting equations (138), (141), and (142) in equation (121) we have: \( 18 \leq 16 \), which is a contradiction.

To prove the ‘if’ part we now show a 5-dimensional vector linear solution when the characteristic of the finite field divides \( q' \).

We first note that \( \mathcal{N}_2 \) has a 3-dimensional vector linear solution over all finite fields. This is because, we know that the generalized M-network for \( m = 3 \) has a 3-dimensional vector linear solution over all finite fields \([18]\), and from Lemma 2 we know that the Char-\( q' \) – \( x \) network has a vector linear solution for any message dimension over all finite fields whose characteristic divides \( q' \). From Lemma 5 we get that \( \mathcal{N}_2 \) has a 2-dimensional vector linear solution over a finite field whose characteristic divides \( q' \). So a 5-dimensional vector linear solution can easily be constructed.

**References**

[1] N. Das and B. K. Rai, “On the Power of Vector Linear Network Coding,” in *IEEE International Symposium on Information Theory and Its Applications (ISITA)*, Singapore, 2018.

[2] S. Jaggi, M. Effros, T. Ho, and M. Médard, “On linear network coding,” in *42st Annu. Allerton Conf. Communication Control and Computing*, Monticello, IL, USA, 2003.

[3] Q. T. Sun, X. Yang, K. Long, X. Yin, and Z. Li, “On Vector Linear Solvability of Multicast Networks,” *IEEE Transactions on Information Theory*, vol. 64, no. 12, pp. 5096–5107, 2018.

[4] J. B. Ebrahimi and C. Fragouli, “Algebraic Algorithms for Vector Network Coding,” *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 996–1007, 2011.

[5] J. Connelly and K. Zeger, “Linear Network Coding over Rings – Part I: Scalar Codes and Commutative Alphabets,” *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 274–291, 2017.

[6] J. Connelly and K. Zeger, “Linear Network Coding over Rings – Part II: Vector Codes and Non-Commutative Alphabets,” *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 292–308, 2017.

[7] J. Connelly and K. Zeger, “Capacity and Achievable Rate Regions for Linear Network Coding over Ring Alphabets,” *IEEE Transactions on Information Theory*, vol. 65, no. 1, pp. 220–234, 2019.

[8] R. Ahlswede, N. Cai, S. R. Li, and R. W. Yeung, “Network Information Flow,” *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[9] S. R. Li, R. W. Yeung, and N. Cai, “Linear Network Coding,” *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, 2003.

[10] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. M. G. M. Tolhuizen, “Polynomial Time Algorithms for Multicast Network Code Construction,” *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 1973–1982, 2005.

[11] 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.

[12] Q. T. Sun, X. Yin, Z. Li, and K. Long, “Multicast Network Coding and Field Sizes,” *IEEE Transactions on Information Theory*, vol. 61, no. 11, pp. 6182–6191, 2015.

[13] Q. T. Sun, S. R. Li, and Z. Li, “On Base Field of Linear Network Coding,” *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 7272–7282, 2016.

[14] T. Etzion and A. Wachtter-Zeh, “Vector Network Coding Based on Subspace Codes Outperforms Scalar Linear Network Coding,” *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 2400–2473, 2018.

[15] N. J. A. Harvey, R. Kleinberg, and A. R. Lehman, “On the Capacity of Information Networks,” *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2345–2364, 2006.

[16] R. Koetter and M. Médard, “An Algebraic Approach to Network Coding,” *IEEE Transactions on Information Theory*, vol. 11, no. 5, pp. 782–795, 2003.

[17] M. Médard, M. Effros, D. Karger, and T. Ho, “On Coding for Non-Multicast Networks,” in *41st Annu. Allerton Conf. Communication Control and Computing*, Monticello, IL, USA, 2003.

[18] N. Das and B. K. Rai, “On the Message Dimensions of Vector Linearly Solvable Networks,” *IEEE Communications Letters*, vol. 20, no. 9, pp. 1701–1704, 2016.
[19] R. Dougherty, C. F. Freiling, and K. Zeger, “Insufficiency of Linear Coding in Network Information Flow,” *IEEE Transactions on Information Theory*, vol. 51, no. 8, pp. 2745–2759, 2005.

[20] R. Dougherty, C. F. Freiling, and K. Zeger, “Unachievability of Network Coding Capacity,” *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2365–2372, 2006.

[21] R. Dougherty, C. F. Freiling, and K. Zeger, “Linear Network Codes and Systems of Polynomial Equations,” *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2203–2316, 2008.

[22] B. K. Rai and B. K. Dey, “On Network Coding for Sum-Networks,” *IEEE Transactions on Information Theory*, vol. 58, no. 1, pp. 50–63, 2012.

[23] R. Dougherty, C. F. Freiling, and K. Zeger, “Networks, Matroids, and Non-Shannon Information Inequalities,” *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 1949–1969, 2007.

[24] V. T. Muralidharan and B. S. Rajan, “Linear Network Coding, Linear Index Coding and Representable Discrete Polymatroids,” *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 4096–4119, 2016.