On the Role of the Message Dimension and the Characteristic of the Finite Field in Linear Network Coding

A

Thesis Submitted

in Partial Fulfilment of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

By

Niladri Das

(Roll No. 136102023)

DEPARTMENT OF ELECTRONICS AND ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI

GUWAHATI - 781 039, ASSAM, INDIA

October, 2019

Declaration

The thesis entitled "On the Role of the Message Dimension and the Characteristic of the Finite Field in Linear Network Coding" is a presentation of my original research work. Wherever contributions of others are involved, every effort is made to indicate this clearly, with due reference to the literature. The work was done under the guidance of Dr. Brijesh Kumar Rai, at the Indian Institute of Technology Guwahati, Guwahati - 781039, Assam, India.

Dated:
Guwahati.

Niladri Das
Roll No. 136102023
Dept. of Electronics and Electrical Engg.
Indian Institute of Technology Guwahati
Guwahati - 781 039, Assam, India.

Certificate

This is to certify that the thesis entitled "On the Role of the Message Dimension and the Characteristic of the Finite Field in Linear Network Coding", submitted by **Niladri Das** (Roll No. 136102023), a research scholar in the *Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati*, for the award of the degree of **Doctor of Philosophy**, is a record of an original research work carried out by him under my supervision and guidance. The thesis has fulfilled all requirements as per the regulations of the institute and in my opinion has reached the standard needed for the degree. The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

Dated:
Guwahati.

Dr. Brijesh K. Rai
Assistant Professor
Dept. of Electronics and Electrical Engg.
Indian Institute of Technology Guwahati
Guwahati - 781 039, Assam, India.

Acknowledgements

I am thankful to my thesis advisor Dr. Brijesh Kumar Rai, Doctoral Committee Chairman Dr. Tony Jacob, other Doctoral Committee members Dr. A. Rajesh and Dr. Ashish Anand, the Head of EEE Department Prof. Rohit Sinha, DPPC secretary Dr. Sisir Kumar Nayak, the office staffs of EEE Department Mr. Mukut Baruah and Mr. Dasarath Das, the Associate Dean of Academic Affairs (PG) Prof. S. Senthilvelan, the Ministry of Human Resource Development (for providing me a stipend for five years), and the Department of Science and Technology (for sponsoring my conference visit to Singapore).

Niladri Das

Date:

Abstract

Consider a communication problem over a directed acyclic network where information is generated at certain nodes (sources), and certain nodes (terminals) require the information generated at a subset of the sources. Routing is predominantly used for such a problem. However, the concept of network coding emerged as an improvisation over routing. Indeed, for certain class of networks called multicast networks, network coding achieves maximum possible throughput, which is non-achievable through routing for many multicast networks.

In network coding, every intermediate node of a network can send an arbitrary function of incoming information through its outgoing edges. Although restriction on operation (functions) performed by the nodes does affect the performance of network coding, a class of network coding called linear network coding is specially attractive due to well developed mathematics related to linear maps/functions. This thesis is focused on linear network coding.

In a generic form of linear network coding, message symbols (chosen from a finite field) generated at the sources are segregated into blocks of certain length r, called as the message dimension. Each block of r symbols are then linearly mapped to blocks of l symbols – one block for each of its outgoing edges. An intermediate node upon receiving these blocks of l symbols – one block from each of its incoming edges, linearly maps them to blocks of l symbols – one block for each of its outgoing edges. And finally all terminals receives blocks of l symbols – one block from each of its incoming edges, and linearly maps them to blocks of r symbols, in an attempt to retrieve the messages generated by the sources it demands. If all terminals are successful in their attempt then the network is said to have a rate r/l linear solution, or that a rate r/l is linearly achievable.

In this thesis, we consider three aspects of linear network coding, viz, dependency on message dimension (value of r) to achieve certain rates, dependency on characteristic of the finite field with varying message dimension to achieve certain rates, and characteristic

dependent linear rank inequalities to find upper-bound on the rates linearly achievable over finite fields whose characteristic belongs to a finite/co-finite set of primes.

It is known that a network may not have a rate 1 linear solution when the message dimension is equal to 1, but have a rate 1 linear solution when the message dimension is equal to 2. The literature also shows a network which has a rate 1 linear solution if and only if the message dimension is equal to a positive integer multiple of 2. In our first work we generalize this result to show that for any integer $m \geq 2$, there exists a network which has a rate 1 linear solution if and only if the message dimension is equal to a positive integer multiple of m. We then further generalize this result to show that for any two co-prime integers k and n, and for any integer $m \geq 2$, there exists a network which has a rate k/n linear solution if and only if the message dimension is equal to mk (and l is equal to mn).

However, these networks raise another question: if m is the least positive integer such that a network has a rate 1 linear solution when the message dimension is equal to m, whether the the network has a rate 1 linear solution if and only if the message dimension is equal to a positive integer multiple of m. We show that for any positive integer $m \geq 2$, there exists a network which has no rate 1 linear solution if the message dimension is less than m, but has a rate 1 linear solution for all values of the message dimension greater than or equal to m. We also generalize this result to show that for any two co-prime integers k and n, and for any integer $m \geq 2$, there exists a network which has a rate k/n linear solution if and only if the message dimension is equal to wk (and l is equal to wn) where $w \geq m$.

It is known that the existence of a rate 1 linear solution may depend upon the characteristic of finite field, *i.e.*, there exist instances of network coding problems in which a rate 1 linear solution exists if and only if the characteristic of the finite field belongs to a certain set of primes. But, does the set of characteristics over which a rate 1 linear solution exists depends upon the message dimension? To the best of our knowledge, no network has been reported in the literature which has a rate 1 linear solution for some value of the message dimension if and only if the characteristic of the finite field belongs to a set P, and for some other value of the message dimension it has a rate 1 linear solution over some

finite field whose characteristic does not belong to P.

We show that there exists a network where by *increasing* the message dimension just by 1, the set of characteristics over which a rate 1 linear solution exists may get arbitrarily larger, which is not necessarily a superset of original set of characteristics. Such result would indicate an advantage of higher values of the message dimension. However, this is not always true. We show that there also exists a network where by *increasing* the message dimension just by 1, the set of characteristics over which a rate 1 linear solution exists may get smaller, which is not necessarily a subset of the original set of characteristics. As a consequence of these findings, we prove two more results: (i) when the message dimension is fixed to 1, rings are superior to finite fields in terms of achieving a rate 1 linear solution over a lesser sized alphabet, (ii) a network having rate 1 linear solutions when the message dimension is equal to m_1 as well as when the message dimension is equal to m_2 may not have a rate 1 linear solution when the message dimension is equal to $m_1 + m_2$.

As mentioned earlier, the literature shows that the rate achievable using linear network coding depends upon the characteristic of the finite field. For example, it has been shown that for a network named as the Fano network, over finite fields of even characteristic, rate 1 linear solution is achievable, but if the characteristic of the finite field is not 2, then no rate higher than 4/5 is linearly achievable. For such networks, the tightest upper-bound produced by Shannon information inequalities and non-Shannon information inequalities is 1, and neither of these two types of inequalities can produce different upper-bounds for different characteristics. Such upper-bounds (like 4/5 for odd characteristics, 1 for even characteristics) may be obtained by using characteristic-dependent linear rank inequalities, which is a class of linear rank inequalities that hold if and only if the characteristic of the finite field belongs to a certain finite/co-finite set of primes. For example, for the Fano network, using a characteristic-dependent linear rank inequality, the 4/5 upper-bound over finite fields of odd characteristic can be obtained.

We produce three new sets of characteristic-dependent linear rank inequalities and show their application in obtaining upper-bounds on the linear coding capacity of networks over a given set of characteristics. For any given set of primes P, the inequalities in the first set hold if the characteristic of the finite field does not belong to P, and the inequalities

in the second and third set hold if the characteristic of the finite field belongs to P.

Contents

List of Figures

List of Tables

List of Publications

Journal Publications

1. Niladri Das and Brijesh Kumar Rai, "Vector Linear Solution iff Message Dimension $\geq m$," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1470-1473, 2019.
   (**from the works of Chapter - 3**)

2. Niladri Das and Brijesh Kumar Rai, "On the Message Dimensions of Vector Linearly Solvable Networks," *IEEE Communications Letters*, vol. 20, no. 9, pp. 1701-1704, 2016.
   (**from the works of Chapter - 3**)

3. Niladri Das and Brijesh Kumar Rai, "On achievability of an (r, l) fractional linear network code," *IET Networks*, vol. 6, no. 3, pp. 54 61, 2017.
   (**from the works of Chapter - 3**)

International Conferences

1. Niladri Das and Brijesh Kumar Rai, "On the Power of Vector Linear Network Coding," in *IEEE International Symposium on Information Theory and Its Applications (ISITA), Singapore*, 2018.
   (**from the works of Chapter - 4**)

Submitted to Journals

1. Niladri Das and Brijesh Kumar Rai, "On Vector Linear Solvability of non-Multicast Networks," submitted to *IEEE Transactions on Information Theory*.
   (**from the works of Chapter - 4**)

Arxiv Uploads

1. Niladri Das and Brijesh Kumar Rai, "On the Dependence of Linear Coding Rates on the Characteristic of the Finite Field," 2017.
   Available: https://arxiv.org/abs/1709.05970
   (**from the works of Chapter - 5**)

2. Niladri Das and Brijesh Kumar Rai, "Linear Network Coding: Effects of Varying the Message Dimension on the Set of Characteristics," 2019.
   Available: https://arxiv.org/abs/1901.04820
   (**from the works of Chapter - 4**)

1

Introduction

Contents

1. Introduction

Consider a general communication network where a set of sources communicates to a set of receivers through some links and intermediate nodes. Traditionally, information is sent from the sources to the receivers using routing whereby the intermediate nodes perform store and forward function. Finding best throughput using routing is a very difficult problem even in case of multicast networks.

At the beginning of twenty first century, Ahlswede *et al.* introduced the revolutionary idea of network coding where nodes can forward arbitrary functions of incoming symbols to their outgoing links [1]. They showed that network coding can achieve the best throughput of a class of networks called multicast networks. Multicast networks has a single source with some symbols (belonging to an alphabet), and all receivers are to receive all of the source symbols. On the contrary, routing cannot achieve the best throughput of all multicast networks.

Linear network coding is a restricted version of network coding. It has been shown by Li *et al.* that linear network coding is sufficient to achieve the best throughput of all multicast networks. The linearity assumption helps in both algebraically analyzing network coding, and in implementing network coding in practical networks. An algebraic framework of linear network coding has been developed by Koetter *et al.* in [2].

M. Médard *et al.* conjectured that linear network coding in its generality is also sufficient to achieve the best throughput if the network has multiple sources and receivers [3]. But this conjecture has been proven incorrect in [4].

In linear network coding, each source generates a set of symbols from a finite field. These symbols are called source messages and is represented by a vector. Each edge carries a linear function of the vectors received by its tail node. These linear functions can be represented by summation of matrix-vector products. Both the source alphabet (a finite field), and the size of the matrices used to compute the linear functions, can decide achievibility of a certain rate. This size (of the matrices) is reflected by two parameters: message dimension and edge dimension. The messages at the source is segregated into chucks where the number of symbols in each chuck is equal to the message dimension. So the number of columns of the matrices which multiply the vectors generated by the sources is equal to the message dimension. In a single use of an edge, it can carry only a limited number of symbols from the source alphabet. This number is the edge dimension. It is assumed that the edge dimension of all edges is the same. As this limits the number of symbols an edge carries, it must be reflected on the size of the matrices. For example, the number of rows of the matrices that multiply the source

vectors, must be less than or equal to the edge dimension.

For a network, a d-dimensional vector linear solution over $\mathbb{F}_q$ means that the source symbols belong to $\mathbb{F}_q$ and using a linear network code having d message dimension, the terminals of the network can receive all of its demanded source messages (the corresponding set of linear functions used in the network is called as a d-dimensional vector linear network code). An 1-dimensional vector linear solution is also called as a scalar linear solution (the corresponding set of linear functions used in the network is called as a scalar linear network code). In the following section, we give a brief description on the existing literature related to the role of message dimension and characteristic of the finite field in linear network coding.

1.1 Background

The concept of network coding was first shown by Ahlswede *et al.* in the year 2000 [1]. They showed that the capacity of a multicast network (networks with a single source and multiple terminals (a terminal is the same as a receiver) where each terminal demands all the messages generated by the source) is equal to the minimum of the min-cut between all source terminal pairs, and that this capacity can be achieved using network coding, but not always with routing. Since then, network coding has been found to be useful in various applications such as: content distribution in peer-to-peer networks (results in faster downloads than routing), wireless data transfer (saves bandwidth; see analog network coding), network tomography (reduces the number of probes required), network security (as data carried by the edges may not be intrinsic source symbols) etc.

In 2003, Li *et al.* showed that the capacity of all multicast networks can be achieved by using a form of network coding called as the scalar linear network coding [5]. In scalar linear network coding, the value of the message dimension is equal to 1. Jaggi *et al.* presented a deterministic algorithm to decide the linear functions (that is to be used in an instance of a scalar linear network coding) each node has to use such that all terminals can retrieve all source messages [6]. Ho *et al.* showed that if these linear functions are chosen randomly and if the alphabet is sufficiently large, then the receivers can retrieve their demands with an arbitrarily small probability of error [7]. Koetter and Médard developed an algebraic framework to study linear network coding in [2].

Médard *et al.* showed that the d-dimensional vector linear network coding, where $d > 1$, is superior to scalar linear network coding in the sense that a network may have a d-dimensional vector linear

solution but no scalar linear solution [3]. They presented a network – named as the M-network – which has a 2-dimensional vector linear solution, but has no scalar linear solution. Dougherty *et al.* showed that the same network has a d-dimensional vector linear solution if and only if d is an even number [8].

Superiority of d-dimensional vector linear network coding where $d > 1$ over scalar linear network coding also holds for multicast networks. Sun *et al.* showed that there exist multicast networks which has a d-dimensional vector linear solution over $\mathbb{F}_q$, but has no scalar linear solution over any finite field whose size is less than or equal to q^d [9]. Etzion *et al.* very recently showed that the gap between: q_s, which is the minimum field size required for a scalar linear solution, and q^d, which is the least number such that the network has a d-dimensional vector linear solution over a finite field of size q, can be very large [10] (the former quantity being greater). Ebrahimi *et al.* developed an algorithm to decide the linear functions in case vector linear network coding and not scalar linear network coding is employed in a multicast network [11]. Sun *et al.* also showed that there exists a multicast network which has a 4-dimensional vector linear solution over $\mathbb{F}_2$ but does not have a 5-dimensional vector linear solution over $\mathbb{F}_2$. This shows that a network that has a linear solution over $\mathbb{F}_q^d$ does not necessarily have a solution over $\mathbb{F}_q^{d'}$ where $d' > d$. The particular network showed by Sun *et al.* has a 5-dimensional vector linear solution over $\mathbb{F}_{2^4}$ – so it is not that the network does not have a 5-dimensional vector linear solution over finite fields of characteristics 2.

Even though this thesis and almost all of network coding literature considers the source alphabet used for linear network coding as a finite field, linear network coding can also be defined over rings or modules [12]. Very recently, Connelly *et al.* showed in [12] that if linear network coding over a ring or a module achieves a certain rate, then linear network coding over some finite field also achieves the same rate. They also showed that any network that has a scalar linear solution over a commutative ring which is not a field or over a module, also has a scalar linear solution over a finite field whose size is less than or equal to that of the ring or the module [13]. Moreover, they show that a d-dimensional vector linear solution over a finite field implies a scalar linear solution over some ring (may be non-commutative). In this thesis, we study the role of message dimension when the underlying alphabet is a finite field, but in one particular instance, we compare the result with the outcome that would have resulted if the underlying alphabet had been a ring.

A finite field has two parameters: the characteristic of the finite field, and the degree of field

extension; together they determine the size of the finite field. Both the size and the characteristic play an important role in deciding whether a network has a (scalar/vector) linear solution over the corresponding finite field. We discuss this now in more detail.

Li *et al.* showed that a multicast network may not have a scalar linear solution unless the size of the finite field is sufficiently large [5]. Sun *et al.* showed that having a scalar linear solution over a certain finite field does not necessarily mean that it has a scalar linear solution over all larger finite fields [14]. Jaggi *et al.* [6] showed that all multicast networks has a scalar linear solution over a finite field whose size is greater than or equal to the the number of terminals. Riis *et al.* showed a network which for any positive integer n, has a scalar linear solution if and only if the size of the finite field is atleast n [15]. In references [14] and [16] 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 in multicast networks.

In [17], Jaggi *et al.* showed that a network having a scalar linear solution over $\mathbb{F}_{q^d}$ has a d-dimensional vector linear solution over $\mathbb{F}_q$. But a network having a d-dimensional vector linear solution over $\mathbb{F}_q$ may not have a scalar linear solution over any finite field whose size is less than or equal to q^d [9, 10]. Ebrahimi *et al.* showed an efficient algorithm to design vector linear network codes that achieves a vector linear solution in multicast networks [11]. 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 [9] by showing an explicit instance of a network exhibiting such a property. In a recent publication [10], 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 [9] 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 $\mathbb{F}_{2^4}$, 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.

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 respective ratio increases by a factor of q^{m^2-m}. In reference [11], which gives an algorithm to design capacity achieving vector linear network codes in 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*".

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 of the finite field belongs to a certain set of primes.

For non-multicast networks though, the characteristic of the finite field plays an important role. Reference [12] also shows that as long as there is no restriction on the value of the message dimension, linear coding capacity is dependent only on the characteristic of the finite field.

Dougherty *et al.* showed that for any set of polynomials over integers there exists a network which has a scalar linear solution over $\mathbb{F}_q$ if and only if the the set of polynomials has a common root in $\mathbb{F}_q$ [18]. This shows that for any finite or co-finite 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.

Dougherty *et al.* presented a network named as the Fano network which has a vector linear solution for any message dimension if and only if the characteristic of the finite field is two [4]. The same authors also presented the non-Fano network which has a vector linear solution for any message dimension if and only if the characteristic of the finite field is not two [4, 8]. Rai *et al.* showed that for any finite or co-finite set of primes there exists a network which has a vector linear solution for any message dimension if and only if the characteristic of the finite field belongs to the given set of primes [19].

It is worth mentioning that linear network coding may not be the most optimal form of network coding in terms of achieving a solution. It has been shown that for non-multicast networks, non-linear

network coding can produce strictly greater throughput than linear network coding. (There are some benefits for using non-linear network coding in multicast networks as well, such as reduction of the alphabet size required for a scalar solution [20]). In [4], Dougherty *et al.* showed that there exists a network for which non-linear network coding achieves strictly greater throughput than linear network coding. In [21], Connelly *et al.* showed an infinite class of networks in which non-linear network coding achieves strictly greater data rates than linear network coding.

We divide the rest of the introduction into two parts. In the first part, we discuss coding capacity, linear coding capacity, and the role that information inequalities and linear rank inequalities play in determining upper-bounds on the capacity and linear coding capacity of a network. In the second part, we discuss about a branch of mathematics called Matroid theory which has found significant application in finding the limits of linear network coding.

1.2 Capacity, Information Inequalities, and Rank Inequalities

Capacity of a network is a measure of the best rate at which data that can be transferred from the sources to the terminals. It is is defined as the *supremum* of all achievable rates. It becomes necessary to use *supremem* instead of maximum so that rates that can be achieved asymptotically is also incorporated. It has been shown that if a certain rate is achievable over one alphabet then it is also achievable over any other alphabet [22] (using non-linear network coding) – and this is why the capacity of a network does not depend upon the source alphabet.

Information inequalities has been shown to be useful to find upper-bounds on the capacity of a network. For all messages either generated by the sources or transmitted by the edges, a corresponding random variable is defined. Generally, the random variables corresponding to the messages generated by the sources are considered as uniformly distributed over the source alphabet. The random variables corresponding to the message transmitted by an edge is a function of the random variables associated with the messages received by the tail node of the edge. The collection of all of these random variables must obey all the information inequalities.

Information inequalities are inequalities obeyed by the entropy of jointly distributed random variables. The definition of an information inequality is reproduced from [23]: if n is a positive integer, c_i for $1 \leq i \leq k$ are real numbers, and I_i for $1 \leq i \leq k$ are subsets of the set $\{1, 2, \ldots, n\}$, then an inequality of the form $c_1 H(\{A_i | i \in I_1\}) + c_2 H(\{A_i | i \in I_2\}) + \cdots + c_k H(\{A_i | i \in I_k\}) \geq 0$ is called an

information inequality if it is obeyed by all jointly distributed random variables $A_1, A_2, \ldots, A_n$. From the random variables $A_1, A_2, \ldots, A_n$ a total of $2^n - 1$ joint distributions can be defined. If the entropy of these distributions are stacked up, then it forms a $2^n - 1$ length vector in $\mathbb{R}^{2^n-1}$. Now, if for a vector in $\mathbb{R}^{2^n-1}$ there exist random variables $A_1, A_2, \ldots, A_n$ such that the values of the components of the vector are equal to the joint entropies of the random variables $A_1, A_2, \ldots, A_n$, then the vector is said to be entropic. The collection of all entropic vectors forms the entropy region. We note that the definition of information inequalities include only linear information inequalities. It has been shown in [24] that there also exist non-linear information inequalities.

Applying information inequalities to a network tells us the rates which are impossible to achieve, and thus produces upper-bounds on its achievable rate. It has been shown that there exist infinite number of these inequalities [25]. Information inequalities that can be expressed as $\sum_i c_i I(A_i; B_i|C_i) \geq 0$, where c_i is a non-negative real number, are called Shannon inequalities. All information inequalities in three or less variables are Shannon inequalities [26]. The list of Shannon inequalities can be found in [8], pp.-1951. There exist non-Shannon information inequalities as well. The first four variable non-Shannon information inequality was discovered by Zhang and Yeung in [27]. More four variable non-Shannon information inequalities have been shown in [23].

The capacity of a network is always less than or equal to the minimum of min-cut between of all source terminal pairs (a source and a terminal forms a pair if the terminal demands the message generated by the source). Moreover, it has been shown that the capacity may be unachievable [22]. Harvey *et al.* in [28] presented a method to obtain an upper-bound on the capacity by combining Shannon inequalities with the constraints imposed by the topology of the network and limited capacity of the edges (the effects of the topology was captured by defining a term named as functional dominance). It has been shown in [23] that the bound obtained from this method may be further improved by additionally incorporating non-Shannon information inequalities. A network named as the Vámos network is a good example to see how these inequalities come together. Vámos network was first considered in [8], where by applying the non-Shannon inequality discovered by Zhang and Yeung, it was shown that its coding capacity is upper-bounded by 10/11. This bound was then further improved to 19/21 by applying other non-Shannon inequalities in [23].

Linear coding capacity is the *supremum* of all rates achievable using linear network coding. So linear coding capacity is always less than or equal to capacity (because linear network coding restricts

all functions to be linear). This is reflected by the fact that in addition to edge capacities and information inequalities, the rates achievable using linear network coding is further hindered by linear rank inequalities. Linear rank inequalities are inequalities that are obeyed by dimensions of vector subspaces of a vector space. It has been shown that for a certain rate to be linearly achievable in a network, a corresponding representable discrete polymatroid, which is a collection of vector subspaces, must exist. Linear rank inequalities put bounds on the dimensions of these vector subspaces (of the discrete polymatroid).

It can be shown that all information inequalities are also linear rank inequalities. This result has been proved in Theorem 2 of [26]. The authors proved this result by showing that for any collection of vector subspaces $\{V_i|1 \leq i \leq n\}$ of a finite dimensional vector space, there exist random variables $\{X_i|1 \leq i \leq n\}$ such that $dim(\sum_{j\in I} V_j) = cH(\{X_j|j \in I\})$ for any $I \subseteq \{1, 2, \ldots, n\}$, where c is a constant. The opposite result that: a linear rank inequality is also an information inequality is however not true. Theorem 4 of [26] shows a four variable linear rank inequality: Ingleton's inequality, which is not an information inequality.

Hammer *et al.* showed that for upto three variables, there exists no linear rank inequality which is not an information inequality (Theorem 3 of [26]). They also showed that for four variables, the only linear rank inequality which is not an information inequality is the Ingleton inequality and permutations of its variables (Theorem 5 of [26]). A list of twenty four new linear rank inequalities in five variables, which are not information inequalities, has been shown in [29].

Reference [30] shows that even an incomplete list of six variable linear rank inequalities crosses one billion. For seven or more variables, references [31], [32] and [33] show that there exist linear rank inequalities that hold if the characteristic of the field is among a certain set of values, but may not hold otherwise. Such an inequality is called as a characteristic-dependent linear rank inequality.

First, Blasiak *et al.* showed two characteristic-dependent linear rank inequalities of seven variables: one holds over finite fields of even characteristic, and the other holds over finite fields of odd characteristic [31]. Thereafter, Dougherty *et al.* showed two more seven variable characteristic-dependent linear rank inequalities in [32]. Subsequently, two new eight variable inequalities has been presented in [33]. Applications (finding upper-bounds on the linear coding capacity of networks over finite fields of a given characteristic) of the inequalities shown in [32] and [33] has been also presented in the respective papers. In [34], the author showed that for any finite or co-finite set of primes there exists a

characteristic-dependent linear rank inequality that holds if the characteristic of the finite field belongs to the given set, but may not hold otherwise.

1.3 Matroids and Linear Network Coding

Matroid Theory is a branch of mathematics which has found significant applications in the analysis of linear network coding. A number of significant theoretical results on linear network coding has been discovered due to the connection between the two subjects. The essence of a matroid is to capture the abstract concept of independence. A matroid is a collection of two sets: a set of elements called as the ground set, and a set of subsets of the ground set called as the independent set. Intuitively, the connection between matroids and networks is this: the messages (vector over a finite field) generated by the sources are independent to each other, and the vectors carried by the edges are dependent on these source messages; and hence there is a possibility that the collection of vectors being generated by sources or carried by the edges forms a matroid. This intuitive connection was first mathematically established in [8]. It was shown that the sources and edges of a network can be mapped to the ground set of a matroid such that the network has a scalar linear solution over $\mathbb{F}_q$ if and only if the matroid is representable over $\mathbb{F}_q$. A matroid is representable over $\mathbb{F}_q$ if it is isomorphic to a matroid whose ground set elements are vectors over $\mathbb{F}_q$ (eg. of a matroid whose ground set elements are vectors: a matrix; the columns of the matrix forms the ground set, and the subset of the columns which are independent forms the independent set – more on this in Chapter 2)

In [8], Dougherty *et al.* developed a method to construct networks from matroids such that if the network has a scalar linear solution over $\mathbb{F}_q$, then the matroid is representable over $\mathbb{F}_q$. Using this method, in [8], Dougherty *et al.* – from the Fano matroid, which is representable only over finite fields of characteristic 2 – constructed a network that has a linear solution if and only if the characteristic of the finite field is 2. Analogously, from the dual of the Fano matroid: the non-Fano matroid, which is known to be representable only over finite fields whose characteristic is not 2, a network which has a linear solution if and only if the characteristic of the finite field is not 2 was constructed [8]. It has been shown in [4] that a network constructed by combining these two networks has no linear solution over any finite field; but has a non-linear solution. This proved that linear network coding may be insufficient to achieve the capacity of a network [4].

Koetter and Médard developed an algebraic framework to study linear network coding in [2].

Given a network, they constructed a set of polynomial equations such that the network has a scalar linear solution over $\mathbb{F}_q$ if and only if the polynomials are satisfiable over $\mathbb{F}_q$. The correspondence between matroid theory and linear network coding was used by Dougherty *et al.* in [18] to show that for any given set of polynomials with integer coefficients there exists a network which has a scalar linear solution over $\mathbb{F}_q$ if and only if the set of polynomials have a solution over $\mathbb{F}_q$. This showed that determining whether a network has a scalar linear solution is as much difficult as solving a set of polynomials. An inference of the results in [18] is that for any finite or co-finite set of prime numbers 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.

Dougherty *et al.* in [8], using the smallest known non-representable matroid: the Vámos matorid, constructed a network named as the Vámos network. They showed that this network does not have a linear solution for any dimension over any finite field. Moreover, they showed that Shannon inequalities produce an upper-bound of 1 on the capacity of the network. But using the Zhang-Yeung information inequality (a non-Shannon information inequality) an upper-bound strictly lesser than 1 was be obtained. Thus, they concluded that Shannon inequalities are insufficient to compute coding capacity.

Like scalar linear network coding is related to representable matroids, it has been shown that vector linear network coding is related to discrete polymatrodis [35]. The main difference between a matroid and a discrete polymatroid is that in a matroid, rank of each element in the ground set is either 0 or 1; where in a discrete polymatroid the rank of each element of the ground set can be any non-negative integer. It has been shown that the sources and edges of a network can be mapped to the ground set of a discrete polymatroid such that the network has a linear solution in d-dimension over $\mathbb{F}_q$ if and only if the discrete polymatroid satisfies some rules and is representable over $\mathbb{F}_q$. A discrete polymatroid is representable if it is isomorphic to a discrete polymatroid whose ground set elements are vector subspaces of a finite dimensional vector space.

1.4 Contributions and Organization of this Thesis

Chapter 1 is Introduction. In Chapter 2, we discuss formal definitions of scalar linear network coding, vector linear network coding, and fractional linear network coding; reproduce some results and definitions from literature that connect matroid theory and networks solvability; reproduce some

results on linear functions; and reproduce the proof that shows all information inequalities are also linear rank inequalities.

The contributions of this thesis is segregated into Chapters 3, 4, and 5.

In reference [3], Medard *et al.* showed that there exists a non-multicast network which has a 2-dimensional linear solution but does not have a scalar linear solution. In Chapter 3, we generalize this result to show that for any positive integer $m \geq 2$, there exists a network which has a w-dimensional vector linear solution if and only if w is a multiple of m. We then show that for any positive integer $m \geq 2$, there exists a network which has a w-dimensional vector linear solution if and only if w is greater than or equal to m.

We also generalize these results to show that for any positive integers k, n, and $m \geq 2$, there exists a network which has a (wk, wn) fractional linear solution if and only if w is a multiple of m, and there also exists a network which has a (wk, wn) fractional linear solution if and only if w is greater than or equal to m. These results conclude that arbitrary large message dimension may be required to achieve a certain rate using linear network coding.

In Chapter 4, we show that there exists a network where by *increasing* the message dimension just by 1, the set of characteristics over which a vector linear solution exists get arbitrarily larger, which is not necessarily a superset of original set of characteristics. Such result would indicate an advantage of higher message dimensions. However, this is not always true. We also show that there also exists a network where by *increasing* the message dimension just by 1, the set of characteristics over which a vector linear solution exists may get smaller, which is not necessarily a subset of the original set of characteristics.

As a consequence of these findings, 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 an m_1-dimensional vector linear solution and an m_2-dimensional vector linear solution do not guarantee the existence of an $(m_1 + m_2)$-dimensional vector linear solution.

In Chapter 5, we derive three new sets of characteristic-dependent linear rank inequalities. For any given set of primes P, the inequalities in the first set hold if the characteristic of the finite field does not belong to P, but may not hold otherwise; and the inequalities in the second and third set hold if the characteristic of the finite field belongs to P, but may not hold otherwise. We also show applications of these inequalities in the same chapter.

2

Preliminaries

Contents

We now present the formal definitions of terms used in this thesis; and reproduce existing results from the literature which will be used as facts while proving the results of this thesis.

A network is represented by a directed acyclic graph $G(V, E)$. The set V is partitioned into three disjoint sets: the set of sources S, the set of terminals T, and the set of intermediate nodes V'. Each source generates an i.i.d. random process uniformly distributed over a finite field $\mathbb{F}_q$. The random process at any source is independent of all source processes. Each terminal demands the information generated by a subset of the sources.

To each source node an imaginary incoming edge is added, and this edge carries the message generated by the corresponding source. For each demand (a demand is a source message demanded by a terminal) of a terminal, an imaginary outgoing edge is added to the terminal, and this edge requires to carry the respective demanded source message. Let the imaginary edge added to a source s be denoted by s', and let the imaginary edge added from a terminal t be denoted by t'.

An edge e has two nodes and an direction. The two nodes are denoted by $tail(e)$ and $head(e)$, and the direction is from $tail(e)$ to $head(e)$. Such an edge is denoted by (u, v) where $u = tail(e)$ and $v = head(e)$. For a node $v \in V$, the set of edges e for which $head(e) = v$ is denoted by $In(v)$, and the set of edges e for which $tail(e) = v$ is denoted by $Out(v)$. The information/message carried by an edge e is denoted by Y_e. Without loss of generality (w.l.o.g.), it is assumed that all the edges in the network are unit capacity edges (meaning, in one usage of an edge it carries one symbol from the source alphabet). There is no delay or error in the network.

2.1 Scalar Linear Network Coding

The term 'scalar' in scalar linear network coding indicates the fact that the messages generated by the sources are elements of a finite alphabet. In majority of works related to linear network coding this finite alphabet is assumed to be a finite field as this is the case in this thesis as well. However, there are some works of theoretical importance and also from pedagogical point of view where the finite alphabet is assumed to be ring, module etc. In this thesis, until unless specified, the assumed alphabet is a finite field. The generalization of scalar linear network coding is vector linear network coding – to be discussed in subsection 2.2 – where the messages generated by the sources are vectors over $\mathbb{F}_q$. The term linear network coding indicates that the messages carried by an edge e is linear combination of the symbols carried by the edges in $In(tail(e))$.

In scalar linear network coding, for all edge pair $(e_i, e_j) \in E \times E$ an element $c_{e_i,e_j} \in \mathbb{F}_q$ is assigned. The collection of all of these elements c_{e_i,e_j} for $\forall (e_i, e_j) \in E \times E$ is called as a scalar linear network code. For any edge e, if $tail(e) = v$ and $In(v) = \{e_1, e_2, \ldots, e_m\}$, then $Y_e = c_{e_1,e}.Y_{e_1} + c_{e_2,e}.Y_{e_2} + \cdots + c_{e_m,e}Y_{e_m}$.

If using a scalar linear network code over some finite field $\mathbb{F}_q$, each terminal can retrieve one source symbol from all the sources intended, then the network is said to have a scalar linear solution over $\mathbb{F}_q$. A network is called as scalar linear solvable if it has a scalar linear solution over some finite field $\mathbb{F}_q$.

Here are some interesting facts on scalar linear network coding:

- All multicast networks – *i.e.*, networks with only one source and all terminals demand the same information from the source – has a scalar linear solution over some finite field [1]. Jaggi *et al.* showed a deterministic algorithm to decide the linear coding coefficients – *i.e.*, the values c_{e_i,e_j} for each edge pair – to achieve a scalar linear solution of multicast networks [6]. Ho *et al.* presented a randomized algorithm where these coefficients are chosen randomly [7].

- For any given set of polynomials with integers coefficients, there exists a network which has a scalar linear solution over $\mathbb{F}_q$ if and only if the set of polynomials has a common root in $\mathbb{F}_q$ [18].

- Non-multicast networks may not have a scalar linear solution. Moreover, non-multicast networks whose linear coding capacity is equal to 1 may not have scalar linear network coding solution either. Medard *et al.* presented a network in [3] which has no scalar linear solution but has a 2-dimensional vector linear solution.

2.2 Vector Linear Network Coding

Vector linear network coding is a generalization of the scalar linear network coding. The term 'vector' in vector linear network coding indicates that the messages generated by the sources are vectors over a finite field $\mathbb{F}_q$. The term linear network coding indicates that the messages carried by an edge is linear combination of the vectors input to the tail node of the edge. The length of the vectors generated by all sources is the same. This number is called as the message dimension. If message dimension is equal to m, then the corresponding vector linear network coding is referred as m-dimensional vector linear network coding.

In Vector linear network coding, for all edge pair $(e_i, e_j) \in E \times E$ a matrix $C_{\{e_i,e_j\}}$ – known as the local coding matrix for the edge pair (e_i, e_j) – is assigned. In an m-dimensional vector linear network

code over $\mathbb{F}_q$, all matrices $C_{\{e_i,e_j\}}$ for $(e_i, e_j) \in E \times E$ belong to $\mathbb{F}_q^{m\times m}$. For any edge pair (e_i, e_j), if $tail(e_j)$ is a source node, then the local coding matrix is called as an encoding matrix, and if $tail(e_j)$ is a terminal node, then the local coding matrix is called as a decoding matrix. The collection of all $C_{\{e_i,e_j\}}$ for $\forall\ (e_i, e_j) \in E \times E$ is denoted as an m-dimensional vector linear network code. For any edge e, if $tail(e) = v$ and $In(v) = \{e_1, e_2, \ldots, e_m\}$, then $Y_e = C_{\{e_1,e\}}.Y_{e_1} + C_{\{e_2,e\}}.Y_{e_2} + \cdots + C_{\{e_m,e\}}Y_{e_m}$.

If using an m-dimensional vector linear network code over some finite field $\mathbb{F}_q$, each terminal can retrieve m source symbols from its intended sources, then the network is said to have an m-dimensional vector linear solution over $\mathbb{F}_q$. A network is said to be vector linearly solvable for message dimension m, or that it has a vector linear solution for message dimension m, if it has an m-dimensional vector linear solution over some finite field. A network is called as vector linearly solvable, or that it has a vector linear solution, if it has a vector linear solution for some message dimension m over some finite field $\mathbb{F}_q$. If a network has a scalar linear solution or a vector linear solution, then the network is said to have a linear solution or to be linearly solvable. Note that an 1-dimensional vector linear solution is a scalar linear solution.

Here are some interesting facts on vector linear network coding:

- If a network has a scalar linear solution over $\mathbb{F}_{p^a}$, then it also has an a-dimensional vector linear solution over $\mathbb{F}_p$ [17]. But if a network has an a-dimensional vector linear solution over $\mathbb{F}_p$, then it may not necessarily have a scalar linear solution over $\mathbb{F}_{p^a}$ [14].
- Vector linear network coding can be employed in multicast networks to achieve a linear solution over a lesser sized alphabet than what would be required to achieve a scalar linear solution [10].
- Algorithm to design the local coding matrices that achieves a vector linear solution in a multicast network can be found in [11].
- A multicast network having an m-dimensional vector linear solution over some alphabet does not imply that it has a vector linear solution for all larger vector dimensions [9] over the same alphabet.
- The M-network is the first network shown to have no scalar linear solution, but has a vector linear solution for every even message dimension [3, 8].
- For any given finite or co-finite set of primes, there exists a network which has an m-dimensional

vector linear solution for any positive integer m if and only if the characteristic of the finite field belongs to the given set [19].

2.3 Fractional Linear Network Coding

Fractional linear network coding is further generalization of vector linear network coding. The term 'fractional' in fractional linear network coding indicates the fact that the length of vectors generated by the sources may not be equal to the length of the vector carried by the edges (*i.e*, message dimension may not be equal to edge dimension).

In a (k, n) fractional linear network coding over $\mathbb{F}_q$, each source generates a k-length vector over $\mathbb{F}_q$ and each edge carries an n-length vector over $\mathbb{F}_q$. For all edge pair $(e_i, e_j) \in E \times E$ a matrix $C_{\{e_i,e_j\}}$ – known as the local coding matrix for the edge pair (e_i, e_j) – is assigned. If $tail(e_j)$ is a source, then $C_{\{e_i,e_j\}} \in \mathbb{F}_q^{k\times n}$; if $tail(e_j)$ is a terminal, then $C_{\{e_i,e_j\}} \in \mathbb{F}_q^{n\times k}$; otherwise $C_{\{e_i,e_j\}} \in \mathbb{F}_q^{n\times n}$. The collection of all $C_{\{e_i,e_j\}}$ for $\forall\ (e_i, e_j) \in E \times E$ is called as a fractional linear network code. For any edge e, if $tail(e) = v$ and $In(v) = \{e_1, e_2, \ldots, e_m\}$, then $Y_e = C_{\{e_1,e\}}.Y_{e_1} + C_{\{e_2,e\}}.Y_{e_2} + \cdots + C_{\{e_m,e\}}Y_{e_m}$.

If using a (k, n) fractional linear network code over some finite field $\mathbb{F}_q$ each terminal can retrieve k source symbols from each of its intended sources, then the network is said to have a (k, n) fractional linear solution over $\mathbb{F}_q$. A network is said to be as fractional linearly solvable, if it has a (k, n) fractional linear solution for some k and n over some finite field $\mathbb{F}_q$. The ratio $\frac{k}{n}$ is called the rate. A network is said to have a rate $\frac{k}{n}$ fractional linear network coding solution if it has a (dk, dn) fractional linear network coding solution for some positive integers d, k, n. Note that a (k, k) fractional linear network code is a k-dimensional vector linear network code.

2.4 Matroids, Polymatroids, and Networks

Matroids and polymatroids are part of mathematics (a branch called matroid theory) and were developed much earlier to network coding. But both of these mathematical structures have found many application in the study of network coding. The relation between these two was developed by Dougherty, Freiling, and Zeger in [8]. They showed a method to construct a network from a matroid such that some key properties of the matroid gets transferred to the network. For example, from the Fano matroid which is not representable over finite fields of odd characteristics, they constructed a

network that has no scalar linear solution over finite fields of odd characteristics. Some of the other results that were proved using this connection are: insufficiency of linear network coding to achieve capacity of a general network (in [4]), insufficiency of Shannon information inequality to compute the capacity of a network (in [8]), unachievability of network coding capacity (in [22]), etc.

In almost all theorems proved in this thesis, rather than matroids, we have used another structure: discrete polymatroids. Using the results of [8], Kim *et al.* showed that if a network is matroidal (to be defined later) then it has a scalar linear solution over a finite field $\mathbb{F}_q$ if and only if the matroid to which the network is matroidal is representable over $\mathbb{F}_q$. However, it was not clear at that time whether there exists matroid analogues that would correspond to vector linear network coding. Rouayheb *et al.* showed that multi linear representation of matorids may capture vector linear network coding [36]. But Murilidharan *et al.* showed that multi linear representations cannot capture all vector linear solutions [35]. They instead showed that polymatroids are a natural extension of matorids, and discrete polymatroids – a class of polymatroids – can capture more general forms of network coding like vector linear network coding and fractional linear network coding. Murilidharan *et al.* showed in a theorem (Theorem 1 of [35]) that a network has a vector linear solution in d message dimension if and only if there exists a corresponding discrete polymatroid with some properties. In many proofs in this paper, to determine whether a network has a vector linear solution in d message dimension we have used this theorem.

2.4.1 Matroids

First we define matroid. The following definition is reproduced from [37] (section 1.3.2.). Let $\mathbb{Z}^+$ be the set of all positive integers.

Definition 1. *Let G be a set and $r : 2^G \rightarrow \{0 \cup \mathbb{Z}^+\}$ be a function that maps all subsets of G into the set of non-negative integers such that:*

R1 *If $X \subseteq G$, then $0 \leq r(X) \leq |X|$*

R2 *If $X \subseteq Y \subseteq G$ then $r(X) \leq r(Y)$*

R3 *If $X, Y \subseteq G$, then $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$*

Let $\mathcal{I}$ be the collection of subsets of G such that if $X \in \mathcal{I}$ then $r(X) = |X|$. Then $(G, \mathcal{I})$ is a matroid having rank function r. Here G is called the ground set and the elements of $\mathcal{I}$ are called as independent

sets. A matroid $(G, \mathcal{I})$ *may also be denoted by a single letter such as* $\mathcal{M}$ *where* $\mathcal{M} = (G, \mathcal{I})$. *The function* $r()$ *is called the rank function of the matroid* $\mathcal{M}$.

Let us take an example of a matroid. Consider the following matrix A over integers:

$$A = \begin{bmatrix} 1 & 0 & 0 & 2 & 3 \\ 0 & 1 & 0 & 3 & 4 \\ 0 & 0 & 1 & 5 & 6 \end{bmatrix}.$$

Any collection of three or lesser number of columns of A are independent and any collection of four or five number of columns are dependent. Let $A(i)$ denote the i^{th} column of A. Let $G = \{1, 2, 3, 4, 5\}$. For any $X = \{j_1, j_2, \ldots, j_{|X|}\} \subseteq G$, let $A(X) = \begin{bmatrix} A(j_1) & A(j_2) & \cdots & A(j_{|X|}) \end{bmatrix}$. Define the rank function r as $r(X) = rank(A(X))$ where $rank()$ denotes the usual rank of a matrix. Then $\mathcal{M} = (G, \mathcal{I})$ is a matroid where $\mathcal{I}$ contains all $X \subset G$ with $|X| \leq 3$.

Here $\mathcal{M} = (G, \mathcal{I})$ is called a vector matroid of A with rank function $r(X) = rank(A(X))$ for any $X \subseteq G$. A matroid is a vector matroid if its ground set elements are vectors.

Two matroids $\mathcal{M}_1 = (G_1, \mathcal{I}_1)$ and $\mathcal{M}_2 = (G_2, \mathcal{I}_2)$ are isomorphic to each other if there exists a bijection $f : G_1 \to G_2$ such that for any $X \in G_1$, $X \in \mathcal{I}_1$ if and only if the set $f(X) \in \mathcal{I}_2$.

A matroid $\mathcal{M}$ said to be representable over a finite field $\mathbb{F}_q$ if $\mathcal{M}$ is isomorphic to a vector matroid of a matrix over $\mathbb{F}_q$.

An alternate but equivalent definition of a representable matroid is given below (not our contribution). This definition will be easier to extend to discrete polymatroids.

Definition 2. *A matroid* $\mathcal{M} = (G, \mathcal{I})$ *with the rank function* $r : 2^G \to \{0 \cup \mathbb{Z}^+\}$ *is said to be representable over* $\mathbb{F}_q$ *if there exists one dimensional vector subspaces* $V_1, V_2, \ldots, V_{|G|}$ *of a finite dimensional vector space over* $\mathbb{F}_q$ *such that for any* $X \subset G$: $r(X) = dim(\sum_{i \in X} V_i)$.

We now reproduce the definition of matroidal networks from [8]. Let $\mathcal{N}$ be a network, and let S be the set of sources in $\mathcal{N}$, E be the set of edges in $\mathcal{N}$, and V be the set of vertices in $\mathcal{N}$.

Definition 3. *[8, Definition V.1, p. 1956] Let* $\mathcal{M} = (G, \mathcal{I})$ *be a matroid with rank function* r. *The network* $\mathcal{N}$ *is a matroidal network with respect to* $\mathcal{M}$ *if there exist a function* $f : \{S, E\} \to G$ *such that the following conditions are satisfied:*

M1 f *is one-to-one on* S.

M2 $f(S) \in \mathcal{I}$.

M3 *for* $\forall v \in V$, $r(f(In(v))) = r(f(In(v) \cup Out(v)))$.

Dougherty *et al.* in [8] proved that a network has a scalar linear solution over $\mathbb{F}_q$ only if it is a matroidal network with respect to a matroid representable over $\mathbb{F}_q$. (a scalar linear solution was translated into a representation of a matroid)

Kim et al. in [38] showed the opposite: if a network is matroidal with respect to a matroid representable over $\mathbb{F}_q$ then it has a scalar linear solution over $\mathbb{F}_q$. (a representation of a matroid was translated into a scalar linear solution)

Muralidharan *et al.* in [35] extended the network matroid mapping to network discrete polymatroid mapping. They also showed that such mappings can correctly capture vector linear network coding and fractional linear network coding.

2.4.2 Discrete Polymatroids

Discrete polymatroids are generalized versions of matroids. In matroid the rank of a single element can be either 0 or 1. In discrete polymatroid the rank of a single element of can be any non-negative integer. There is also a difference in describing matroids and polymatroids as we will see.

First, discrete polymatroid [35, 39, 40] is defined. Let $G = \{1, 2, \ldots n\}$. Also let $\mathbb{Z}_{\geq 0} = \{0 \cup \mathbb{Z}^+\}$. Define $\mathbb{Z}^n_{\geq 0}$ as the set of all n length vector whose elements are in $\mathbb{Z}_{\geq 0}$. If v is an n length vector and $A \subseteq G$, then $v(A)$ is the vector having only the components indexed by the elements of A, and $|v(A)|$ is the sum of the components of $v(A)$.

Definition 4. *[35, Definition 2, p. 4098] Let ρ be a function that maps 2^G into $\mathbb{Z}_{\geq 0}$ such that*

P1 $\rho(\phi) = 0$.

P2 $\rho(A) \leq \rho(B)$ *if* $A \subseteq B$.

P3 $\rho(A) + \rho(B) \geq \rho(A \cup B) + \rho(A \cap B)$.

Let $\mathbb{D}$ be the collection of all elements $x \in \mathbb{Z}^n_{\geq 0}$ such that $|x(A)| \leq \rho(A)$ for $\forall A \subseteq G$. Then $\mathbb{D}$ is a discrete polymatroid having rank function ρ and ground set G.

A discrete polymatroid $\mathbb{D}$ has $\rho_{max} = d$ if ρ follows this additional rule: for $\forall A \subseteq G$, $\rho(A) \leq d|A|$. By setting $\rho_{max} = 1$, one can completely describe a matroid [35]. So discrete polymatroids can be viewed as the generalized version of matroids.

Note that **P1** of Definition 4 is less restricted than **R1** of Definition 1; because if **P1** holds then **R1** may not hold, but if **R1** holds then **P1** will also hold. This shows that all matroids are also discrete polymatroids but all discrete polymatroids are not matroids.

Also note that matroids and discrete polymatroids are described differently. For example if the matroid, which is the vector matroid of the matrix A in equation (2.1), is described as discrete polymatroid $\mathbb{D}_A$, we get:

$$\begin{aligned}\mathbb{D} =\{&(1,1,1,0,0),(1,1,0,1,0),(1,1,0,0,1),(1,0,1,1,0),(1,0,1,0,1),(1,0,0,1,1),(0,1,1,1,0),\\ &(0,1,1,0,1),(0,1,0,1,1),(0,0,1,1,1),(1,1,0,0,0),(1,0,1,0,0),(1,0,0,1,0),(1,0,0,0,1),\\ &(0,1,1,0,0),(0,1,0,1,0),(0,1,0,0,1),(0,0,1,1,0),(0,0,1,0,1),(0,0,0,1,1),(1,0,0,0,0),\\ &(0,1,0,0,0),(0,0,1,0,0),(0,0,0,1,0),(0,0,0,0,1)\}.\end{aligned}$$

Definition 5. *[35, Definition 3, p. 4099] A discrete polymatroid $\mathbb{D}$ with rank function ρ and ground set $G = \{1, 2, \ldots n\}$ is said to be representable over $\mathbb{F}_q$ if there exist vector subspaces $V_1, V_2, \ldots, V_n$ of a vector space V over $\mathbb{F}_q$ such that $dim(\sum_{i\in X} V_i) = \rho(X)$ for $\forall X \subseteq G$. The set of vector spaces $\{V_i, i \in G\}$ is said to form a representation of $\mathbb{D}$. A discrete polymatroid is said to be representable if it is representable for some field.*

In [35] the authors defined the notion of a network being discrete polymatroidal with respect to a discrete polymatroid. We reproduce the definition below but with some different notations. Let ϵ_{in} be a n length vector whose i^{th} component is one and all other components are zero. Let $\mathcal{N}$ be a network whose set of sources is S, set of edges is E, and set of vertices is V.

The following definition is reproduced from [35].

Definition 6. *[35, Definition 7, p. 4102] Let $\mathbb{D}$ be a discrete polymatroid with rank function ρ, and ground set $G = \{1, 2, \ldots n\}$. The network $\mathcal{N}$ is said to be a (k, n)-discrete polymatroidal network with respect to the discrete polymatroid $\mathbb{D}$, if there exists a map $f : \{S \cup E\} \to G$ such that*

D1 *f is one-to-one on S.*

D2 $\sum_{i\in f(S)} k\epsilon_{in} \in \mathbb{D}$.

D3 $\forall s \in S$, $\rho(f(s)) = k$, *and* $\forall e \in E$, $\rho(f(e)) \leq n$.

D4 $\rho(f(In(v))) = \rho(f(In(v) \cup Out(v)))$, $\forall v \in V$.

If X_s is the message generated by a source s, and if Y_e is the symbols carried by an edge e, there is a one-to-one correspondence between s and X_s, as well as between e and Y_e, and hence, the Definition 6 holds if S is the set of messages generated by the sources and E is the set of symbols carried by the edges.

The following theorem is also reproduced from [35].

Theorem 1. *[35, Theorem 1, p. 4102] A network has a (k, n) fractional linear network coding solution over $\mathbb{F}_q$ if and only if it is a (k, n)-discrete polymatroidal network with respect to a discrete polymatroid $\mathbb{D}$ representable over $\mathbb{F}_q$.*

When $k = n$, Theorem 1 reduces to the following.

Theorem 2. *A network has a k-dimensional vector linear solution over $\mathbb{F}_q$ if and only if it is a (k, k)-discrete polymatroidal network with respect to a discrete polymatroid $\mathbb{D}$ representable over $\mathbb{F}_q$.*

In such a case, according to Defintion 6, discrete polymatroid $\mathbb{D}$ will have $\rho_{max} = k$. Also note that if a network is matroidal with respect to a matroid, then it is also $(1, 1)$-discrete polymatroidal with respect to a discrete polymatroid which has $\rho_{max} = 1$.

The following three Lemmas as a result of the relation between discrete polymatroids and linear solvability. Let S be the set of sources of a network which has a d-dimensional vector linear solution, and let $\mathbb{D}$ be the corresponding discrete polymatroid as per Definition 6. 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 $\mathbb{D}$, and ρ be the rank function of $\mathbb{D}$. Define $\mathsf{g} = \rho \circ f$.

Lemma 3. $\mathsf{g}(S_1, S_2) = \mathsf{g}(S_1) + \mathsf{g}(S_2)$.

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 to [D1] of Definition 6, 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 Definition 6, the vector $v = \sum_{i \in f(S)} d\epsilon_{in}$ is in $\mathbb{D}_1$. Hence, from Definition 4 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 $|v(\{f(s_1), f(s_2), f(s_3), f(s_4)\})|$

is equal to $4d$, this implies: $4d \leq \rho(\{f(s_1), f(s_2), f(s_3), f(s_4)\})$. Also, from [D3] of Definition 6 we have: $\rho(f(s_1)) = \rho(f(s_2)) = \rho(f(s_3)) = \rho(f(s_4)) = d$. So,

$$\rho(f(s_1)) + \rho(f(s_2)) + \rho(f(s_3)) + \rho(f(s_4)) \leq \rho(\{f(s_1), f(s_2), f(s_3), f(s_4)\}) \tag{2.1}$$

On the other hand, from [P3] of Definition 4 we have:

$$\rho(\{f(s_1), f(s_2), f(s_3), f(s_4)\}) \leq \rho(f(s_1)) + \rho(f(s_2)) + \rho(f(s_3)) + \rho(f(s_4)) \tag{2.2}$$

From equations (2.1) and (2.2) we must have: $\rho(\{f(s_1), f(s_2), f(s_3), f(s_4)\}) = \rho(f(s_1)) + \rho(f(s_2)) + \rho(f(s_3)) + \rho(f(s_4))$. □

Lemma 4. *If $C \subseteq B$, then $\mathrm{g}(A, B) - \mathrm{g}(A, C) \leq \mathrm{g}(B) - \mathrm{g}(C)$*

Proof.

$$\begin{aligned}
&\mathrm{g}(A, C) + \mathrm{g}(B) \geq \mathrm{g}(A, B, C) + \mathrm{g}(C) && \text{[from [P3] of Definition 4]} \\
&\text{or, } \mathrm{g}(A, C) + \mathrm{g}(B) \geq \mathrm{g}(A, B) + \mathrm{g}(C) && \text{[as } C \subseteq B\text{]} \\
&\text{or, } \mathrm{g}(B) - \mathrm{g}(C) \geq \mathrm{g}(A, B) - \mathrm{g}(A, C)
\end{aligned}$$

□

Lemma 5. *Let E_1 and E_2 be set of edges such that $\mathrm{g}(S_1, E_1) = \mathrm{g}(S_1)$ and $\mathrm{g}(S_2, E_2) = \mathrm{g}(S_2)$. If $\bar{S}_1$ is a subset of S_1 and $\bar{S}_2$ is a subset of S_2, then $\mathrm{g}(\bar{S}_1, E_1) + \mathrm{g}(\bar{S}_2, E_2) = \mathrm{g}(\bar{S}_1, E_1, \bar{S}_2, E_2)$.*

Proof. Note that, due to Lemma 3, we have:

$$\mathrm{g}(S_1, E_1) + \mathrm{g}(S_2, E_2) = \mathrm{g}(S_1, E_1, S_2, E_2) \tag{2.3}$$

Now,

$$\begin{aligned}
&\mathrm{g}(S_2, E_2) - \mathrm{g}(\bar{S}_2, E_2) \\
&= \mathrm{g}(S_1, E_1, S_2, E_2) - \mathrm{g}(S_1, E_1) - \mathrm{g}(\bar{S}_2, E_2) && \text{[using equation 2.3]} \\
&\leq \mathrm{g}(S_1, E_1, S_2, E_2) - \mathrm{g}(S_1, E_1, \bar{S}_2, E_2) \\
&\leq \mathrm{g}(S_2, E_2) - \mathrm{g}(\bar{S}_2, E_2) && \text{[taking } A = \{S_1 \cup E_1\} \text{ in Lemma 4]}
\end{aligned} \tag{2.4}$$

From equation 2.4 we have:

$$\mathrm{g}(S_1, E_1, S_2, E_2) - \mathrm{g}(S_1, E_1, \bar{S}_2, E_2) = \mathrm{g}(S_2, E_2) - \mathrm{g}(\bar{S}_2, E_2) \tag{2.5}$$

$$\begin{aligned}
&\mathrm{g}(S_1, E_1) - \mathrm{g}(\bar{S}_1, E_1) \\
&= \mathrm{g}(S_1, E_1, S_2, E_2) - \mathrm{g}(S_2, E_2) - \mathrm{g}(\bar{S}_1, E_1) \qquad \text{[using equation 2.3]} \\
&\leq \mathrm{g}(S_1, E_1, S_2, E_2) - \mathrm{g}(\bar{S}_1, E_1, S_2, E_2) \qquad \text{[applying [P3] of Definition 4]} \\
&\leq \mathrm{g}(S_1, E_1, \bar{S}_2, E_2) - \mathrm{g}(\bar{S}_1, E_1, \bar{S}_2, E_2) \qquad \text{[taking } A = S_2 \setminus \bar{S}_2 \text{ in Lemma 4]} \\
&\leq \mathrm{g}(S_1, E_1) - \mathrm{g}(\bar{S}_1, E_1) \qquad \text{[taking } A = \bar{S}_2 \cup E_2 \text{ in Lemma 4]}
\end{aligned} \tag{2.6}$$

From equation 2.6 we have:

$$\mathrm{g}(S_1, E_1, \bar{S}_2, E_2) - \mathrm{g}(\bar{S}_1, E_1, \bar{S}_2, E_2) = \mathrm{g}(S_1, E_1) - \mathrm{g}(\bar{S}_1, E_1) \tag{2.7}$$

Adding equations (2.5) and (2.7) we get:

$$\begin{aligned}
&\mathrm{g}(S_1, E_1, S_2, E_2) - \mathrm{g}(S_1, E_1, \bar{S}_2, E_2) + \mathrm{g}(S_1, E_1, \bar{S}_2, E_2) - \mathrm{g}(\bar{S}_1, E_1, \bar{S}_2, E_2) \\
&\qquad = \mathrm{g}(S_2, E_2) - \mathrm{g}(\bar{S}_2, E_2) + \mathrm{g}(S_1, E_1) - \mathrm{g}(\bar{S}_1, E_1) \\
&\text{or, } \mathrm{g}(S_1, E_1, S_2, E_2) - \mathrm{g}(\bar{S}_1, E_1, \bar{S}_2, E_2) = \mathrm{g}(S_1, E_1, S_2, E_2) - \mathrm{g}(\bar{S}_2, E_2) - \mathrm{g}(\bar{S}_1, E_1) \\
&\text{or, } \mathrm{g}(\bar{S}_1, E_1, \bar{S}_2, E_2) = \mathrm{g}(\bar{S}_2, E_2) + \mathrm{g}(\bar{S}_1, E_1)
\end{aligned}$$

□

2.5 Some Conventions and Lemmas on Co-dimension

It can be seen from Theorem 1 and Definition 5 that existence of a (k, n) fractional linear network coding solution depends on whether there exists a corresponding representable discrete polymatroid. For a discrete polymatroid to be representable, there has to exist a certain set of vector subspaces of appropriate dimension (see Definition 5). In Chapter 5 we discuss linear rank inequalities that may decide whether a set of vector subspaces with given dimensions can exist. Here we present some conventions and lemmas that will be used in Chapter 5.

A list of conventions followed in this thesis:

(i) $\sum_{i=1}^{2} A_i + B$ is equal to $A_1 + A_2 + B$, and not equal to $(A_1 + B) + (A_2 + B)$. To indicate the

latter we write $\sum_{i=1}^{2}(A_i + B)$.

(ii) If A is a vector space, then $dim(A)$ denotes the dimension of A. In [32] and [33], $H(A)$ has been used to denote $dim(A)$, but we have refrained from this notation for our original contents in this thesis.

(iii) For two vector subspaces A and B of a finite dimensional vector space, $< A, B >$ denotes the vector space spanned by the vectors in $A \cup B$; $dim(A, B)$ denotes the dimension of $< A, B >$; $dim(A \cap B)$ denotes the dimension of the vector space spanned by the vectors in $A \cap B$; and $dim(A|B) = dim(A, B) - dim(B)$.

Grassmann's Identity states that $dim(A) + dim(B) = dim(A, B) + dim(A \cap B)$. Hence we have: $dim(A \cap B) = dim(A) - dim(A|B) = dim(B) - dim(B|A)$.

(iv) We define what is meant by inverse of a linear function. Let $f : A \to B$ be a linear function. If B' is a subspace of B, then $f^{-1}(B')$ denotes a vector subspace A' of A such that $f(A') = B'$. (This may be an abuse of notation as $f^{-1}()$ is not a well defined function unless $f()$ is one-to-one.)

If A is a subspace of V then co-dimension of A in V is $codim_V(A) = dim(V) - dim(A)$. The following lemmas are reproduced from [32]. The proofs of these lemmas are also reproduced here from [32] (other than Lemma 6, for which no proofs has been given in [32]). In all of these lemmas, V is a finite dimensional vector space, and $A, A_1, A_2, \ldots, A_m, B$ are subspaces of V.

Lemma 6. *[32, Lemma 2, p. 2501]*

$$codim_V(\cap_{i=1}^{m} A_i) \leq \sum_{i=1}^{m} codim_V(A_i)$$

Proof. We prove this by induction. The result trivially holds for $m = 1$. We show that the result holds for $m = 2$.

$$\begin{aligned}
&codim_V(A_1 \cap A_2) = dim(V) - dim(A_1 \cap A_2) \\
&= dim(V) - (dim(A_1) + dim(A_2) - dim(A_1, A_2)) \qquad \text{[from Grassmann's Identity]} \\
&= dim(V) + dim(A_1, A_2) - dim(A_1) - dim(A_2) \\
&\leq dim(V) + dim(V) - dim(A_1) - dim(A_2) \qquad \text{[Since } < A_1, A_2 > \text{ is a subspace of } V\text{]} \\
&= codim_V(A_1) + codim_V(A_2) \qquad (2.8)
\end{aligned}$$

Say, the lemma holds for $m = k$. We then prove that it holds for $m = k + 1$.

Let $C =< A_1, A_2, \ldots, A_k >$. Then,

$$\begin{aligned} codim_V(C \cap A_{k+1}) &\leq codim_V(C) + codim_V(A_{k+1}) && \text{[Proceeding similar to equation (2.8)]} \\ &\leq \sum_{i=1}^{k} codim_V(A_i) + codim_V(A_{k+1}) && \text{[due to the induction hypothesis]} \\ &= \sum_{i=1}^{k+1} codim_V(A_i) \end{aligned}$$

□

Lemma 7. *[32, Lemma 3, p. 2501] If $f : A \to B$ is a linear function and B' is a subspace of B, then*

$$codim_A(f^{-1}(B')) \leq codim_B(B')$$

Proof. Let T be the collection of all elements of A such that $T \cup f^{-1}(B') = A$ and $T \cap f^{-1}(B') = \{0\}$. Also note $f(T) \cap B' = \{0\}$ as otherwise, if $b \neq 0$ and $b \in B'$, then any $a \in A$ for which $f(a) = b$ is in $f^{-1}(B')$, and then, since $T \cap f^{-1}(B') = \{0\}$, there cannot be any $a \in T$ such that $f(a) = b$ (note a cannot be zero for f to be linear function).

Let T' be a subspace of T such that $f(T') = \{0\}$. Say $t \in T'$ such that $t \neq 0$. Now, as $f(t) = 0$ and $0 \in B'$, we have $t \in f^{-1}(B')$. But the latter is a contradiction to our assumption that $T \cap f^{-1}(B') = \{0\}$. Then, we must have $T' = \{0\}$. Now,

$$\begin{aligned} &codim_A(f^{-1}(B')) = dim(T) = dim(f(T)) + dim(T') \\ &= dim(f(T)) = dim(f(T), B') - dim(B') && \text{[as } f(T) \cap B' = \{0\}\text{]} \\ &\leq dim(B) - dim(B') = codim_B(B') \end{aligned}$$

□

Lemma 8. *[32, Lemma 4, p. 2501] There exist linear functions $f_i : A \to A_i$ for $1 \leq i \leq m$ such that $f_1 + \cdots + f_m = I$ on a subspace A' of A with*

$$codim_A(A') \leq dim(A|A_1, A_2, \ldots, A_m)$$

Proof. It can be shown that for any vector in the subspace $W =< A_1, A_2, \ldots, A_m > \cap A$ there exists such functions. Let w_j for $1 \leq j \leq dim(W)$ be the basis vectors of W. Write each basis

w_j as $w_j = \sum_{i=1}^{m} x_{ij}$ where $x_{ij} \in A_i$. (one way to construct this sum is this: arbitrarily select a subspace A_k among $A_1, A_2, \ldots, A_m$ such that w_j is an element of say A_k (it must be in at least one of $A_1, A_2, \ldots, A_m$), and make x_{kj} equal to w_j and set all other components equal to zero). Now construct f_i such that $f_i(w_j) = x_{ij}$ for $1 \leq i \leq m$ and $1 \leq j \leq dim(W)$, and extend f_i over A to construct a linear function $f_i : A \to A_i$. Then we have:

$$f_1(w_j) + f_2(w_j) + \cdots + f_m(w_j) = x_{1j} + x_{2j} + \cdots + x_{mj} = w_j \tag{2.9}$$

Let w be any vector in W where $w = \sum_{j=1}^{dim(W)} c_j w_j$. Then,

$$\begin{aligned}
&f_1(w) + f_2(w) + \cdots + f_m(w) \\
&= f_1(\sum_{j=1}^{dim(W)} c_j w_j) + f_2(\sum_{j=1}^{dim(W)} c_j w_j) + \cdots + f_m(\sum_{j=1}^{dim(W)} c_j w_j) \\
&= \sum_{j=1}^{dim(W)} c_j f_1(w_j) + \sum_{j=1}^{dim(W)} c_j f_2(w_j) + \cdots + \sum_{j=1}^{dim(W)} c_j f_m(w_j) \\
&= c_1(\sum_{i=1}^{m} f_i(w_1)) + c_2(\sum_{i=1}^{m} f_i(w_2)) + \cdots + c_{dim(W)}(\sum_{i=1}^{m} f_i(w_{dim(W)})) \\
&= c_1 w_1 + c_2 w_2 + \cdots + c_{dim(W)} w_{dim(W)} \qquad \text{[from equation (2.9)]} \\
&= w
\end{aligned}$$

So f_i for $1 \leq i \leq m$ become the functions the lemma asserts. Then $A' = W$.

$$\begin{aligned}
codim_A(W) &= dim(A) - dim(W) = dim(A) - dim(< A_1, A_2, \ldots, A_m > \cap A) \\
&= dim(A) - dim(A_1, A_2, \ldots, A_m) - dim(A) + dim(A, A_1, A_2, \ldots, A_m) \\
&= dim(A|A_1, A_2, \ldots, A_m)
\end{aligned}$$

□

Lemma 9. *[32, Lemma 6, p. 2502] For $1 \leq i \leq m$, let $f_i : A \to A_i$ be linear functions such that $f_1 + f_2 + \cdots + f_m = 0$ on A. Then $f_1 = \cdots = f_m = 0$ on a subspace A' of A with*

$$codim_A(A') \leq dim(A_1) + dim(A_2) + \cdots + dim(A_m) - dim(A_1, A_2, \ldots, A_m)$$

Proof. The result is proved by induction. For $m = 1$, the result holds trivially. Let $m = 2$. For any $a \in A$, $f_1(a) + f_2(a) = 0$ implies that $f_1(a)$ and $f_2(a)$ must be in the same subspace, which is equal to $A_1 \cap A_2$. Let $\bar{A}_1$ be the subspace such that $\bar{A}_1 \cup (A_1 \cap A_2) = A_1$ and $\bar{A}_1 \cap (A_1 \cap A_2) = \{0\}$ (*i.e.* $\bar{A}_1$

is the complement subspace of $A_1 \cap A_2$ in A_1). Then for all $a \in A$ such that $f_1(a) \in \bar{A}_1$, it must be that $f_1(a) = 0$ (as $f_1(a)$ must also lie in $A_1 \cap A_2$); and $f_2(a) = 0$ (as $f_1(a) + f_2(a) = 0$). Similarly for all $a \in A$ such that $f_2(a)$ lie in $\bar{A}_2$ – which is defined as the complement subspace of $A_1 \cap A_2$ in A_2 – it must be that $f_2(a) = 0$ and $f_1(a) = 0$. So we have $A' = \bar{A}_1 \cup \bar{A}_2$. Then,

$$codim_A(A') = dim(A_1 \cap A_2) = dim(A_1) + dim(A_2) - dim(A_1, A_2) \tag{2.10}$$

The induction hypothesis assumes that the result holds for $m = k$. It is to be shown that the result holds for $m = k+1$. According to the proposition of the lemma, $f_1 + f_2 + \cdots + f_k + f_{k+1} = 0$ on A. Then proceeding similar to above we know that for any $a \in A$, $f_1(a) + f_2(a) + \cdots + f_k(a) = 0$ and $f_{k+1}(a) = 0$ over a subspace A^* of A which is the complement subspace of $< A_1, A_2, \ldots, A_k > \cap A_{k+1}$ in A. So,

$$codim_A(A^*) = dim(A_1, A_2, \ldots, A_k) + dim(A_{k+1}) - dim(A_1, A_2, \ldots, A_k, A_{k+1}) \tag{2.11}$$

Due to the induction hypothesis (the assumption of the induction) we also know that over a subspace A' of A^* we have $f_1 = f_2 = \cdots = f_k = 0$ where,

$$codim^*_A(A') \leq dim(A_1) + dim(A_2) + \cdots + dim(A_k) - dim(A_1, A_2, \ldots, A_k) \tag{2.12}$$

Then,

$$\begin{aligned} codim_A(A') &= codim_A(A^*) + codim^*_A(A') \\ &\leq dim(A_1) + dim(A_2) + \cdots + dim(A_k) + dim(A_{k+1}) \\ &\quad - dim(A_1, A_2, \ldots, A_k, A_{k+1}) \end{aligned}$$

□

2.6 Dimensions of Vector Spaces Obey Information Inequalities

Here we reproduce a proof from [26] which shows that information inequalities are a subset of linear rank inequalities. First the definition of an information inequality is reproduced from [23].

Definition 7. *Let $S_1, S_2, \ldots, S_k$ be subsets of $\{1, 2, \ldots, n\}$ where k and n are positive integers. Let*

$\alpha_i \in \mathbb{R}$ for $1 \leq i \leq k$. Then an inequality of the form

$$\alpha_1 H(\{A_i | i \in S_1\}) + \alpha_2 H(\{A_i | i \in S_2\}) + \cdots + \alpha_k H(\{A_i | i \in S_k\}) \geq 0 \tag{2.13}$$

is called information inequality if it holds for all jointly distributed random variables $A_1, A_2, .., A_n$.

An information inequality is called Shannon-type information inequality if it can be expressed in the form ([8]):

$$\sum_i \alpha_i I(A_i, B_i | C_i) \geq 0 \tag{2.14}$$

where $I(A_i; B_i | C_i) = H(A, C) + H(B, C) - H(C) + H(A, B, C)$.

Hammer *et al.* showed in Theorem 2 of [26] that any Shannon information inequality is also obeyed by dimensions of the vector subspaces of a finite dimensional vector space. But this result can easily be extended to show that in all information inequalities, if the entropy function is replaced by the dimension function and the random variables represent vector subspaces, then the inequality still remains valid. Below we reproduce the first part of the proof of Theorem 2 of [26] (This theorem proves the result for any vector space, but we only show the part for finite dimensional vector spaces).

Theorem 10. *Any linear inequality valid for Shannon entropy is valid for ranks (dimensions) of vector subspaces of a finite dimensional vector space over any finite field.*

Consider vector subspaces $V_1, V_2, \ldots, V_n$ of a finite dimensional vector space V over a finite field $\mathbb{F}_q$. The proof constructs random variables $R_1, R_2, \ldots, R_n$ such that for any $S \subseteq \{1, 2, \ldots, n\}$: $dim(\sum_{i \in S} V_i) = \frac{H(\{R_i | i \in S\})}{\log q}$.

We now show how to construct the random variables $R_1, R_2, \ldots, R_n$ (proof reproduced from [26]). Consider a random linear function $R : V \rightarrow \mathbb{F}_q$. Let R_i be the restricted function $R|_{V_i}$ (domain restricted to the subset V_i). This function is the random variable corresponding to V_i.

$R|_{V_i}$ is a random linear function that maps each element of V_i to an element of $\mathbb{F}_q$. All elements of V_i can be expressed as a $dim(V_i)$ length vector over $\mathbb{F}_q$. Then $R|_{V_i}$ can be expressed as a $1 \times dim(V_i)$ sized matrix (since all linear functions can be represented as a matrix transformation) (This matrix right multiplies the vector). Since there can be $q^{dim(V_i)}$ number of $1 \times dim(V_i)$ matrices, $H(R|_{V_i}) = dim(V_i) \log q$.

For the vector subspace $\sum_{i \in S} V_i$ where $S \subseteq \{1, 2, \ldots, n\}$, the corresponding constructed random variable is $R|_{\sum_{i \in S} V_i}$. Like earlier, $R|_{\sum_{i \in S} V_i}$ is a $1 \times dim(\sum_{i \in S} V_i)$ sized matrix; and hence

$H(R|_{\sum_{i\in S} V_i}) = dim(\sum_{i\in S} V_i)\log q$. This completes the proof.

3

Dependency of a linear solution on the message dimension

Contents

It is known that scalar linear network coding is sufficient to achieve the capacity of all multicast networks. However, there are non-multicast networks having no scalar linear solution but have a vector linear solution. To the best of our knowledge, till we started our work in 2015, there were five such reported networks/class of networks in the literature. Here's a chronological list: (i) Lehman *et al.* in [41] showed that from an unsatisfiable 3-CNF formula a network can be constructed such that the network has no scalar linear solution but has a 2-dimensional vector linear solution. (ii) Médard *et al.* in [3] showed a network, named as the M-network, which has no scalar linear solution but has 2-dimensional vector linear solution. We reproduce this network in Fig. 3.1. The network has four sources s_1, s_2, s_3, s_4 and four terminals t_1, t_2, t_3, t_4. The message vector generated by the source s_i is denoted by X_i. The demands of the terminals are shown below each terminal inside round brackets. The proof that the M-network does not have a scalar linear solution can be found in [3]. A 2-dimensional vector linear solution of the M-network is reproduced in Fig. 3.2 from [3]. In [8] the M-network was shown to have a d-dimensional vector linear solution if and only if d is a multiple of 2. (iii) Riis, in [42], showed two networks (in Fig. 5 and Fig. 7 of [42]) which have no scalar linear solutions but both have a 3-dimensional vector linear solution. (iv) The non-Pappus network shown by Rouayheb *et al.* in [43] has no scalar linear solution but has a 2-dimensional vector linear solution. (v) Muralidharan *et al.* showed a network in Fig. 4 of [35] that has no scalar linear solution but has a 2-dimensional vector linear solution.

To the best of our understanding, it is not shown in the literature how the networks of (i), (iii), (iv) and (v) behave for other/higher message dimensions. But, from the M-network of (ii), a natural question emerges: whether for any positive integer $m \geq 2$, there exists a network which admits an m dimensional vector linear solution but has no vector linear solution over any finite field when message dimension is less than m.

In [8], it was shown that the notion of scalar linear solvability of networks can be captured by matroids. Specifically, it was shown that a network is scalar linearly solvable only if it is a matroidal network associated with a representable matroid over a finite field. The converse of this result was proved in [38]. [35] generalized the results of [8] and [38] to the vector linearly solvable networks and showed that the existence of an m dimensional vector linear network code solution implies the existence of a discrete polymatroid with certain properties and vice versa. To show that for any positive integer $m \geq 2$ there exists a network which has an m dimensional vector linear solution but has no vector

linear solution for a message dimension less than m, either one has to give construction of such a network, or equivalently, one can construct a discrete polymatroid such that it is representable if the rank of its every element is allowed to be less than or equal to m, but not representable if the rank of its every element is strictly lesser than m [35]. To the best of our knowledge, neither such a network has been presented in the literature nor it has been shown that for every integer $m \geq 2$ there do not exist such networks; likewise in the area of matroid theory, no discrete polymatroid having the above mentioned property has been reported nor it has been shown that such a discrete polymatroid does not exist.

First, we show that for any positive integer $m \geq 2$ there exists a network $\mathcal{N}_m$ which has a w-dimensional vector linear solution if and only if w is a multiple of m. This shows that indeed, for any positive integer $m \geq 2$ there exists a network which has no w-dimensional vector linear solution for any w less than m, but has a m-dimensional vector linear solution.

Subsequent to our work, in reference [44] a network named as the Dim-k network was presented, which behaves similar to the network $\mathcal{N}_m$ shown by us. The Dim-k network has an w-dimensional vector linear solution if and only if w is a positive integer multiple of k. The M-network, the network $\mathcal{N}_m$ for all integers $m \geq 3$, and the Dim-k network for all integers $k \geq 3$ have a common property: for each network, there exists a positive integer m such that the network has a w-dimensional vector linear solution if and only if w is a positive integer multiple of m (to the best of our knowledge there exists no other network in the literature whose behaviour for message dimensions greater than 3 has been analysed). Is this a general property of all networks that have a vector linear solution but have no scalar linear solution? We answer this question in the negative by showing that for any positive integer $m \geq 2$, there exists a network which has no vector linear solution if the message dimension is less than m, but has a vector linear solution for all message dimensions greater than or equal to m. We prove this result by constructing a network that we name as the MDim-m ($m \geq 3$) network (short form of 'modified Dim-m').

We also generalize these results to show that (i) for any positive integer $m \geq 2$, there exists a network which has a (wk, wn) fractional linear solution if and only if w is a multiple of m, (ii) for any positive integer $m \geq 2$, there exists a network which has a (wk, wn) fractional linear solution if and only if w is greater than or equal to m.

In Section 3.1, we show that for any positive integer m there exists a network which has a w-

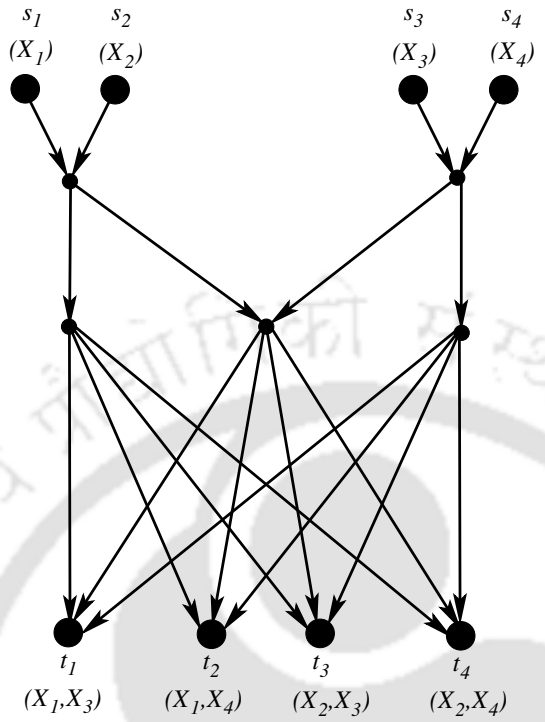

Figure 3.1: The M-network reproduced from [3].

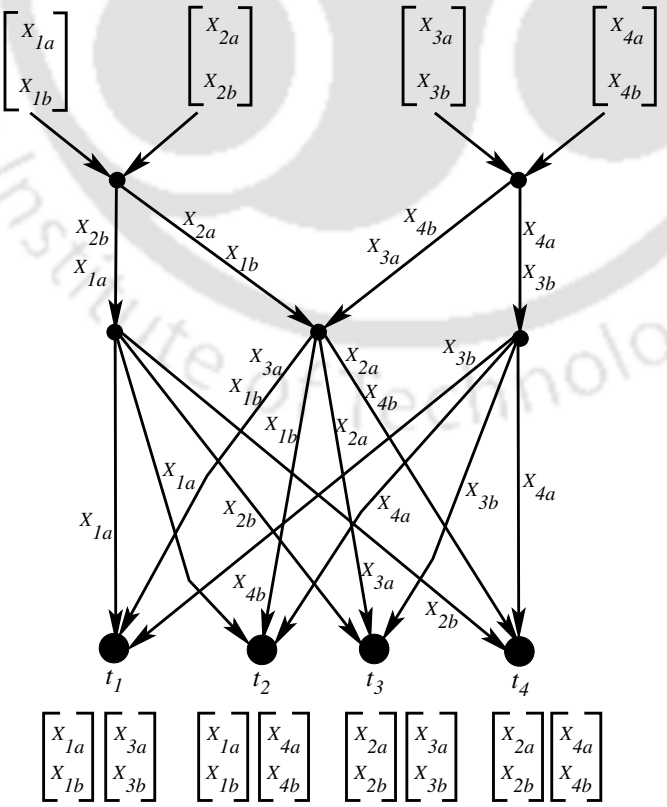

Figure 3.2: A 2-dimensional vector linear solution of the M-network.

dimensional vector linear solution if and only if w is a positive integer multiple of m. In Section 3.2 we show that for any positive integer m, there exits a network which has a (wk, wn) fractional linear solution if and only if w is a positive integer multiple of m. In Section 3.3 we show that for any positive integer $m \geq 2$, there exists a network which has a w-dimensional vector linear solution if and only if w is greater than or equal to m. We then generalize these results to show that for any positive integers k, n, and $m \geq 2$, there exists a network which has a (wk, wn) fractional linear solution if and only if w is greater than or equal to m.

3.1 Generalized M-network

Theorem 11. *For any positive integers $m \geq 2$ and d, there exists a network which has a d-dimensional vector linear solution if and only if d is a multiple of m.*

Proof. We prove this result using the network shown in Fig. 3.3. We show that the network $\mathcal{N}_m$ presented in Fig. 3.3 has a d-dimensional vector linear solution if and only if d is a multiple of m. First we give a description of the network.

$\mathcal{N}_m$ has m^2 sources and m^m terminals. The sources are partitioned into m sets $S_1, S_2, \ldots, S_m$ where $S_i = \{s_{i1}, s_{i2}, \ldots, s_{im}\}$ for $1 \leq i \leq m$ (so each of these sets contains m number of source nodes). The source s_{ij} generates the message X_{ij}. Below we list the edges in the network:

(i) An edge (s_{ij}, u_i) for $1 \leq i, j \leq m$.

(ii) An edge $e_{ii} = (u_i, v_i)$ and an edge $e_{ij} = (u_i, v_j)$ for $1 \leq i \leq m$ and $m+1 \leq j \leq 2m-1$.

(iii) An edge (v_i, t_j) for $1 \leq i \leq 2m-1$ and $1 \leq j \leq m^m$.

The message transmitted over the edge (s_{ij}, u_i) is considered to be equal to X_{ij}. The message transmitted over the edge e_{ij} is denoted by Y_{ij} for $1 \leq i \leq m$, $1 \leq j \leq 2m-1$; and the message transmitted over the edge (v_i, t_j) is denoted by Z_{ij} for $m+1 \leq i \leq 2m-1$ and $1 \leq j \leq m^m$.

Each terminal demands a unique tuple of m source messages where the i^{th} element of the tuple could be any element from the set S_i. So there are m^m number of such tuples; and for each such tuple there is a terminal that demands the message vector generated by the sources in the tuple. W.l.o.g, we assume that t_1 demands the source messages: $X_{11}, X_{21}, \ldots, X_{m1}$.

We note that for $m = 2$, $\mathcal{N}_m$ is the M-network presented in [3].

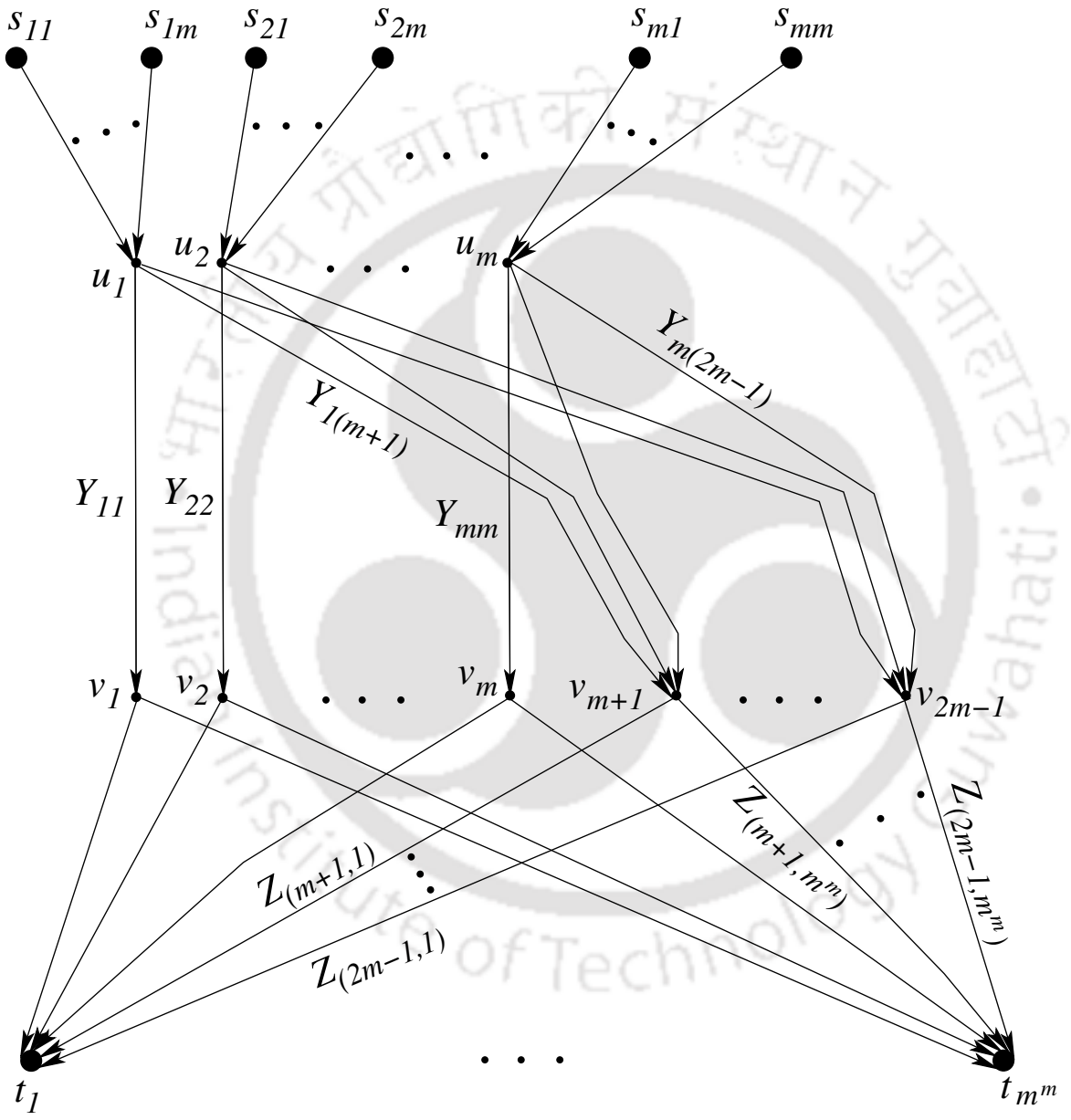

Figure 3.3: A communication network $\mathcal{N}_m$ – named as the "generalized M-network"– has a d-dimensional vector linear solution if and only if d is a multiple of m.

Our proof, in principle, is similar to that used in [8] to show that the M-network is not a matroidal network. First we consider the only if part. So, we show that if $\mathcal{N}_m$ has a d-dimensional vector linear solution then d is a multiple of m. From Theorem 2 we know that if $\mathcal{N}_m$ has a d-dimensional vector linear solution then it is a (d, d)-discrete polymatroidal network with respect to a representable discrete polymatroid. Let this discrete polymatroid be $\mathbb{D}$. Also let ρ be the rank function of $\mathbb{D}$. From Definition 4 we get that for a network to be a (d, d)-discrete polymatroidal network there must exists a function that maps the sources and edges of the network to the elements of $\mathbb{D}$ conforming to the rules of mapping given in the definition. Let f be this function. Now let $\mathsf{g} = \rho \circ f$. (In Definition 6, S is the set of sources and E is the set of edges, but if X_s is the message generated by a source s, and if Y_e is the symbols carried by an edge e, there is a one-to-one correspondence between s and X_s, as well as between e and Y_e, and hence, the Definition 6 holds if S is the set of messages generated by the sources and E is the set of symbols carried by the edges.)

Our proof depends on the following two sets of inequalities.

Set I:

$$\mathsf{g}(Y_{11}, X_{1j_1}) + \mathsf{g}(Y_{22}, X_{2j_2}) + \cdots + \mathsf{g}(Y_{mm}, X_{mj_m}) \leq (2m-1)d \tag{3.1}$$
$$\text{where } j_i \in \{1, 2, \ldots, m\}, \text{ for } 1 \leq i \leq m.$$

Set II:

$$\mathsf{g}(Y_{ii}, X_{i1}) + \mathsf{g}(Y_{ii}, X_{i2}) + \cdots + \mathsf{g}(Y_{ii}, X_{im}) \geq (2m-1)d \text{ for } 1 \leq i \leq m. \tag{3.2}$$

Claim 1. *The inequalities in Set I hold true.*

Proof.

$$\begin{aligned}
&\mathsf{g}(Y_{11}, X_{11}) + \mathsf{g}(Y_{22}, X_{21}) + \cdots + \mathsf{g}(Y_{mm}, X_{m1}) \\
&= \mathsf{g}(Y_{11}, X_{11}, Y_{22}, X_{21}, \ldots, Y_{mm}, X_{m1}) \qquad \text{[using Lemma 5 repetitively]} \\
&\leq \mathsf{g}(Y_{11}, X_{11}, Y_{22}, X_{21}, \ldots, Y_{mm}, X_{m1}, Z_{(m+1,1)}, Z_{(m+2,1)}, \ldots, Z_{(2m-1,1)}) \\
&= \mathsf{g}(Y_{11}, Y_{22}, \ldots, Y_{mm}, Z_{(m+1,1)}, \ldots, Z_{(2m-1,1)}) \qquad (3.3) \\
&\leq (2m-1)d. \qquad (3.4)
\end{aligned}$$

The equation (3.3) is true because the terminal t_1 computes $(X_{11}, X_{21}, \ldots, X_{m1})$ from the messages

$\{Y_{11}, Y_{22}, \ldots, Y_{mm}, Z_{(m+1,1)}, Z_{(m+2,1)}, \ldots, Z_{(2m-1,1)}\}$. Equation (3.4) is true because each element can have rank maximum of d and there are $(2m-1)$ elements. This concludes the proof of Claim 1. □

Claim 2. *The inequalities in Set II hold true.*

Proof. We will give the proof of the inequality for $i = 1$. The rest can be proved similarly. First we show that $\mathsf{g}(Y_{ii}) = \mathsf{g}(Y_{ij}) = d$ for $1 \leq i \leq m, m+1 \leq j \leq 2m-1$. Since all source messages are independent,

$$\begin{aligned}
&m^2 d = \mathsf{g}(X_{11}, X_{12}, \ldots, X_{mm}) \\
&\leq \mathsf{g}(X_{11}, \ldots, X_{mm}, Y_{11}, \ldots, Y_{mm}, Y_{1(m+1)}, \ldots, Y_{m(2m-1)}) \\
&= \mathsf{g}(Y_{11}, Y_{22}, \ldots, Y_{mm}, Y_{1(m+1)}, Y_{1(m+2)}, \ldots, Y_{m(2m-1)}) \qquad (3.5) \\
&\leq \mathsf{g}(Y_{11}) + \mathsf{g}(Y_{22}) + \cdots + \mathsf{g}(Y_{mm}) + \mathsf{g}(Y_{1(m+1)}) + \mathsf{g}(Y_{1(m+2)}) + \cdots + \mathsf{g}(Y_{m(2m-1)}) \\
&\leq md + m(m-1)d = m^2 d.
\end{aligned}$$

Equality in (3.5) follows because every symbol is demanded by some terminal. Hence,

$$\mathsf{g}(Y_{11}) + \mathsf{g}(Y_{22}) + \cdots + \mathsf{g}(Y_{mm}) + \mathsf{g}(Y_{1(m+1)}) + \mathsf{g}(Y_{1(m+2)}) + \cdots + \mathsf{g}(Y_{m(2m-1)}) = m^2 d. \qquad (3.6)$$

Since, there are m^2 terms and each term can take a maximum value of d,

$$\mathsf{g}(Y_{ii}) = \mathsf{g}(Y_{ij}) = d \text{ for } 1 \leq i \leq m \text{ and } m+1 \leq j \leq 2m-1. \qquad (3.7)$$

Now we prove the inequality:

$$\begin{aligned}
&\mathsf{g}(Y_{11}, X_{11}) + \mathsf{g}(Y_{11}, X_{12}) + \cdots + \mathsf{g}(Y_{11}, X_{1m}) \\
&\geq \mathsf{g}(Y_{11}, X_{11}, X_{12}) + \mathsf{g}(Y_{11}) + \cdots + \mathsf{g}(Y_{11}, X_{1m}) \qquad \text{[applying P3 of Definition 4]} \\
&\geq \mathsf{g}(Y_{11}, X_{11}, X_{12}, X_{13}) + 2\mathsf{g}(Y_{11}) + \cdots + \mathsf{g}(Y_{11}, X_{1m}) \\
&\qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots \\
&\geq \mathsf{g}(Y_{11}, X_{11}, X_{12}, \ldots, X_{1m}) + (m-1)\mathsf{g}(Y_{11}) \\
&= md + (m-1)d = (2m-1)d.
\end{aligned}$$

Here we have used condition [P3] from Definition 4 repeatedly. This concludes the proof of Claim 2. □

We prove the theorem by finding a constraint on the rank function using the inequalities in Set I

and Set II. We show that $\mathsf{g}(Y_{ii}, X_{ij}) = \frac{(2m-1)d}{m}$ for $1 \leq i, j \leq m$. We will give the proof only for $\mathsf{g}(Y_{mm}, X_{m1}) = \frac{(2m-1)d}{m}$. The rest can be proved similarly. To prove that $\mathsf{g}(Y_{mm}, X_{m1}) = \frac{(2m-1)d}{m}$, we consider an inequality from Set I which has $\mathsf{g}(Y_{mm}, X_{m1})$ on the left hand side. We then eliminate (one by one) all the rest of the terms except $\mathsf{g}(Y_{mm}, X_{m1})$ from left hand side using other inequalities from the Set I and inequalities from Set II. Consider the inequality:

$$\mathsf{g}(Y_{11}, X_{11}) + \mathsf{g}(Y_{22}, X_{21}) + \cdots + \mathsf{g}(Y_{mm}, X_{m1}) \leq (2m-1)d. \tag{3.8}$$

Now consider all other inequalities from Set I which differ only at the first term of the above inequality. There are exactly $m-1$ such inequalities. These inequalities are written below:

$$\begin{aligned}
&\mathsf{g}(Y_{11}, X_{12}) + \mathsf{g}(Y_{22}, X_{21}) + \cdots + \mathsf{g}(Y_{mm}, X_{m1}) \leq (2m-1)d \\
&\mathsf{g}(Y_{11}, X_{13}) + \mathsf{g}(Y_{22}, X_{21}) + \cdots + \mathsf{g}(Y_{mm}, X_{m1}) \leq (2m-1)d \\
&\qquad\vdots \qquad\qquad\vdots \qquad\qquad\vdots \\
&\mathsf{g}(Y_{11}, X_{1m}) + \mathsf{g}(Y_{22}, X_{21}) + \cdots + \mathsf{g}(Y_{mm}, X_{m1}) \leq (2m-1)d.
\end{aligned}$$

Summing up all of the above $m-1$ inequalities and the inequality in the equation (3.8), we get:

$$\mathsf{g}(Y_{11}, X_{11}) + \mathsf{g}(Y_{11}, X_{12}) + \cdots + \mathsf{g}(Y_{11}, X_{1m}) + m\big\{\mathsf{g}(Y_{22}, X_{21}) + \cdots + \mathsf{g}(Y_{mm}, X_{m1})\big\} \leq m(2m-1)d.$$

From Set II, we know that $\mathsf{g}(Y_{11}, X_{11}) + \mathsf{g}(Y_{11}, X_{12}) + \cdots + \mathsf{g}(Y_{11}, X_{1m}) \geq (2m-1)d$. Substituting this in the above equation, we get:

$$m\big\{\mathsf{g}(Y_{22}, X_{21}) + \mathsf{g}(Y_{33}, X_{31}) + \cdots + \mathsf{g}(Y_{mm}, X_{m1})\big\} \leq m(2m-1)d - (2m-1)d. \tag{3.9}$$

Note that the term $\mathsf{g}(Y_{11}, X_{11})$ has been eliminated in the equation (3.9). In the similar manner as above, we can show that

$$\text{for } 2 \leq j \leq m: \; m\big\{\mathsf{g}(Y_{22}, X_{2j}) + \mathsf{g}(Y_{33}, X_{31}) + \cdots + \mathsf{g}(Y_{mm}, X_{m1})\big\} \leq m(2m-1)d - (2m-1)d.$$

Summing up the above $m-1$ inequalities and the inequality in the equation (3.9), we get:

$$\begin{aligned}
m\mathsf{g}(Y_{22}, X_{21}) + m\mathsf{g}(Y_{22}, X_{22}) + \cdots + m\mathsf{g}(Y_{22}, X_{2m}) + m^2\mathsf{g}(Y_{33}, X_{31}) + \cdots + m^2\mathsf{g}(Y_{mm}, X_{m1}) \\
\leq m^2(2m-1)d - m(2m-1)d.
\end{aligned} \tag{3.10}$$

From Set II, we have $\mathsf{g}(Y_{22}, X_{21}) + \mathsf{g}(Y_{22}, X_{22}) + \cdots + \mathsf{g}(Y_{11}, X_{2m}) \geq (2m-1)d$. Using this inequality

in the equation (3.10), we have:

$$m^2\mathsf{g}(Y_{33}, X_{31}) + \cdots + m^2\mathsf{g}(Y_{mm}, X_{m1}) \leq m^2(2m-1)d - 2m(2m-1)d. \tag{3.11}$$

Note that, in the above inequality, the term $\mathsf{g}(Y_{22}, X_{21})$ from the equation (3.9) has been eliminated and thereby the terms $\mathsf{g}(Y_{11}, X_{11})$ and $\mathsf{g}(Y_{22}, X_{21})$ from the equation (3.8) have been eliminated. In this way, eliminating term after term from the left hand side of the equation (9), we get

$$m^{m-1}\mathsf{g}(Y_{mm}, X_{m1}) \leq m^{m-1}(2m-1)d - (m-1)m^{m-2}(2m-1)d \tag{3.12}$$

$$\text{And hence,} \quad \mathsf{g}(Y_{mm}, X_{m1}) \leq \frac{(2m-1)d}{m}. \tag{3.13}$$

Similarly, it can be shown that

$$\mathsf{g}(Y_{mm}, X_{mj}) \leq \frac{(2m-1)d}{m} \quad \text{for } 2 \leq j \leq m. \tag{3.14}$$

From Set II, we have that $\mathsf{g}(Y_{mm}, X_{m1}) + \mathsf{g}(Y_{mm}, X_{m2}) + \cdots + \mathsf{g}(Y_{mm}, X_{mm}) \geq (2m-1)d$. Hence, it must be that

$$\mathsf{g}(Y_{mm}, X_{m1}) = \frac{(2m-1)d}{m}. \tag{3.15}$$

Note that for any integer m, $\gcd(2m-1, m) = 1$. Also, by definition, the rank function is integer valued. Therefore, for $\mathsf{g}(Y_{ii}, X_{ij})$ to be a positive integer, d has to be a positive integer multiple of m. Thus, by Theorem 2, for $\mathcal{N}_m$ to be vector linearly solvable, it is necessary that the message dimension is a positive integer multiple of m.

Now we prove the if part by describing a coding scheme that achieves an m dimensional vector linear solution. In fact, our coding scheme is a routing scheme. Let the k^{th} symbol of the source s_{ij} is denoted by X_{ijk} where $1 \leq k \leq m$. The edge e_{ii} for $1 \leq i \leq m$ carries the following m length vector: $[X_{i11}, X_{i21}, \ldots, X_{im1}]$. And the edge e_{ij} for $1 \leq i \leq m$ and $m+1 \leq j \leq 2m-1$, carries the vector $[X_{i1(j-m+1)}, X_{i2(j-m+1)}, \ldots, X_{im(j-m+1)}]$. Now, for any terminal it can be seen that the demands can be satisfied just by routing the required symbols from v_i for $1 \leq i \leq 2m-1$ to the terminals. For example, the demands of the terminal t_1 is met in the following way: the terminal t_1 gets X_{i11} from the message coming from (v_i, t_1) for $1 \leq i \leq m$; and $[X_{11(j+1)}, X_{21(j+1)}, \ldots, X_{m1(j+1)}]$ for $1 \leq j \leq m-1$ from the edge (v_{m+j}, t_1). □

As a consequence of Theorem 11, we have the following corollary:

Corollary 12. *For any positive integer m there exists a network which has no w-dimensional vector linear solution if $w < m$.*

3.2 Role of Message Dimension in Fractional Linear Network Coding

In the above section we have seen that for any positive integer $m \geq 2$ there exists a network which has a w-dimensional vector linear solution if and only if w is an integer multiple of m. In this section we extend this result to fractional linear network coding. We show that for any positive integers k, n, and $m \geq 2$ there exists a network which has a (wk, wn) fractional linear network coding solution if and only if w is a positive integer multiple of m. Using this result we establish the fact that for any positive rational number k/n and for any arbitrary large number m, there exists a network in which to achieve a k/n linear coding rate the message dimension has to be larger than m.

Towards establishing this result, for any network $\mathcal{N}$ we first define a network called as the n-factored network of $\mathcal{N}$. Let us consider a network $\mathcal{N}$. Without loss of generality assume that each source of $\mathcal{N}$ generates only one random process and each terminal demands information from only one source. (The following transformation preserves solvability. If a source s generates r random processes, then add r new nodes; let each of these new nodes generate only one unique random process from the r random processes generated by s; from each of these new nodes add an outgoing edge to the original source node s; and let s act as an intermediate node and not a source. If a terminal t demands messages from r sources; then add r new nodes; let each of these new nodes demand information from only one unique source from the r sources demanded by t; from t add an outgoing edge to each of these new nodes; and let t act as an intermediate node and not a terminal. It can be easily shown that the resultant network is solvably equivalent to the original network. Note that $\mathcal{N}$ does not necessarily has to be a multiple-unicast network to satisfy this property.)

To construct the n-factored network of $\mathcal{N}$ a sub-graph is added to each of the sources and each of the terminals. For each source node s in $\mathcal{N}$, the sub-graph added to s is shown in Fig. 3.4. This sub-graph contains n new source nodes $s_1, s_2, \ldots, s_n$ and an intermediate node s'. For $1 \leq i \leq n$ each source s_i is connected to s' by an edge (s_i, s'). The node s' is connected to s by an edge (s', s). Similarly, for each terminal node t the sub-graph added to t is shown in Fig. 3.5. This sub-graph contains n new terminal nodes say $t_1, t_2, \ldots, t_n$ and an intermediate node say t'. The node t' is

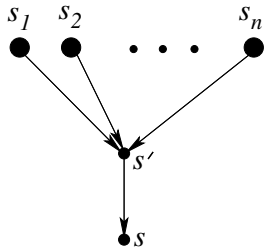

Figure 3.4: Sub-graph that attaches to the source node s in the original network. Nodes $s_1, s_2, \ldots, s_n$, s', and edges (s_i, s') for $1 \leq i \leq n$ and (s', s), are part of this sub-graph.

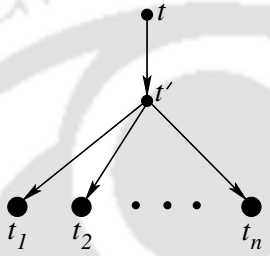

Figure 3.5: Sub-graph that attaches to the terminal node t in the original network. Nodes $t_1, t_2, \ldots, t_n$, t', and edges (t', t_i) for $1 \leq i \leq n$ and (t, t'), are part of this sub-graph.

connected to each terminal t_i by an edge (t', t_i) for $1 \leq i \leq n$; and t is connected to t' by an edge (t, t'). In the n-factored network of $\mathcal{N}$, the nodes s and t are intermediate nodes. The demands of the terminals in the n-factored network of $\mathcal{N}$ are set in the following way. If any terminal t of $\mathcal{N}$ demands information from a source s, then in the n-factored network of $\mathcal{N}$, each of the n terminals in the sub-graph connected from t demands the message generated by one unique source present in the sub-graph connected to s, *i.e.*, in the figure say t_i demands s_i. We now consider the following theorem.

Theorem 13. *For any network $\mathcal{N}$, the n-factored network of $\mathcal{N}$ has a $(1, n)$ fractional linear network coding solution over $\mathbb{F}_q$ if and only if $\mathcal{N}$ has an n-dimensional vector linear solution over $\mathbb{F}_q$.*

Proof. Let us denote the the n-factored network of $\mathcal{N}$ by $\mathcal{N}^n$. Consider a source node s and a terminal node t of $\mathcal{N}$ such that t demands the messages generated by s. Both of these two nodes are intermediate nodes in $\mathcal{N}^n$. As earlier, let the non-source node in the sub-graph that attaches to s be denoted by s'; the non-terminal node in the sub-graph that attaches to t be denoted by t'; the source nodes connected to s' be denoted by $s_1, s_2, \ldots, s_n$; and the terminal nodes connected from t' be denoted by $t_1, t_2, \ldots, t_n$. Without loss generality we assume that t_i demands the message generated by the source s_i for $1 \leq i \leq n$. Let the messages transmitted by the edges (s', s) and (t, t') of $\mathcal{N}^n$ be

denoted by $Y_{(s',s)}$ and $Y_{(t,t')}$ respectively. And let the random process generated by the source s_i be denoted by X_{s_i}.

Consider the only if part. We show that a $(1, n)$ fractional linear network code solution for $\mathcal{N}^n$ implies a n-dimensional vector linear solution of $\mathcal{N}$. To show this, we will design the local coding matrices of $\mathcal{N}$ using the local coding matrices of $\mathcal{N}^n$. In $\mathcal{N}^n$ let the local coding matrix associated with the edge pair $((s_i, s'), (s', s))$ be denoted by $A_{(s_i,s)}$. Then we have:

$$Y_{(s',s)} = A_{(s_1,s)}X_{s_1} + A_{(s_2,s)}X_{s_2} + \cdots + A_{(s_n,s)}X_{s_n}.$$

For $1 \leq i \leq n$, $A_{(s_i,s')}$ is a local coding matrix of size $n \times 1$ (n-length column vector); and X_{s_i} is an element from the finite field $\mathbb{F}_q$. It can be seen that the n-length vector $Y_{(s',s)}$ can also be represented as

$$Y_{(s',s)} = \begin{bmatrix} A_{(s_1,s')} & A_{(s_2,s')} & \cdots & A_{(s_n,s')} \end{bmatrix} \begin{bmatrix} X_{s_1} \\ X_{s_2} \\ \vdots \\ X_{s_n} \end{bmatrix}.$$

Let A_s be the matrix $\begin{bmatrix} A_{(s_1,s')} & A_{(s_2,s')} & \cdots & A_{(s_n,s')} \end{bmatrix}$, and X_s be the vector $\begin{bmatrix} X_{s_1} & X_{s_2} & \cdots & X_{s_n} \end{bmatrix}^T$. So, for any edge e emanating from s, we have $Y_e = A_e A_s X_s$, where A_e is the local coding matrix associated with the edge pair $((s', s), e)$. Now, for the same edge e, this can be easily achieved in $\mathcal{N}$ if the vector X_s generated at s is multiplied by $A_e A_s$. Hence the message $Y_{(t,t')}$ received by the edge (t, t') of $\mathcal{N}^n$ can also be received by t of $\mathcal{N}$.

At the terminal t_i for $1 \leq i \leq n$, X_{s_i} is retrieved by t_i in $\mathcal{N}^n$ from $Y_{(t,t')}$. So there exists a decoding matrix A_{t_i} of size $1 \times n$ such that $X_{s_i} = A_{t_i} Y_{(t,t')}$. Let the matrix $\begin{bmatrix} A_{t_1} & A_{t_2} & \cdots & A_{t_n} \end{bmatrix}^T$ be denoted by A_t. Then the vector X_s can be decoded by t of $\mathcal{N}$ with the operation $A_t Y_{(t,t')}$.

Let us now consider the if part. We show that an n-dimensional vector linear solution in $\mathcal{N}$ implies an $(1, n)$ fractional linear coding solution of $\mathcal{N}^n$. For $1 \leq i \leq n$, let the matrix $A_{(s_i,s')}$ be an $n \times 1$ column vector whose i^{th} element is one and all other elements are zero; and let A_{t_i} be an $1 \times n$ row vector whose i^{th} element is one and all other elements are zero. For the local coding matrices of the rest of the edge pairs in $\mathcal{N}^n$, copy the local coding matrix of the corresponding edge pairs from $\mathcal{N}$. Then the solution is immediate. □

We now further generalize Theorem 13.

Theorem 14. *For any network $\mathcal{N}$, and positive numbers a, b, l where $l \geq ab$, the b-factored network of $\mathcal{N}$ has an (a, l) fractional linear coding solution over $\mathbb{F}_q$ if and only if $\mathcal{N}$ has an (ab, l) fractional linear network coding solution over $\mathbb{F}_q$.*

Proof. The proof of this theorem is similar to that of Theorem 13; only the size of the local coding matrices are different. Let us denote the b-factored network of $\mathcal{N}$ by $\mathcal{N}^b$. Let the nomenclature of sources and edges in $\mathcal{N}^b$ remain the same as that has been used for the network $\mathcal{N}^n$ Theorem 13.

If $\mathcal{N}^b$ has an (a, l) fractional linear coding solution, then X_{s_i} for $1 \leq i \leq b$ is an a-length vector, and $A_{(s_i,s')}$ is an $l \times a$ sized matrix. Accordingly, A_s is of size $l \times ab$, and X_s is an ab-length vector. At the terminals, A_{t_i} is of size $a \times l$; and hence A_t is of size $ab \times l$.

Consider the only if part. Proceeding similar to Theorem 13, if an edge e emanating from s in $\mathcal{N}^b$ carries the message $A_e A_s X_s$, then the same can be obtained in $\mathcal{N}$. At the terminal t, multiplying $Y_{(t,t')}$ by A_t retrieves X_s.

The proof of if part is also similar to the proof of if part of Theorem 13. Let us say $A_{(s_i,s')} = \begin{bmatrix} \mathbf{0}_{a(i-1)\times a} & I_{a\times a} & \mathbf{0}_{(l-ai)\times a} \end{bmatrix}^T$. Then the node s in $\mathcal{N}^b$ can retrieve the ab-length message X_s. As $\mathcal{N}$ has an (ab, l) fractional linear network coding solution, terminal t can retrieve the information X_s if all the local coding matrices of the in-between edge pairs of $\mathcal{N}^b$ are copied from $\mathcal{N}$. Then, by setting $A_{t_i} = \begin{bmatrix} \mathbf{0}_{a(i-1)\times a} & I_{a\times a} & \mathbf{0}_{(ab-ai)\times a} \end{bmatrix}$ the message vector X_{s_i} can be computed at t_i by the operation $A_{t_i} Y_{(t',t_i)}$. □

Now, using this above theorem we prove the following result:

Theorem 15. *Let $\mathcal{N}_m$ be the generalized M-network for $m = dn$. The n-factored network of $\mathcal{N}_m$ has a (w, wn) fractional linear network coding solution if and only if w is an integer multiple of d.*

Proof. Let the n-factored network of $\mathcal{N}_m$ be denoted by $\mathcal{N}^n$. From Theorem 14 it can be seen that $\mathcal{N}^n$ has a (w, wn) fractional linear network coding solution if and only if $\mathcal{N}_m$ has a (wn, wn) fractional linear network coding solution. However, from Theorem 11 we know that for the latter to hold wn must be an integer multiple of dn. This implies that w must be an integer multiple of d. □

This lemma leads to the following corollary.

Corollary 16. *For any positive integer d and n, there exists a network which has a (w, wn) fractional linear network coding solution if and only if w is an integer multiple of d.*

TH-2118_136102023

Consider a network $\mathcal{N}$. Replace each edge of $\mathcal{N}$ by k parallel edges. Name the resultant network as $\mathcal{N}_{||=k}$.

Theorem 17. *$\mathcal{N}$ has an (a, kl) fractional linear solution if and only if $\mathcal{N}_{||=k}$ has an (a, l) fractional linear solution.*

Proof. First we show the 'if' part. Let e be an edge in $\mathcal{N}$ which is replaced by k parallel edges in $\mathcal{N}_{||=k}$. Each each of these parallel edges carry l symbols. These symbols can be accumulated to construct a kl-length vector. Then $\mathcal{N}_{||=k}$ network would still have some fractional linear solution if one edge out of the l parallel edges carry the kl-length vector, and other edges carry no symbols. Now, if the remaining edges carrying no symbol can be deleted, and if this is done for every edge, the resultant network becomes $\mathcal{N}$ with a (r, kl) fractional linear network code solution.

We now prove the 'only if' part. Let an edge e carry a kl-length vector in $\mathcal{N}$. This edge is replaced by k parallel edges in $\mathcal{N}_{||=k}$. Let the kl symbols carried by e be distributed among k parallel edges such that no edge carries any more than l symbols. This is to be for every edge e of $\mathcal{N}$. Since this transformation does not disrupts the information received by the downstream edges or nodes, the network achieves a (a, l) fractional linear solution. □

Theorem 18. *For any positive integers k, n, and d, there exists a network which has a (wk, wn) fractional linear network code solution if and only if w is a multiple of d.*

Proof. Consider the generalized M-network $\mathcal{N}_m$ for $m = dkn$. Let $\mathcal{N}^n$ be the n-factored network of $\mathcal{N}_{dkn}$. It can be seen from Theorem 15 that $\mathcal{N}^n$ has a (w, wn) fractional linear solution if and only if w is an integer multiple of dk. Replace each edge of $\mathcal{N}^n$ by k parallel edges. Name the resultant network as $\mathcal{N}^n_{||=k}$. We show $\mathcal{N}^n_{||=k}$ is a network that Theorem 18 proposes to exist.

First consider the only if part. We assume $\mathcal{N}^n_{||=k}$ has a (wk, wn) fractional linear network code solution. Then from Theorem 17, $\mathcal{N}^n$ has a (wk, wkn) fractional linear solution. But due to Theorem 15, this implies wk is a positive integer multiple of dk, which in turn implies w is a positive integer multiple of d. So $\mathcal{N}^n_{||=k}$ has a (wk, wn) fractional linear only if w is a multiple of d.

Now consider the if part. Let us say that w is a multiple of d. Then $\mathcal{N}^n$ has a (wk, wkn) fractional linear solution. Hence, from Theorem 17 we get that $\mathcal{N}^n_{||=k}$ has a (wk, wn) fractional linear solution. □

From Theorem 18, we have the following corollary:

Corollary 19. *For any rational number $\frac{k}{n}$ and for any arbitrarily large number x, there exists a network which has a rate $\frac{k}{n}$ fractional linear network coding solution only if the message dimension is larger than x.*

Proof. Let a be any given number. Let x be any positive integer greater than a. Then, setting $d = x$ in Theorem 18, guarantees existence of such a network. □

3.3 MDim-m network

In Section 3.1 we showed that for any positive integer $m \geq 3$ there exists a network which has a vector linear solution if and only if the message dimension is a multiple of m (particular case for $m = 2$ was shown in [3] and [8]). Subsequent to our work, in reference [44] a network named as the Dim-k network was presented. The Dim-k network behaves like the generalized M-network $\mathcal{N}_m$: Dim-k has an w-dimensional vector linear solution if and only if the message dimension is a multiple of k. Both networks reduces to the M-network for the special case of $m = 2$ and $k = 2$ respectively, but for higher values of m and k their topological constructions are different.

In this section, we show that for any positive integer m there exists a network which has no w-dimensional vector linear solution if w is less than m, but has a w-dimensional vector linear solution for all w greater than or equal to m. We prove this result by constructing a network which is a modification of the Dim-k network shown in [44]. We have named this network as MDim-m network which is a short form of 'modified Dim-m network'.

First we describe the MDim-m network. The MDim-m network is a modified version of the Dim-m (originally named as Dim-k) network shown in [44]. The MDim-m for $m = 3$ is shown in Fig. 3.6. There are m^2 sources and the sources are segregated into m sets: S_i for $1 \leq i \leq m$, with each set having m sources. For any fixed ordering, let the j^{th} source in S_i be denoted by s_{ij}. The network has two sets of intermediate nodes $U = \{u_1, u_2, \ldots, u_m\}$ and $V = \{v_1, v_2, \ldots, v_m, v_{m+1}\}$. The source s_{ij} is connected to the node u_i by an edge (s_{ij}, u_i) for $1 \leq i, j \leq m$. The node u_i and v_i is connected by $m-1$ parallel edges, and the k^{th} edge is denoted by (u_i, v_i, k) for $1 \leq k \leq m-1$. Let $E_i = \{(u_i, v_i, k) | 1 \leq k \leq m-1\}$. Node u_i for $1 \leq i \leq m$ is connected to the node v_{m+1} by an edge $e_{i(m+1)} = (u_i, v_{m+1})$.

Let T denote the set of all terminals. Each node v_i for $1 \leq i \leq m$ is connected to each terminal $t \in T$ by $m-1$ parallel edges (directed from v_i to t). The node v_{m+1} is connected to each terminal $t \in T$ by an edge (v_{m+1}, t). T is partitioned into m sets: T_i for $1 \leq i \leq m-1$, and a set T^*. A

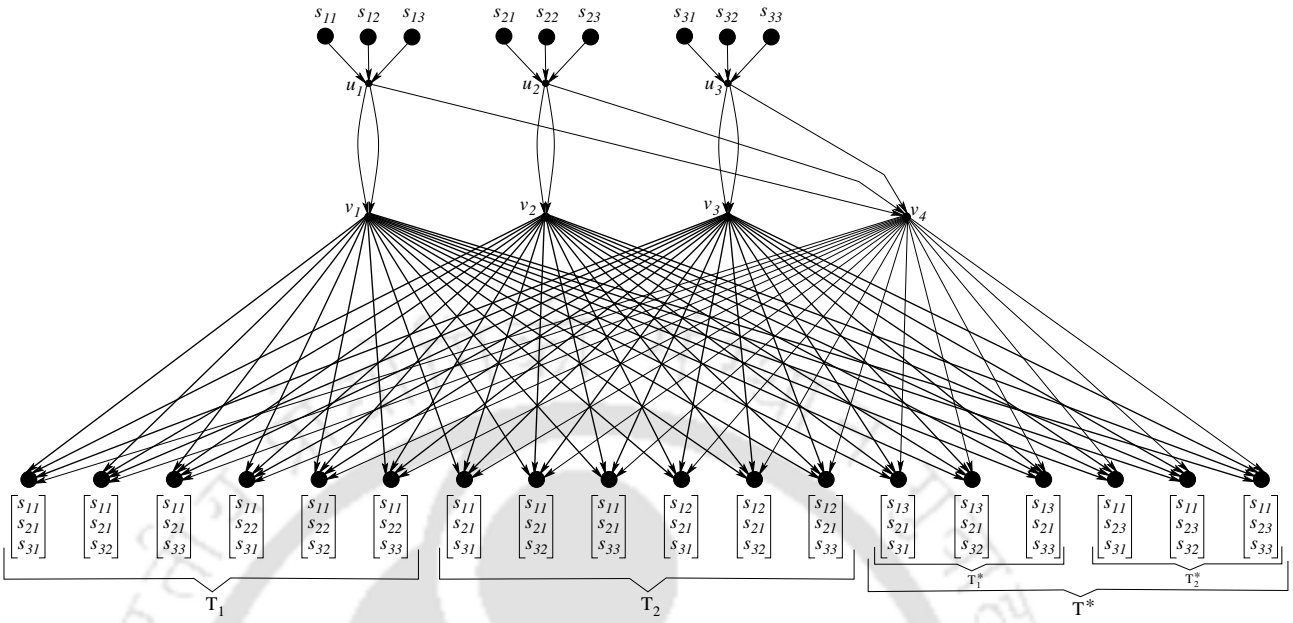

Figure 3.6: The MDim-m network for $m = 3$. The elements of the vector under each terminal are the sources from which messages are demanded. Note that T_1 and T_2 have 3 terminals demanding the same sources. A terminal $t \in T$ is connected to node the v_i for $1 \leq i \leq m$ by $m-1$ edges. To protect clarity we represent these $m-1$ edges with a thicker but single edge.

terminal t in T_i demands a unique tuple of m source messages (but two different terminals belonging respectively to T_i and T_j for $i \neq j$ may demand the same set of sources). This unique tuple is decided following these rules: (1) all $t \in T_i$ demands the message generated by the source s_{i1} (2) for each $j \in \{1, 2, \ldots, m-1\}$, $j \neq i$, terminal $t \in T_i$ must demand one source from the set $\{s_{j1}, s_{j2}, \ldots, s_{j(m-1)}\}$ (note it doesn't demand s_{jm}) (3) $t \in T_i$ demands any one source from set S_m. It can be seen that each T_i has $m(m-1)^{(m-2)}$ terminals (to choose one element from $(m-1)$ elements of each set S_j for $1 \leq j \leq m-1$, $j \neq i$, and one element from m elements of S_m). The set T^* is further partitioned into $m-1$ subsets: $T_1^*, T_2^*, \ldots, T_{m-1}^*$. Each of T_i^* for $1 \leq i \leq m-1$ contains m terminals. For any fixed ordering the j^{th} terminal for $1 \leq j \leq m$ in T_i^* demands messages from the sources: s_{im}, s_{mj}, and all sources in the set $\{s_{k1} | 1 \leq k \leq m-1, k \neq i\}$. (Note that MDim-$m$ is the M-network for $m = 2$.)

Theorem 20. *For any positive integer $m \geq 3$, the MDim-m network has a w-dimensional vector linear solution if and only if w is greater than or equal to $m-1$.*

Proof. First we show the 'only if' part. Let f be the function that maps the network MDim-m to a discrete polymatroid $\mathbb{D}$ such that the conditions of Definition 6 are satisfied. Let ρ be the rank function of $\mathbb{D}$, and let $\mathsf{g} = \rho \circ f$. Say that the MDim-$m$ has a d-dimensional vector linear solution.

Claim 3. $\mathsf{g}(E_1) = \mathsf{g}(E_2) = \cdots = \mathsf{g}(E_m) = (m-1)d$

Proof. As per D3 of Definition 6, $\mathsf{g}(s_{ij}) = d$. So,

$$\begin{aligned} m^2 d &= \sum_{i,j=1}^{m} \mathsf{g}(s_{ij}) = \mathsf{g}(s_{11}, s_{12}, \ldots, s_{mm}) \qquad \text{[using Lemma 4]} \\ &\leq \mathsf{g}(s_{11}, \ldots, s_{mm}, E_1, \ldots, E_m, e_{1(m+1)}, \ldots, e_{m(m+1)}) \\ &= \mathsf{g}(E_1, E_2, \ldots, E_m, e_{1(m+1)}, \ldots, e_{m(m+1)}) \qquad (3.16) \\ &\leq \mathsf{g}(E_1) + \cdots + \mathsf{g}(E_m) + \mathsf{g}(e_{1(m+1)}) + \cdots + \mathsf{g}(e_{m(m+1)}). \qquad (3.17) \end{aligned}$$

Equation (3.16) holds because of D4 and the fact that every source message is demanded by some terminal, which must be retrieved from $E_i \cup \{e_{i(m+1)} | 1 \leq i \leq m\}$. Since E_i contains $m-1$ edges, using D3 of Definition 6 we get $\mathsf{g}(E_i) \leq (m-1)d$, and also $\mathsf{g}(e_{i(m+1)}) \leq d$ for $1 \leq i \leq m$. So for equation (3.17) to hold we must have: $\mathsf{g}(E_i) = (m-1)d$ for $1 \leq i \leq m$. □

Claim 4. *for* $1 \leq i \leq m$*:*

$$\mathsf{g}(E_i, s_{i1}) + \mathsf{g}(E_i, s_{i2}) + \cdots + \mathsf{g}(E_i, s_{im}) \geq (m^2 - m + 1)d.$$

Proof. This is proved by using the Definition 4.

$$\begin{aligned} \mathsf{g}(E_i, s_{i1}) + \mathsf{g}(E_i, s_{i2}) + \cdots + \mathsf{g}(E_i, s_{im}) &\geq \mathsf{g}(E_i, s_{i1}, s_{i2}, \ldots, s_{im}) + (m-1)\mathsf{g}(E_i) \qquad (3.18) \\ &= \mathsf{g}(s_{i1}, s_{i2}, \ldots, s_{im}) + (m-1)\mathsf{g}(E_i) \\ &= md + (m-1)(m-1)d = (m^2 - m + 1)d. \end{aligned}$$

equation (3.18) is obtained by using P3 of Definition. 4 $(m-1)$ times. □

As per Definition 6 and Definition 5, for any $X \subseteq \{S \cup E\}$, $f(X)$ maps X to a subset of G, and for each $j = f(x_i)$, where $x_i \in X$, there exists a vector space V_j such that $dim(\sum_{\forall x_i \in X} V_{f(x_i)}) = \mathsf{g}(X)$. Then, for any $1 \leq i \leq m$:

$$\begin{aligned} md &= \mathsf{g}(s_{i1}, \ldots, s_{im}) = \mathsf{g}(e_i, s_{i1}, \ldots, s_{im}) \qquad \text{[from D3, D4]} \\ \text{or, } md &= dim(\sum_{l=1,\ldots,m} V_{f(s_{il})}) = dim(\sum_{l=1,\ldots,m} V_{f(s_{il})} + V_{f(e_i)}). \qquad (3.19) \end{aligned}$$

Since for any two vector space U and V, $dim(U) + dim(V) = dim(U \cup V) + dim(U \cap V)$. Then, for

any $1 \leq i, j \leq m$, $i \neq j$,

$$dim(\sum_{l=1,\ldots,m} V_{f(s_{il})} + V_{f(e_i)}) + dim(\sum_{l=1,\ldots,m} V_{f(s_{jl})} + V_{f(e_j)})$$
$$= dim(\sum_{l=1,\ldots,m} V_{f(s_{il})} + V_{f(e_i)} + \sum_{l=1,\ldots,m} V_{f(s_{jl})} + V_{f(e_j)}) + dim((\sum_{l=1,\ldots,m} V_{f(s_{il})} + V_{f(e_i)}) \cap (\sum_{l=1,\ldots,m} V_{f(s_{jl})} + V_{f(e_j)})).$$

Then from D3 of Definition 6 and using equation (3.19):

$$dim((\sum_{l=1,\ldots,m} V_{f(s_{il})} + V_{f(e_i)}) \cap (\sum_{l=1,\ldots,m} V_{f(s_{jl})} + V_{f(e_j)})) = 0.$$

This implies, for any $1 \leq i, j, l, k \leq m$:

$$dim((V_{f(s_{il})} + V_{f(e_i)}) \cap (V_{f(s_{jk})} + V_{f(e_j)})) = 0.$$

So, $dim(V_{f(s_{il})} + V_{f(e_i)}) + dim(V_{f(s_{jk})} + V_{f(e_j)}) = dim(V_{f(s_{il})} + V_{f(e_i)} + V_{f(s_{jk})} + V_{f(e_j)})$

or, $\mathrm{g}(s_{il}, e_i) + \mathrm{g}(s_{jk}, e_j) = \mathrm{g}(s_{il}, e_i, s_{jk}, e_j)$. (3.20)

It can be seen that equation (3.20) can also be obtained by using Lemma 5.

Claim 5. *Let $1 \leq j_1, j_2, \ldots, j_{m-1} \leq m-1$ and $1 \leq j_m \leq m$. Then for $1 \leq i \leq m-1$ the eqns. (3.21) and (3.22) shown below hold*

$$\mathrm{g}(E_1, s_{1j_1}) + \cdots + \mathrm{g}(E_{i-1}, s_{(i-1)j_{i-1}}) + \mathrm{g}(E_i, s_{i1}) + \mathrm{g}(E_{i+1}, s_{(i+1)j_{i+1}}) + \cdots$$
$$\cdots + \mathrm{g}(E_m, s_{mj_m}) \leq (m^2 - m + 1)d \quad (3.21)$$

$$\mathrm{g}(E_1, s_{11}) + \cdots + \mathrm{g}(E_{i-1}, s_{(i-1)1}) + \mathrm{g}(E_i, s_{im}) + \mathrm{g}(E_{i+1}, s_{(i+1)1}) + \cdots$$
$$\cdots + \mathrm{g}(E_{m-1}, s_{(m-1)1}) + \mathrm{g}(E_m, s_{mj_m}) \leq (m^2 - m + 1)d. \quad (3.22)$$

Proof. According to the network description there exists a terminal $t \in T_i$ that demands the messages from sources in $\{s_{1j_1}, s_{2j_2}, \ldots, s_{(i-1)j_{(i-1)}}, s_{i1}, s_{(i+1)j_{(i+1)}}, \ldots, s_{mj_m}\}$, and the $(j_m)^{\text{th}}$ terminal in T_i^* demands the messages from sources $\{s_{11}, .., s_{(i-1)1}, s_{im}, s_{(i+1)1}, .., s_{(m-1)1}, s_{mj_m}\}$. Proof of (3.21):

$$\mathrm{g}(E_1, s_{1j_1}) + \cdots + \mathrm{g}(E_{i-1}, s_{(i-1)j_{i-1}}) + \mathrm{g}(E_i, s_{i1}) + \mathrm{g}(E_{i+1}, s_{(i+1)j_{i+1}}) + \cdots + \mathrm{g}(E_m, s_{mj_m})$$
$$= \mathrm{g}(E_1, s_{1j_1}, \ldots, E_i, s_{i1}, \ldots, E_m, s_{mj_m}) \quad \text{[using equation (3.20)].}$$
$$\leq \mathrm{g}(E_1, s_{1j_1}, \ldots, E_i, s_{i1}, \ldots, E_m, s_{mj_m}, (v_{m+1}, t))$$
$$= \mathrm{g}(E_1, \ldots, E_i, \ldots, E_m, (v_{m+1}, t)) \quad \text{[Due to } t \in T_i\text{]}$$
$$\leq m(m-1)d + d = (m^2 - m + 1)d. \quad \text{[D3 of Definition 6].}$$

Proof of equation (3.22) is similar (due to demands of $t \in T^*$). □

Claim 6. *For each $i \in \{1, 2, \ldots, m-1\}$ there exist at least two distinct values of j in the range $1 \leq j \leq m$ such that $\mathsf{g}(E_i, s_{ij}) \geq (m-1)d+1$. And there exists at least one value of $j \in \{1, 2, \ldots, m\}$ such that $\mathsf{g}(E_m, s_{mj}) \geq (m-1)d+1$.*

Proof. Say for some value of i there exists no such j. Then $\mathsf{g}(E_i, s_{ij}) = (m-1)d$ for $1 \leq j \leq m$ (as $\mathsf{g}(E_i) = (m-1)d$ and $\mathsf{g}(E_i, s_{ij}) \geq \mathsf{g}(E_i)$). But if these values are substituted in the equation given by Claim 4, we get: $m(m-1)d \geq (m^2-m+1)d$, which is a contradiction.

We show that there exist at least 2 such j for $1 \leq i \leq m-1$. Say, for some $1 \leq i \leq m-1$ there is only one value of j for which $\mathsf{g}(E_i, s_{ij}) \geq (m-1)d+1$. Hence, $\mathsf{g}(E_i, s_{ij'}) = (m-1)d$ for any $j' \neq j$. Then to satisfy equation of Claim (4) and equation of Claim (3) we must have: $\mathsf{g}(E_i, s_{ij}) = (m-1)d + d$. We show this is not possible. Let $j_m \in \{1, 2, \ldots, m\}$ be such that $\mathsf{g}(E_m, s_{mj_m}) \geq (m-1)d+1$.

Case I: $j \in \{1, 2, \ldots, m-1\}$.

equation (3.21) tells us that there exist an $l \in \{1, 2, \ldots, m-1\}$, $l \neq i$, and $1 \leq j_1, \ldots, j_{m-1} \leq m-1$ such that

$$\mathsf{g}(E_l, s_{l1}) + \sum_{k=1, k\neq l, i}^{m} \mathsf{g}(E_k, s_{kj_k}) + \mathsf{g}(E_i, s_{ij}) \leq (m^2-m+1)d.$$

Substituting $\mathsf{g}(E_l, s_{l1}) \geq (m-1)d$, for $1 \leq k \leq m-1, k \neq i, l$, $\mathsf{g}(E_k, s_{kj_k}) \geq (m-1)d$, $\mathsf{g}(E_i, s_{ij}) = (m-1)d + d$, and $\mathsf{g}(E_m, s_{mj_m}) \geq (m-1)d+1$, we have:

$$\begin{aligned} &(m-1)(m-1)d + (m-1)d + d + 1 \leq (m^2-m+1)d \\ &\text{or, } (m^2-m+1)d + 1 \leq (m^2-m+1)d. \end{aligned} \tag{3.23}$$

equation (3.23) is a contradiction.

Case II: $j = m$.

From equation (3.22), we have:

$$\sum_{k=1, k\neq i, m}^{m-1} \mathsf{g}(E_k, s_{k1}) + \mathsf{g}(E_i, s_{im}) + \mathsf{g}(E_m, s_{mj_m}) \leq (m^2-m+1)d.$$

Substituting $\mathsf{g}(E_k, s_{k1}) \geq (m-1)d$ for $1 \leq k \leq m-1$, $k \neq i, l$, $\mathsf{g}(E_i, s_{im}) = (m-1)d + d$, and $\mathsf{g}(E_m, s_{mj_m}) \geq (m-1)d+1$, same contradiction as equation (3.23) can be obtained. □

Claim 6 guarantees that there exist $1 \leq j_2, ..., j_{m-1} \leq m-1$ and $1 \leq j_m \leq m$ such that $\mathsf{g}(E_i, s_{j_i}) \geq$

$(m-1)d+1$ for $2 \leq i \leq m$. Now, from equation (3.21) of Claim 5, we have:

$$\mathsf{g}(E_1, s_{11}) + \mathsf{g}(E_2, s_{2j_2}) + \mathsf{g}(E_3, s_{3j_3}) + \cdots + \mathsf{g}(E_m, s_{mj_m}) \leq (m^2 - m + 1)d. \tag{3.24}$$

In Equation (3.24), substituting $\mathsf{g}(E_1, s_{11}) \geq (m-1)d$, and for $i \neq 1$: $\mathsf{g}(E_i, s_{ij_i}) \geq (m-1)d+1$, we get:

$$\begin{aligned} &(m-1)d + (m-1)((m-1)d+1) \leq (m^2 - m + 1)d \\ &\text{or, } (m-1)(md+1) \leq (m-1)md + d \\ &\text{or, } d \geq m-1. \end{aligned}$$

For any positive integer $m \geq 3$, we now show that the MDim-m network has a w-dimensional vector routing solution for any $w \geq m-1$ ('if part'). We first give an $(m-1)$-dimensional vector routing solution. We denote the message vector generated at the source s_{ij} by X_{ij}, and the k^{th} component of X_{ij} by X_{ijk}. Let the edges in E_i for $1 \leq i \leq m$ carry all components of the vector X_{i1}, and the last $m-2$ components of each vector X_{ij} for $2 \leq j \leq m$ (Note that $m-1+(m-2)(m-1) = (m-1)(m-1)$). The messages carried by $e_{i(m+1)}$ for $1 \leq i \leq m$ are shown in Table 3.1. It can be seen that if Table 3.1 is followed then a terminal $t \in T_i$ needs no more than $m-1$ symbols through (v_{m+1}, t), and if $t \in T^*$, then (v_{m+1}, t) carries no more than 2 symbols.

Table 3.1: Messages carried by $\{(u_i, v_{m+1}) | 1 \leq i \leq m\}$ when $d = m-1$.

$e_{1(m+1)}$	$e_{2(m+1)}$	$\cdots$	$e_{(m-1)(m+1)}$	$e_{m(m+1)}$
X_{121}	X_{221}	$\cdots$	$X_{(m-1)21}$	X_{m21}
X_{131}	X_{231}	$\cdots$	$X_{(m-1)31}$	X_{m31}
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
X_{1m1}	X_{2m1}	$\cdots$	$X_{(m-1)m1}$	X_{mm1}

Now, if the terminals that demand the exact same set of sources are considered as one (since they receive information from the same set of edges, this does not affect solvability), then MDim-m network is a sub-network of the Dim-m network of [44], and hence it has an m-dimensional vector routing solution. Furthermore, an $(m-1)$-dimensional vector routing solution and an m-dimensional vector routing solution guarantees an $(2m-1)$-dimensional and $(2m-2)$-dimensional vector routing solution. So the case for $m = 3$ is already solved. We now show that MDim-m has an $(m+k)$-dimensional vector routing solution for $1 \leq k \leq m-3$ and $m \geq 4$. For $1 \leq i \leq m-1$, let the edges in

Table 3.2: Messages carried by $\{(u_i, v_{m+1})|1 \leq i \leq m\}$ when $d = m + k$.

$e_{1(m+1)}$	$e_{2(m+1)}$	$\cdots$	$e_{(m-1)(m+1)}$	$e_{m(m+1)}$
X_{121}	X_{221}	$\cdots$	$X_{(m-1)21}$	X_{m11}
X_{131}	X_{231}	$\cdots$	$X_{(m-1)31}$	X_{m21}
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
$X_{1(m-1)1}$	$X_{2(m-1)1}$	$\cdots$	$X_{(m-1)(m-1)1}$	$X_{m(m-2)1}$
X_{1m1}	X_{2m1}	$\cdots$	$X_{(m-1)m1}$	$X_{m(m-1)1}$
X_{1m2}	X_{2m2}	$\cdots$	$X_{(m-1)m1}$	X_{mm1}
X_{1m3}	X_{2m3}	$\cdots$	$X_{(m-1)m3}$	X_{m12}
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
$X_{1m(k+2)}$	$X_{2m(k+2)}$	$\cdots$	$X_{(m-1)m(k+2)}$	X_{mk2}

E_i carry all components of the vector X_{i1}, last $m+k-1$ components of X_{ij} for $2 \leq j \leq m-1$, and the last $m-2$ components of X_{im} (Note $m+k+(m-2)(m+k-1)+m-2 = (m-1)(m+k)$). Edges in E_m carries the last $m+k-2$ components of X_{mj} for $1 \leq j \leq k$, and the last $m+k-1$ components of X_{mj} for $k+1 \leq j \leq m$ (Note $k(m+k-2)+(m-k)(m+k-1) = (m-1)(m-k)$). The symbols not sent through $\{E_i|1 \leq i \leq m\}$ are carried by $\{e_{i(m+1)}|1 \leq i \leq m\}$ as shown in Table 3.2.

It can be seen that for a terminal $t \in T_i$, the edge (v_{m+1}, t) carries no more than $m+1$ symbols. Notice that no terminal demands any two vectors from the set $\{X_{im}|1 \leq i \leq m-1\}$. So if $t \in T^*$ demands X_{im} for some $1 \leq i \leq m-1$, then v_{m+1} carries no more than $k+4$ symbols ($k+2$ symbols of X_{ij}, and maximum 2 symbols of X_{ml} for some $1 \leq l \leq k$). So we must have $k+4 \leq m+k$, or, $m \geq 4$. □

We now show that there exists a network which has a (wk, wn) fractional linear solution if and only if w is greater than or equal to d.

Theorem 21. *Consider the MDim-m network for $m = dn+1$. The n-factored network of MDim-m has a (w, wn) fractional linear network coding solution if and only if w is greater than or equal to d.*

Proof. Let the n-factored network of MDim-m be denoted by MDim^n-m. From Theorem 14 it can be seen that MDim^n-m has a (w, wn) fractional linear network coding solution if and only if MDim-m has a (wn, wn) fractional linear network coding solution. However, from Theorem 20 we know that for the latter to hold wn must be greater than or equal to $m-1$. Now, $wn \geq m-1 \Rightarrow wn \geq dn \Rightarrow w \geq d$. □

Corollary 22. *For any positive integers d and n, there exists a network which has a (w, wn) fractional linear network coding solution if and only if w is greater than or equal to d.*

Theorem 23. *For any positive integers k, n, and d, there exists a network which has a (wk, wn) fractional linear network code solution if and only if w is greater than or equal to d.*

Proof. Consider the MDim-m for $m = dkn+1$. Let MDim^n-m be the n-factored network of MDim-m. Replace each edge of MDim^n-m by k parallel edges. Name the resultant network as MDim$^n_{||=k}$-m. Theorem 17 says that MDim$^n_{||=k}$-m has a (wk, wn) fractional linear solution if and only if MDim^n-m has a (wk, wkn) fractional linear solution. But from Theorem 21, MDim^n-m has a (wk, wkn) fractional linear solution if and only if wk is greater than or equal to dk, which in turn implies w is greater than d. So MDim$^n_{||=k}$-m is the network that the theorem proposes to exist. □

Corollary 24. *For any rational number $\frac{k}{n}$ and for any arbitrary large number m, there exists a network which has a rate $\frac{k}{n}$ fractional linear network coding solution if and only if the message dimension is larger than m.*

3.4 Network Coding Solution but No Routing Solution

The network shown in the proof of Theorem 18 has a (wk, wn) fractional linear network code solution if and only if w is a multiple of d. We also showed in the proof of Theorem 18 that the network has a (wk, wn) fractional routing solution if and only if w is a multiple of d. In light of this result, it is an interesting question whether all networks which have a (wk, wn) fractional linear network code solution if and only if w is an integer multiple of an integer, have a (wk, wn) routing solution as well. We answer this question in negative by constructing an example network $\mathcal{N}_*$ shown in Fig. 3.7. We show that $\mathcal{N}_*$ neither has a $(1, 2)$ fractional linear network code solution, nor has a $(2, 4)$ routing solution, but it has a $(2, 4)$ fractional linear network code solution.

Let Y_{ii} be the set of symbols carried by the edge (u_i, v_i), $Y_{(u_1,v*)}$ be the set of symbols carried by the edge (u_1, v^*), and Y_{i3} be the set of symbols carried by the edge (u_i, v_3). Also denote the message carried by the edge (v_3, t_i) by $Z_{(3,i)}$ for $1 \leq i \leq 36$. Because of the demands of the terminals, all symbols from the sources s_{11}, s_{12}, s_{13} and s_{14} must pass though the edges (u_1, v_1) and (u_1, v_3). Also let the source s_{ij} generate the message X_{ij} for $1 \leq i \leq 2$, $1 \leq j \leq 4$.

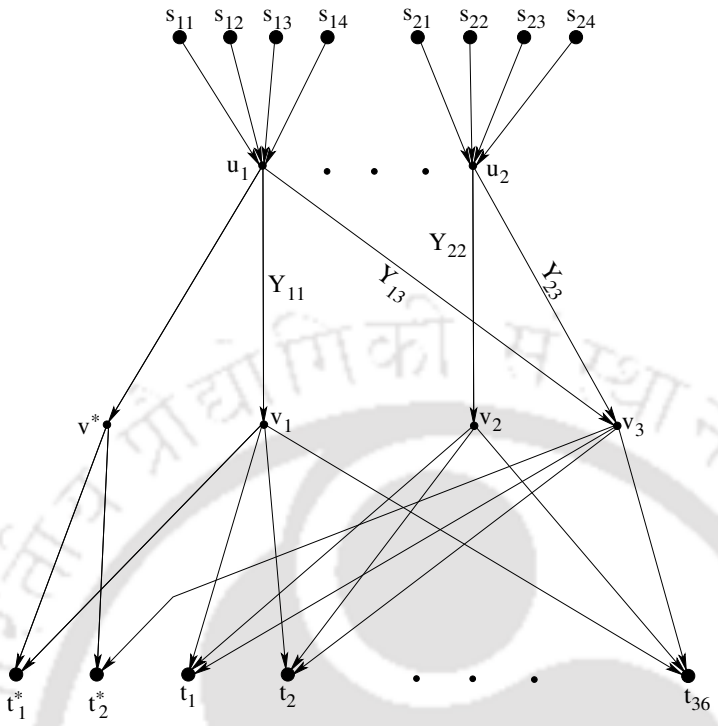

Figure 3.7: A network $\mathcal{N}_*$. Each terminal t_i for $1 \leq i \leq 36$ demands information from a unique combination of 4 sources, two of which belongs to $\{s_{11}, s_{12}, s_{13}, s_{14}\}$, and the other two belongs to $\{s_{21}, s_{22}, s_{23}, s_{24}\}$. The terminals t_1^* and t_2^* demands to compute the message generated by all sources in $\{s_{11}, s_{12}, s_{13}, s_{14}\}$. We show that $\mathcal{N}_*$ has a $(2, 4)$ fractional linear network code solution, but it neither has a $(1, 2)$ fractional linear network code solution, nor has a $(2, 4)$ fractional routing solution.

First let us say that $\mathcal{N}_*$ has a $(1, 2)$ fractional linear network coding solution. As per Theorem 1, $\mathcal{N}_*$ has a $(1, 2)$ fractional linear network code solution over some finite field $\mathbb{F}_q$ if and only if it is a $(1, 2)$-discrete polymatroidal network with respect to a discrete polymatroid $\mathbb{D}$ representable over $\mathbb{F}_q$. Let f be the function that maps the source nodes and the edges of $\mathcal{N}_*$ to the elements of $\mathbb{D}$ such that $\mathcal{N}_*$ is a $(1, 2)$-discrete polymatroidal network with respect to $\mathbb{D}$ (f follows the rules shown in Definition 6). Let ρ be the rank function of $\mathbb{D}$. Now let $\mathsf{g} = \rho \circ f$.

Say $X_{1i_1}, X_{1i_2} \in \{X_{11}, X_{12}, X_{13}, X_{14}\}$ and $X_{2j_1}, X_{2j_2} \in \{X_{21}, X_{22}, X_{23}, X_{24}\}$. Then, there exists a terminal t_n among $\{t_1, t_2, \ldots, t_{36}\}$ that demands the messages $\{X_{1i_1}, X_{1i_2}, X_{2j_1}, X_{2j_2}\}$. Let t_n be that terminal. Hence,

$$\begin{aligned}
&\mathsf{g}(Y_{11}, X_{1i_1}, X_{1i_2}) + \mathsf{g}(Y_{22}, X_{2j_1}, X_{2j_2}) \\
&= \mathsf{g}(Y_{11}, X_{1i_1}, X_{1i_2}, Y_{22}, X_{2j_1}, X_{2j_2}) \qquad \text{[using Lemma 5 repetitively]} \\
&\leq \mathsf{g}(Y_{11}, X_{1i_1}, X_{1i_2}, Y_{22}, X_{2j_1}, X_{2j_2}, Z_{(3,n)}) = \mathsf{g}(Y_{11}, Y_{22}, Z_{(3,n)}) \leq 4 + 2 = 6. \qquad (3.25)
\end{aligned}$$

Now, consider the following inequality.

$$\begin{aligned}
8 &= \mathsf{g}(X_{11}, X_{12}, X_{13}, X_{14}, X_{21}, X_{22}, X_{23}, X_{24}) \\
&\leq \mathsf{g}(X_{11}, X_{12}, X_{13}, X_{14}, X_{21}, X_{22}, X_{23}, X_{24}, Y_{11}, Y_{22}, Y_{13}, Y_{23}) \\
&= \mathsf{g}(Y_{11}, Y_{22}, Y_{13}, Y_{23}) \\
&\leq \mathsf{g}(Y_{11}) + \mathsf{g}(Y_{22}) + \mathsf{g}(Y_{13}) + \mathsf{g}(Y_{23}) \\
&\leq 8.
\end{aligned}$$

Since $\mathsf{g}(Y_{ij}) \leq 2$, hence it must be that $\mathsf{g}(Y_{11}) = \mathsf{g}(Y_{22}) = \mathsf{g}(Y_{13}) = \mathsf{g}(Y_{23}) = 2$.

Now, we have the following result:

$$\begin{aligned}
&\mathsf{g}(Y_{11}, X_{11}, X_{12}) + \mathsf{g}(Y_{11}, X_{13}, X_{14}) \\
&\geq \mathsf{g}(Y_{11}, X_{11}, X_{12}, X_{13}, X_{14}) + \mathsf{g}(Y_{11}) \qquad \text{[from rule } \mathbf{P3} \text{ of Definition 4]} \\
&= \mathsf{g}(X_{11}, X_{12}, X_{13}, X_{14}) + \mathsf{g}(Y_{11}) \\
&= 4 + 2 = 6.
\end{aligned}$$

Similarly for $i = 1, 2$ if $U_{i1}, U_{i2} \subset \{X_{i1}, X_{i2}, X_{i3}, X_{i4}\}$, $|U_{i1} = |U_{i2}| = 2$, and $U_{i1} \cap U_{i2} = \emptyset$, we have:

$$\mathsf{g}(Y_{ii}, X_{U_{i1}}) + \mathsf{g}(Y_{ii}, X_{U_{i2}}) \geq 6. \tag{3.26}$$

From equation (3.25), we know that the following two inequalities are true.

$$\begin{aligned}
\mathsf{g}(Y_{11}, X_{11}, X_{12}) + \mathsf{g}(Y_{22}, X_{21}, X_{22}) &\leq 6 \\
\mathsf{g}(Y_{11}, X_{11}, X_{12}) + \mathsf{g}(Y_{22}, X_{23}, X_{24}) &\leq 6.
\end{aligned}$$

By summing both of the above inequalities, we get:

$$2\mathsf{g}(Y_{11}, X_{11}, X_{12}) + \mathsf{g}(Y_{22}, X_{21}, X_{22}) + \mathsf{g}(Y_{22}, X_{23}, X_{24}) \leq 12. \tag{3.27}$$

From equation (3.26) we know:

$$\mathsf{g}(Y_{22}, X_{21}, X_{22}) + \mathsf{g}(Y_{22}, X_{23}, X_{24}) \geq 6. \tag{3.28}$$

Substituting equation (3.28) in Equation (3.27), we get:

$$2\mathsf{g}(Y_{11}, X_{11}, X_{12}) \leq 6$$
$$\mathsf{g}(Y_{11}, X_{11}, X_{12}) \leq 3.$$

In a similar way, if X_R is any subset of $\{X_{i1}, X_{i2}, X_{i3}, X_{i4}\}$ for $i = 1, 2$ and $|X_R| = 2$, it can be shown that,

$$\mathsf{g}(Y_{ii}, X_R) \leq 3. \tag{3.29}$$

Consider the following inequality.

$$\begin{aligned}
&\mathsf{g}(Y_{11}, X_{11}, X_{12}) + \mathsf{g}(Y_{11}, X_{11}, X_{13}) + \mathsf{g}(Y_{11}, X_{11}, X_{14}) \\
&\geq \mathsf{g}(Y_{11}, X_{11}, X_{12}, X_{13}) + \mathsf{g}(Y_{11}, X_{11}) + \mathsf{g}(Y_{11}, X_{11}, X_{14}) \qquad \text{[rule } \mathbf{P3} \text{ of Definition 4]} \\
&\geq \mathsf{g}(Y_{11}, X_{11}, X_{12}, X_{13}, X_{14}) + 2\mathsf{g}(Y_{11}, X_{11}) \\
&= \mathsf{g}(X_{11}, X_{12}, X_{13}, X_{14}) + 2\mathsf{g}(Y_{11}, X_{11}) \\
&= 4 + 2\mathsf{g}(Y_{11}, X_{11}).
\end{aligned} \tag{3.30}$$

Since, from equation (3.29) we know $\mathsf{g}(Y_{11}, X_{11}, X_{1j}) \leq 3$, for $j = 2, 3, 4$, we have from equation (3.30):

$$\begin{aligned}
3.3 &\geq 4 + 2\mathsf{g}(Y_{11}, X_{11}) \\
\text{or, } \mathsf{g}(Y_{11}, X_{11}) &\leq \frac{5}{2}.
\end{aligned} \tag{3.31}$$

Similarly for $j = 2, 3, 4$ it can be shown that:

$$\mathsf{g}(Y_{11}, X_{1j}) \leq \frac{5}{2}. \tag{3.32}$$

Now,

$$\begin{aligned}
&\mathsf{g}(Y_{11}, X_{11}) + \mathsf{g}(Y_{11}, X_{12}) + \mathsf{g}(Y_{11}, X_{13}) + \mathsf{g}(Y_{11}, X_{14}) \\
&\geq \mathsf{g}(Y_{11}, X_{11}, X_{12}) + \mathsf{g}(Y_{11}) + \mathsf{g}(Y_{11}, X_{13}) + \mathsf{g}(Y_{11}, X_{14}) \\
&\geq \mathsf{g}(Y_{11}, X_{11}, X_{12}, X_{13}) + 2\mathsf{g}(Y_{11}) + \mathsf{g}(Y_{11}, X_{14}) \\
&\geq \mathsf{g}(Y_{11}, X_{11}, X_{12}, X_{13}, X_{14}) + 3\mathsf{g}(Y_{11}) \\
&\geq \mathsf{g}(X_{11}, X_{12}, X_{13}, X_{14}) + 3\mathsf{g}(Y_{11}) \\
&= 4 + 6 = 10.
\end{aligned} \tag{3.33}$$

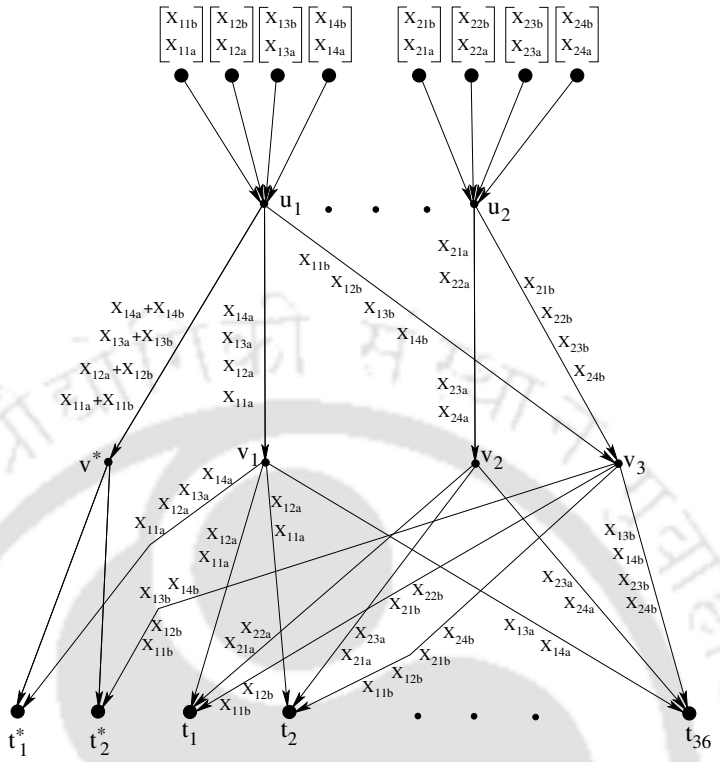

Figure 3.8: A coding scheme showing a $(2, 4)$ fractional linear network coding solution for $\mathcal{N}_*$.

Since from equations (3.31) and (3.32), each of the term in the right hand side of equation (3.33) is less than or equal to $\frac{5}{2}$, and the four terms must sum to make at least 10, it must be that $\mathsf{g}(Y_{11}, X_{11}) = \mathsf{g}(Y_{11}, X_{12}) = \mathsf{g}(Y_{11}, X_{13}) = \mathsf{g}(Y_{11}, X_{14}) = \frac{5}{2}$. In a similar fashion, it can be shown that $\mathsf{g}(Y_{22}, X_{21}) = \mathsf{g}(Y_{22}, X_{22}) = \mathsf{g}(Y_{22}, X_{23}) = \mathsf{g}(Y_{22}, X_{24}) = \frac{5}{2}$.

Since according to definition 4, a rank function of a discrete polymatroid always maps the argument to an integer, and since 2 does not divides 5, the assumption that $\mathcal{N}$ is a $(1, 2)$-discrete polymatroidal network with respect to a discrete polymatroid $\mathbb{D}$ is invalid. Thus $\mathcal{N}_*$ does not have a $(1, 2)$ fractional linear network coding solution.

Let us now assume that $\mathcal{N}_*$ has a $(2, 4)$ routing solution. Let the source s_{ij} generate the message $[X_{ija}\ \ X_{ijb}]$.

Say $X_1 = \{X_{11a}, X_{11b}, X_{12a}, X_{12b}, X_{13a}, X_{13b}, X_{14a}, X_{14b}\}$. Then $Y_{11}, Y_{(u_1,v*)}, Y_{13} \subset X_1$. Because of the demands of the terminals we have, $Y_{11} \cup Y_{13} = X_1$. Also note that $|Y_{11}| \leq 4$, $Y_{(u_1,v*)} \leq 4$ and $|Y_{22}| \leq 4$. Since, $|X_1| = 8$, it must be that $Y_{11} \cap Y_{13} = \emptyset$, and $X_1 \setminus Y_{11} = Y_{13}$ ($\setminus$ is the setminus sign). Now, since the terminal t_1^* must compute all the symbols contained in X_1, we have $Y_{11} \cup Y_{(u_1,v*)} = X_1$. However, as $|X_1| = 8$, and $|Y_{11}| \leq 4$, $Y_{(u_1,v*)} \leq 4$, it must be that $Y_{(u_1,v*)} = X_1 \setminus Y_{11}$. By similar

argumentation, because of the demands of the terminal t_2^*, we have $Y_{(u_1,v*)} = X_1 \setminus Y_{13}$. Therefore $X_1 \setminus Y_{11} = X_1 \setminus Y_{13}$. But, as $X_1 \setminus Y_{11} = Y_{13}$, we have $Y_{13} = X_1 \setminus Y_{13}$, which is certainly not true and hence a contradiction.

A $(2, 4)$ fractional linear network code solution for $\mathcal{N}_*$ is shown in Fig 3.8.

4

Dependency of Characteristic Set on the Message Dimension in Linear Network Coding

Contents

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 which has a scalar/vector linear solution if and only if the characteristic of the finite field belongs to a certain set of primes.

For non-multicast networks, the existence of a vector linear solution may depend upon the characteristic of the finite field, *i.e.*, there exist instances of network coding problems in which a vector linear solution exists if and only if the characteristic of the finite field belongs to a certain set of primes. It has been shown in [18] 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 [19] 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.

Consider a network which has a scalar linear solution if and only if the characteristic of the finite field belongs to P. We first consider the problem that whether such a network can 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 a 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, the network has a d-dimensional vector linear solution if and only if the characteristic of the finite field belongs to P.

We first 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. This shows that if the message dimension is increased from 1 to 2, the set of characteristics over which a vector linear solution exists may get larger. We also show that a similar behaviour may be observed if the message dimension increased from 2 to 3. For any three sets of primes P_1, P_2 and P_3, we show that there exists a network which has a scalar linear solution if and only if the characteristic of the finite field belongs to P_1, has a 2-dimensional vector linear solution if and only if the characteristic of the finite field belongs to $\{P_1, P_2\}$, and has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to $\{P_1, P_2, P_3\}$.

The above two results may indicate that a higher message dimension is superior to a lower message dimension in terms of achieving a vector linear solution over a larger set of characteristics. (Note: A

network having a scalar linear solution over $\mathbb{F}_q$ always has a d-dimensional vector linear solution over $\mathbb{F}_q$, but not vice versa. So a d-dimensional vector linear solution over a finite field can be said to be superior to a scalar linear solution over the same finite field.) But such a hierarchy does not exist between two message dimensions greater than 1. 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 that, if a network has vector linear solutions for two different message dimensions, the set of characteristics over which the network has the vector linear solution for the higher some message dimension, may not be a subset or a superset of the set of characteristics over which the network has the vector linear solution for the lower message dimension.

As a consequence of these results, we prove two more properties of linear network coding. First, recently linear network coding over finite ring alphabets has been studied. In three papers [13], [44], and [12], 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 [13] 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 non-commutative ring 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.

Second, it is known that, an m_1-dimensional vector linear solution and an m_2-dimensional vector linear solution over the same finite field guarantees the existence of an $(m_1 + m_2)$-dimensional vector

linear solution. We show that for a network, the existences 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 if and 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.

In Section 4.1, we present three networks, using which, the results claimed above is proved in Section 4.2. The chapter is concluded in Section 4.3.

4.1 Networks Char-q-y, $\mathcal{G}_1$, $\mathcal{G}_2$, and $\mathcal{G}_3$

In this section, we present four networks Char-q-y, $\mathcal{G}_1$, $\mathcal{G}_2$, and $\mathcal{G}_3$, using which we prove the main results of the chapter.

4.1.1 The Char-q-y network

In [12], Joseph Connelly and Kenneth Zeger presented a network named as the Char-q network which has a vector linear solution for any message dimension if and only if the characteristics of the finite field divides q. Inspired by the Char-q network, we construct a network that we name as the Char-q-y network, where y is a label of a source node. This Char-q-y network will be used for each and every proof presented in this chapter. The source labelled by y is distinguished from the rest because no terminal demands y. We show that if the middle edges of the network do not transmit any information generated by the source y, then the Char-q-y has a scalar linear linear solution over any finite field. But if the middle edges transmit any symbol generated by y, then the Char-q-y 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 another network in such a way that if the other network does not receive any information about y from one of Char-q-y network's 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 vector linear solution for that particular message dimension).

We first give a description of the Char-q-y network. For $q = 2$, the Char-q-y network is presented in Fig. 4.1. It has $q + 3$ sources and $q + 3$ terminals. In q-y of the Char-q-y network, q is a positive

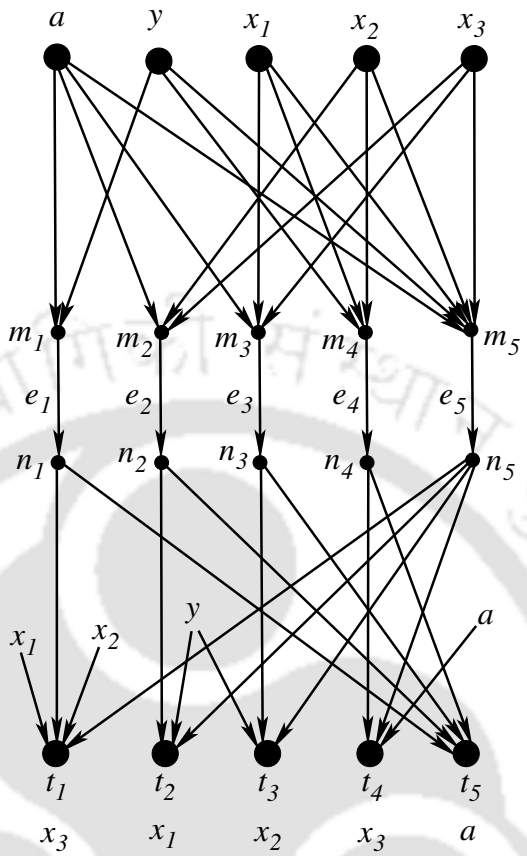

Figure 4.1: The Char-q-y network for $q = 2$. The network has 5 sources and 5 terminals. Out of the 5 sources, 2 sources are labelled as a and y, and the rest 3 sources are labelled as x_1, x_2, and x_3. The Char-2-y network has 5 middle edges: e_1, e_2, e_3, e_4 and e_5. The demands of each terminal is shown below the terminal's label. Note that the source y is not demanded by any of the terminals.

integer (a product of primes), and y is a source label. The source nodes in the Char-q-y network are labelled as: $a, y, x_1, x_2, \ldots, x_{q+1}$ (the reason of why the first two labels a and y are different from the rest will be clear when we will use this network to prove theorems), and the terminal nodes are labelled as: $t_1, t_2, \ldots, t_{q+3}$. The intermediate nodes of the Char-q-y network are union of these two sets: $\{m_1, m_2, \ldots, m_{q+3}\}$ and $\{n_1, n_2, \ldots, n_{q+3}\}$. The list of the edges are given below.

- for $1 \leq i \leq q+3$: $e_i = (m_i, n_i)$ (these are the middle edges).
- for $1 \leq i \leq q+1$ and $i = q+3$: (a, m_i).
- for $i = 1$ and $4 \leq i \leq q+3$: (y, m_i).
- for $1 \leq i \leq q+1$, $2 \leq j \leq q+3$, and $j \neq i+1$: (x_i, m_j).
- for $1 \leq i \leq q+2$: (n_i, t_i) and (n_{q+3}, t_i).

- for $1 \leq i \leq q+2$: (n_i, t_{q+3}).
- for $1 \leq i \leq q$: (x_i, t_1).
- for $i = 2, 3$: (y, t_i).
- (a, t_{q+2}).

The demands of the terminals are given below.

- t_1 demands x_{q+1}.
- for $1 \leq i \leq q+1$: t_{i+1} demands x_i.
- t_{q+3} demands a.

Among the local coding matrices of the Char-q-y network, let the encoding matrices (local coding matrices associated with each source-edge pair) be denoted by $C_{\{s,e\}}$ where s is a source and e is an edge, let the decoding matrices (local coding matrices associated with each edge-terminal pair) be denoted by $C_{\{e,t\}}$ where e is an edge and t is a terminal, and let all other local coding matrices be denoted by $C_{\{e_i,e_j\}}$ where both e_i and e_j are adjacent edges. We now define the following matrices.

(i) $M_i = C_{\{(a,m_i),e_i\}} C_{\{a,(a,m_i)\}}$ for $1 \leq i \leq q+1$ and $i = q+3$.

(ii) $A_i = C_{\{(y,m_i),e_i\}} C_{\{y,(y,m_i)\}}$ for $i = 1$ and $4 \leq i \leq q+3$.

(iii) $W_{(j,i)} = C_{\{(x_i,m_j),e_j\}} C_{\{x_i,(x_i,m_j)\}}$ for $1 \leq i \leq q+1$, $2 \leq j \leq q+3$, and $j \neq i+1$.

(iv) $T_{i1} = C_{\{(n_i,t_i),t_i\}} C_{\{e_i,(n_i,t_i)\}}$ for $1 \leq i \leq q+2$.

(v) $T_{i2} = C_{\{(n_{q+3},t_i),t_i\}} C_{\{e_{q+3},(n_{q+3},t_i)\}}$ for $1 \leq i \leq q+2$.

(vi) $Z_i = C_{\{(n_i,t_{q+3}),t_{q+3}\}} C_{\{e_i,(n_i,t_{q+3})\}}$ for $1 \leq i \leq q+2$.

Let the message carried by the edge e_i be denoted by Y_{e_i} for $1 \leq i \leq q+3$. Below we list the expressions of these messages. Let the message vector generated by the source a be denoted by a, the message vector generated by the source y be denoted by y, and the messgae generated by x_i for $1 \leq i \leq q+1$ be denoted by x_i. Then,

$$Y_{e_1} = M_1 a + A_1 y \tag{4.1}$$

$$Y_{e_2} = M_2 a + \sum_{i=2}^{q+1} W_{(2,i)} x_i \tag{4.2}$$

$$Y_{e_3} = M_3 a + W_{(3,1)} x_1 + \sum_{i=3}^{q+1} W_{(3,i)} x_i \tag{4.3}$$

$$\text{for } 4 \leq j \leq q+1: \quad Y_{e_j} = M_j a + A_j y + \sum_{i=1, i\neq(j-1)}^{q+1} W_{(j,i)} x_i \tag{4.4}$$

$$Y_{e_{q+2}} = A_{q+2} y + \sum_{i=1}^{q} W_{(q+2,i)} x_i \tag{4.5}$$

$$Y_{e_{q+3}} = M_{q+3} a + A_{q+3} y + \sum_{i=1}^{q+1} W_{(q+3,i)} x_i. \tag{4.6}$$

We now prove the following lemma.

Lemma 25. *Over a finite field whose characteristic does not divide q, for any positive integer d, the Char-q-y network has a d-dimensional vector linear solution if and only if A_1 is zero.*

Proof: First consider the 'only if' part. Due to the demands of the terminal t_1, from equations (4.1) and (4.6), we have the following equations.

$$T_{11} M_1 + T_{12} M_{q+3} = 0 \tag{4.7}$$

$$T_{11} A_1 + T_{12} A_{q+3} = 0 \tag{4.8}$$

$$T_{12} W_{(q+3,q+1)} = I. \tag{4.9}$$

Due to the demands of terminal t_2, from equations (4.2) and (4.6), we have the following equations.

$$T_{21} M_2 + T_{22} M_{q+3} = 0 \tag{4.10}$$

$$T_{22} W_{(q+3,1)} = I \tag{4.11}$$

$$\text{for } 2 \leq i \leq q+1: \; T_{21} W_{(2,i)} + T_{22} W_{(q+3,i)} = 0. \tag{4.12}$$

Due to the demands of terminal t_3, from equations (4.3) and (4.6), we have the following equations.

$$T_{31} M_3 + T_{32} M_{q+3} = 0 \tag{4.13}$$

$$T_{31} W_{(3,1)} + T_{32} W_{(q+3,1)} = 0 \tag{4.14}$$

$$T_{32} W_{(q+3,2)} = I \tag{4.15}$$

$$\text{for } 3 \leq i \leq q+1: \quad T_{31} W_{(3,i)} + T_{32} W_{(q+3,i)} = 0. \tag{4.16}$$

Due to the demands of the terminal t_j for $4 \leq j \leq q+1$, from equations (4.4) and (4.6), we have:

$$T_{j1}M_j + T_{j2}M_{q+3} = 0 \tag{4.17}$$

$$T_{j1}A_j + T_{j2}A_{q+3} = 0 \tag{4.18}$$

$$T_{j2}W_{(q+3,j-1)} = I \tag{4.19}$$

$$\text{for } 1 \leq i \leq q+1, i \neq j-1: \quad T_{j1}W_{(j,i)} + T_{j2}W_{(q+3,i)} = 0. \tag{4.20}$$

Due to the demands of the terminal t_{q+2}, from equations (4.5) and (4.6), we have:

$$T_{(q+2)1}A_{q+2} + T_{(q+2)2}A_{q+3} = 0 \tag{4.21}$$

$$\text{for } 1 \leq i \leq q: \quad T_{(q+2)1}W_{(q+2,i)} + T_{(q+2)2}W_{(q+3,i)} = 0 \tag{4.22}$$

$$T_{(q+2)2}W_{(q+3,q+1)} = I. \tag{4.23}$$

Due to the demands of the terminal t_{q+3}, from equations (4.1)-(4.5), we have:

$$Z_1M_1 + Z_2M_2 + ... + Z_{q+1}M_{q+1} = I \tag{4.24}$$

$$Z_1A_1 + Z_4A_4 + ... + Z_{q+2}A_{q+2} = 0 \tag{4.25}$$

$$\text{for } 1 \leq i \leq q+1: \quad \sum_{j=2, j\neq i+1}^{q+2} Z_jW_{(j,i)} = 0. \tag{4.26}$$

From equations (4.9), (4.11), (4.15), (4.19) and (4.23), we get: T_{i2} is invertible for $1 \leq i \leq q+2$, and $W_{(q+3,i)}$ is invertible for $1 \leq i \leq q+1$. Then, from equations (4.12), (4.14), (4.16), (4.20) and (4.22): T_{i1} is invertible for $2 \leq i \leq q+2$, and $W_{(j,i)}$ is invertible for $2 \leq j \leq q+2$, $1 \leq i \leq q+1$, $i \neq j-1$.

From equations (4.7), (4.10), (4.13) and (4.17), we have:

$$\text{for } 2 \leq i \leq q+1: \quad M_i = -T_{i1}^{-1}T_{i2}M_{q+3}. \tag{4.27}$$

Substituting equation (4.27) in equation (4.24), we get:

$$Z_1M_1 - (Z_2T_{21}^{-1}T_{22} + \cdots + Z_{q+1}T_{(q+1)1}^{-1}T_{(q+1)2})M_{q+3} = I. \tag{4.28}$$

From equations (4.18), and (4.21), we have:

$$\text{for } 4 \leq i \leq q+2: \quad A_i = -T_{i1}^{-1}T_{i2}A_{q+3}. \tag{4.29}$$

Substituting equation (4.29) in equation (4.25), we get:

$$Z_1A_1 - (Z_4T_{41}^{-1}T_{42} + \cdots + Z_{q+2}T_{(q+2)1}^{-1}T_{(q+2)2})A_{q+3} = 0. \tag{4.30}$$

From equations (4.12), (4.14), (4.16), (4.20) and (4.22), we have:

$$\text{for } 2 \leq j \leq q+2, 1 \leq i \leq q+1, i \neq j-1 : W_{(j,i)} = -T_{j1}^{-1}T_{j2}W_{(q+3,i)}. \tag{4.31}$$

Substituting equation (4.31) in equation (4.26), for $1 \leq i \leq q+1$ we have:

$$\sum_{j=2, j\neq i+1}^{q+2} Z_jT_{j1}^{-1}T_{j2}W_{(q+3,i)} = 0. \tag{4.32}$$

Since $W_{(q+3,i)}$ for $1 \leq i \leq q+1$ has been already shown to be invertible, for $1 \leq i \leq q+1$, we must have:

$$\sum_{j=2, j\neq i+1}^{q+2} Z_jT_{j1}^{-1}T_{j2} = 0. \tag{4.33}$$

Expanding equation (4.33) for each value of $1 \leq i \leq q+1$, we have:

$$Z_3T_{31}^{-1}T_{32} + Z_4T_{41}^{-1}T_{42} + \cdots + Z_{q+2}T_{(q+2)1}^{-1}T_{(q+2)2} = 0 \tag{4.34}$$

$$Z_2T_{21}^{-1}T_{22} + Z_4T_{41}^{-1}T_{42} + \cdots + Z_{q+2}T_{(q+2)1}^{-1}T_{(q+2)2} = 0 \tag{4.35}$$

$$\vdots \qquad\qquad \vdots \tag{4.36}$$

$$Z_2T_{21}^{-1}T_{22} + Z_3T_{31}^{-1}T_{32} + Z_4T_{41}^{-1}T_{42} + \cdots + Z_{q+1}T_{(q+1)1}^{-1}T_{(q+1)2} = 0. \tag{4.37}$$

Substituting equation (4.37) in equation (4.28) we get:

$$Z_1M_1 = I \tag{4.38}$$

Adding the $q+1$ equations shown in equations (4.34)-(4.37), *i.e.* by performing the operation $\sum_{i=1}^{q+1}\sum_{j=2, j\neq i+1}^{q+2} Z_jT_{j1}^{-1}T_{j2}$, we have:

$$q(Z_2T_{21}^{-1}T_{22} + Z_3T_{31}^{-1}T_{32} + Z_4T_{41}^{-1}T_{42} + \cdots + Z_{q+2}T_{(q+2)1}^{-1}T_{(q+2)2}) = 0. \tag{4.39}$$

Since the characteristic of the finite field does not divide q, we must have $q \neq 0$ in the finite field. Then, from equation (4.39), we must have:

$$Z_2T_{21}^{-1}T_{22} + Z_3T_{31}^{-1}T_{32} + Z_4T_{41}^{-1}T_{42} + \cdots + Z_{q+2}T_{(q+2)1}^{-1}T_{(q+2)2} = 0. \tag{4.40}$$

For each value of $1 \leq i \leq q+1$, subtracting equation (4.33) from (4.40), we get:

$$\text{for } 2 \leq j \leq q+2: \ Z_j T_{j1}^{-1} T_{j2} = 0. \tag{4.41}$$

Substituting the values set by equation (4.41) in equation (4.30), we get:

$$Z_1 A_1 = 0 \tag{4.42}$$

Since Z_1 is invertible due to equation (4.38), we must have $A_1 = 0$. This proves the only if part.

To show the 'if' part, we present a scalar linear solution of the Char-q-y network. In this case all the local coding matrices are elements of the underlying finite field. Chose suitable coding coefficients such that the middle edges carry the following information.

$$\begin{aligned}
&Y_{e_1} = a \\
&\text{for } 2 \leq i \leq q+1: \ Y_{e_i} = a + \sum_{j=1, j\neq i-1}^{q+1} x_i \\
&Y_{e_{q+2}} = \sum_{j=1}^{q} x_i \\
&Y_{e_{q+3}} = a + \sum_{j=1}^{q+1} x_j.
\end{aligned}$$

It can be easily seen that if the middle edges carry information as shown above, all the terminals can compute its desired information. ■

We now proof the following lemma.

Lemma 26. *Over a finite field whose characteristic divides q, the Char-q-y network has scalar linear solution even when $A_i \neq 0$ for $i = 1$ and $4 \leq i \leq q+3$.*

Proof: Let the characteristic of the finite field be p. Chose suitable coding coefficients such

that the middle edges carry the following information.

$$Y_{e_1} = a + y \tag{4.43}$$

$$Y_{e_2} = a + x_2 + x_3 + \cdots + x_{q+1} \tag{4.44}$$

$$Y_{e_3} = a + x_1 + x_3 + \cdots + x_{q+1} \tag{4.45}$$

$$\text{for } 4 \leq i \leq q+1: \; Y_{e_i} = a + y + \sum_{j=1, j\neq i-1}^{q+1} x_i \tag{4.46}$$

$$Y_{e_{q+2}} = y + \sum_{j=1}^{q} x_i \tag{4.47}$$

$$Y_{e_{q+3}} = a + y + \sum_{j=1}^{q+1} x_j. \tag{4.48}$$

Terminals t_i for $1 \leq i \leq q+2$ receives its desired symbols by subtracting the sum of Y_{e_i} and the symbols received from the direct edges, from $Y_{e_{q+3}}$. Terminal t_{q+3} retrieves a by the operation: $\sum_{i=1}^{q+2} Y_i$, as

$$\sum_{i=1}^{q+2} Y_i = (p+1)a + py + \sum_{j=1}^{q+1} px_j = a. \tag{4.49}$$

■

4.1.2 Network $\mathcal{G}_1$

In this subsection we present a network that we label as $\mathcal{G}_1$. Network $\mathcal{G}_1$ is constructed by joining together the M-network and the Char-q-$\bar{y}$ network. Recall from [3] that the M-network has four sources and four terminals, where each terminals demand two sources. The sources of the M-network are grouped into two subsets $(\bar{a}, \bar{b})$ and $(\bar{x}, \bar{y})$, and each terminal demands a unique tuple of two sources with the condition that none of the terminals can demand either of $(\bar{a}, \bar{b})$ and $(\bar{x}, \bar{y})$. The four terminals of the M-network are labelled as $\bar{t}_1, \bar{t}_2, \bar{t}_3$ and $\bar{t}_4$. The Char-q-$\bar{y}$ network consist of $q+3$ sources: $\bar{a}, \bar{y}, \bar{x}_1, \ldots, \bar{x}_{q+1}$, and $q+3$ terminals: $\bar{t}_5, \bar{t}_6, \ldots, \bar{t}_{q+7}$. $\mathcal{G}_1$ is shown in Fig. 4.2 for $q = 2$. The Char-q-$\bar{y}$ network and the M-network are connected to construct $\mathcal{G}_1$ in the following way: the sources $\bar{a}$ and $\bar{y}$ are made common to both of the networks, and an edge $(\bar{n}_1, \bar{t}_4)$ (where $\bar{n}_1$ is the head node of $\bar{e}_1$) connects edge $\bar{e}_1$ of the Char-q-$\bar{y}$ network to the terminal $\bar{t}_4$ of the M-network. Let the message carried by the edge $\bar{e}_i$ be denoted by Y_i.

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 $\bar{t}_4$ receives an extra symbol

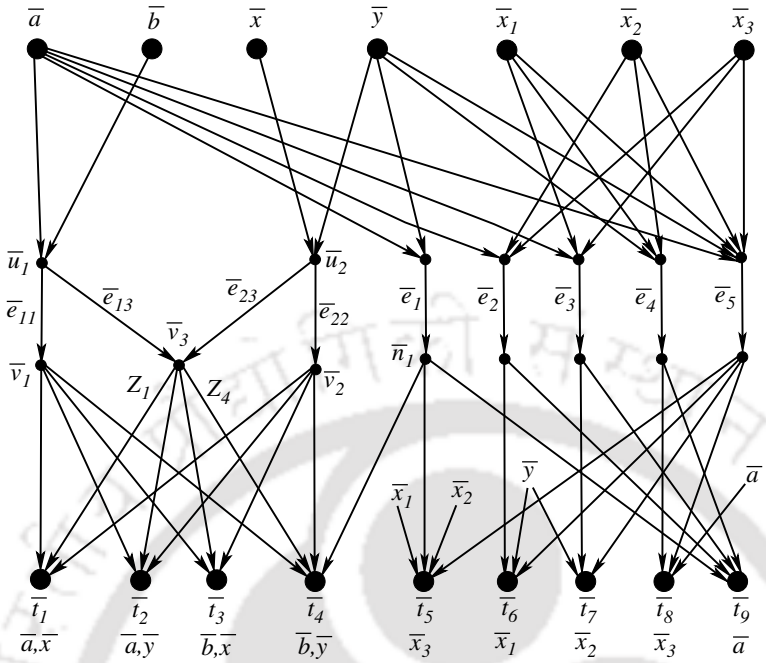

Figure 4.2: Network $\mathcal{G}_1$ for $q = 2$. This network is a conjunction of the M-network and a Char-2-$\bar{y}$ network (with sources $\bar{a}$ and $\bar{y}$ common to both networks). The demands of the terminals are written below the label of the terminals. Terminals $\bar{t}_1, \bar{t}_2, \bar{t}_3$ and $\bar{t}_4$ demands two source messages. The sources $\bar{a}, \bar{b}, \bar{x}, \bar{y}$ are the four sources of the M-network, and $\bar{a}, \bar{y}, \bar{x}_1, \bar{x}_2, \bar{x}_3$ are the 5 sources of the Char-2-$\bar{y}$ network.

which is a function of $\bar{a}$ and $\bar{y}$, then the network does have a scalar linear solution. In $\mathcal{G}_1$, terminal $\bar{t}_4$ can have this extra information if the message $Y_{\bar{e}_1}$ is a function of $\bar{y}$. But, from Lemma 25 we know that if $Y_{\bar{e}_1}$ is a function of $\bar{y}$, then the characteristic of the finite field has to divide q, thus limiting the set of finite fields that over which a scalar linear solution exists.

$\mathcal{G}_1$ will be used to prove some of the theorems in this chapters. We here prove that for odd message dimensions, $\mathcal{G}_1$ has a vector linear solution if and only if the characteristic of the finite field divides q.

Let f be the function that maps the network $\mathcal{G}_1$ to a discrete polymatroid $\mathbb{D}_1$ such that $\mathcal{G}_1$ is a discrete polymatroidal network with respect to $\mathbb{D}_1$. Let ρ be the rank function of $\mathbb{D}_1$. Now let $\mathsf{g} = \rho \circ f$.

Lemma 27. *For any odd number d, the network $\mathcal{G}_1$ has a d-dimensional vector linear solution if and only if the characteristic of the finite field divides q.*

Proof: Consider the 'only if' part. We show that if the characteristic of the finite field does not divide q, then $\mathcal{G}_1$ has no odd dimensional vector linear solution. Since the characteristic either divides q or does not divide q, proving the latter statement would prove the 'only if' part. Let's assume that over a finite field whose characteristic does not divide q, $\mathcal{G}_1$ has a d-dimensional vector linear solution

for any odd number d. Due to the demands of terminal $\bar{t}_1$ we get the following:

$$\begin{aligned}
\mathsf{g}(Y_{11},\bar{a})+\mathsf{g}(Y_{22},\bar{x}) &= \mathsf{g}(Y_{11},\bar{a},Y_{22},\bar{x}) && \text{[using Lemma 5 repetitively]}\\
&\leq \mathsf{g}(Y_{11},\bar{a},Y_{22},\bar{x},Z_1)\\
&= \mathsf{g}(Y_{11},Y_{22},Z_1) && \text{[due to the demands of } \bar{t}_1\text{]}\\
&\leq 3d. && \text{[as rank of each element is less than or equal to } d\text{]}. \qquad (4.50)
\end{aligned}$$

Similar to equation (4.50), due to the demands of $\bar{t}_1, \bar{t}_2$ and $\bar{t}_3$ we have the following equations.

$$\mathsf{g}(Y_{11},\bar{a})+\mathsf{g}(Y_{22},\bar{y}) \leq 3d \qquad (4.51)$$

$$\mathsf{g}(Y_{11},\bar{b})+\mathsf{g}(Y_{22},\bar{x}) \leq 3d. \qquad (4.52)$$

Since the characteristic of the finite field does not divide q, from lemma 25 we know that the message carried by $Y_{\bar{e}_1}$ is not a function of $\bar{y}$.

$$\begin{aligned}
\mathsf{g}(Y_{11},\bar{a})+d+d &\geq \mathsf{g}(Y_{11},\bar{a})+\mathsf{g}(Y_{22})+\mathsf{g}(Z_4)\\
&\geq \mathsf{g}(Y_{11},\bar{a},Y_{22},Z_4)\\
&= \mathsf{g}(Y_{11},\bar{a},Y_{22},Z_4,Y_{\bar{e}_1}) && \text{[since } Y_{\bar{e}_1} \text{ is function of only } \bar{a}\text{]}\\
&= \mathsf{g}(Y_{11},\bar{a},Y_{22},Z_4,Y_{\bar{e}_1},\bar{b},\bar{y}) && \text{[due to the demands of } \bar{t}_4\text{]}\\
&\geq \mathsf{g}(\bar{a},Y_{22},\bar{b},\bar{y})\\
&= \mathsf{g}(\bar{a},\bar{b})+\mathsf{g}(Y_{22},\bar{y}|\bar{a},\bar{b})\\
&= \mathsf{g}(\bar{a},\bar{b})+\mathsf{g}(Y_{22},\bar{y}) && \text{[since } \{Y_{22},\bar{y}\} \text{ is independent of } \{\bar{a},\bar{b}\}\text{]}\\
&= 2d+\mathsf{g}(Y_{22},\bar{y}). \qquad (4.53)
\end{aligned}$$

From equation (4.53), we get that

$$\mathsf{g}(Y_{11},\bar{a}) \geq \mathsf{g}(Y_{22},\bar{y}). \qquad (4.54)$$

We know:

$$\begin{aligned}
4d &= \mathsf{g}(\bar{a},\bar{b},\bar{x},\bar{y})\\
&= \mathsf{g}(\bar{a},\bar{b},\bar{x},\bar{y},Y_{11},Y_{13},Y_{22},Y_{23})\\
&= \mathsf{g}(Y_{11},Y_{13},Y_{22},Y_{23})\\
&\leq \mathsf{g}(Y_{11})+\mathsf{g}(Y_{13})+\mathsf{g}(Y_{22})+\mathsf{g}(Y_{23})
\end{aligned}$$

$$\leq 4d. \tag{4.55}$$

Since rank of any element is less than or equal to d, from equation (4.55), we get:

$$\mathrm{g}(Y_{11}) = \mathrm{g}(Y_{13}) = \mathrm{g}(Y_{22}) = \mathrm{g}(Y_{23}) = d. \tag{4.56}$$

We also have:

$$\begin{aligned}
&\mathrm{g}(Y_{11}, \bar{a}) + \mathrm{g}(Y_{11}, \bar{b}) \\
&\geq \mathrm{g}(Y_{11}, \bar{a}, \bar{b}) + \mathrm{g}(Y_{11}) \qquad \text{[using rule [P3] of Definition 4]} \\
&= \mathrm{g}(\bar{a}, \bar{b}) + \mathrm{g}(Y_{11}) \\
&= 3d \qquad \text{[we used equation (4.56)].}
\end{aligned} \tag{4.57}$$

Similar to equation (4.57) we have:

$$\mathrm{g}(Y_{22}, \bar{x}) + \mathrm{g}(Y_{22}, \bar{y}) \geq 3d. \tag{4.58}$$

Adding equations (4.50) and (4.51), we get:

$$\begin{aligned}
&2\mathrm{g}(Y_{11}, \bar{a}) + \mathrm{g}(Y_{22}, \bar{x}) + \mathrm{g}(Y_{22}, \bar{y}) \leq 6d \\
&\text{or, } 2\mathrm{g}(Y_{11}, \bar{a}) \leq 3d \qquad \text{[substituting equation (4.58)]} \\
&\text{or, } \mathrm{g}(Y_{11}, \bar{a}) \leq \frac{3d}{2}.
\end{aligned} \tag{4.59}$$

Adding equations (4.50) and (4.52), we get:

$$\begin{aligned}
&\mathrm{g}(Y_{11}, \bar{a}) + \mathrm{g}(Y_{11}, \bar{b}) + 2\mathrm{g}(Y_{22}, \bar{x}) \leq 6d \\
&\text{or, } 2\mathrm{g}(Y_{22}, \bar{x}) \leq 3d \qquad \text{[substituting equation (4.57)]} \\
&\text{or, } \mathrm{g}(Y_{22}, \bar{x}) \leq \frac{3d}{2}.
\end{aligned} \tag{4.60}$$

From equation (4.54) we have:

$$\mathrm{g}(Y_{22}, \bar{y}) \leq \frac{3d}{2}. \tag{4.61}$$

Since d is an odd integer, let $d = 2n - 1$ where n is any positive integer. Then, from equations (4.60)

and (4.61), we have:

$$\mathrm{g}(Y_{22}, \bar{x}) \leq \frac{3(2n-1)}{2} = 3n - \frac{3}{2} = 3n - 2 + \frac{1}{2} \tag{4.62}$$

$$\mathrm{g}(Y_{22}, \bar{y}) \leq \frac{3(2n-1)}{2} = 3n - \frac{3}{2} = 3n - 2 + \frac{1}{2}. \tag{4.63}$$

Since the rank function $\mathrm{g}()$ is integer valued by definition, from equations (4.62) and (4.63), we have:

$$\mathrm{g}(Y_{22}, \bar{x}) \leq 3n - 2 \tag{4.64}$$

$$\mathrm{g}(Y_{22}, \bar{y}) \leq 3n - 2. \tag{4.65}$$

Substituting values from equation (4.64) and (4.65) in equation (4.58), we get:

$$6n - 4 \geq 3d = 3(2n-1) = 6n - 3. \tag{4.66}$$

Equation (4.66) results in $3 \geq 4$, which is a contradiction.

We now show the 'if' part of the proof. We show that $\mathcal{G}_1$ 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 edges $Y_{\bar{e}_i}$ for $1 \leq i \leq q+3$ carry the messages as indicated by equations (4.43)-(4.48). Then, the terminals $\bar{t}_5$ to $\bar{t}_{q+7}$ can retrieve its desired information (the terminals in the Char-q-$\bar{y}$ part retrieves its desired information as shown in Lemma 26). Now, in the M-network part, let $Y_{11} = \bar{a}$, $Y_{13} = \bar{b}$, $Y_{22} = \bar{x}$, and $Y_{23} = \bar{y}$. Then, it can be easily seen that terminals $\bar{t}_1, \bar{t}_2$ and $\bar{t}_3$ can retrieve its desired information. The terminal $\bar{t}_4$ receives $\bar{a}$ from Y_{11}, $\bar{b}$ from Z_4, $\bar{a} + \bar{y}$ from $Y_{\bar{e}_1}$, and as a result it can deduce $\bar{y}$ as well (by subtracting $\bar{a}$ from $\bar{a} + \bar{y}$). ■

4.1.3 Network $\mathcal{G}_2$

In this section, we present another network that we label as $\mathcal{G}_2$. In Fig. 3.3 of Chapter 3, for each value of a positive integer $m \geq 2$ we constructed a network $\mathcal{N}_m$ called as the generalized M-network. For convenience $\mathcal{N}_3$ is produced in Fig. 4.3. The network $\mathcal{G}_2$ is a conjunction the network $\mathcal{N}_3$, the Char-q'-x network, and some additional edges. For $q' = 2$, the network $\mathcal{G}_2$ is shown in Fig. 4.4.

In the $\mathcal{N}_3$ part of $\mathcal{G}_2$, the nine sources are: $a, b, c, r, s, w, x, y, z$. The messages carried by edges (v_i, u_i) and (v_i, u_j) for $i = 1, 2, 3$, $j = 4, 5$ is denoted by Y_{ii} and Y_{ij} respectively. For terminals t_i for $1 \leq i \leq 27$ there exists an edge (u_j, t_i) for $j = 1, 2, 3, 4, 5$. For $1 \leq i \leq 27$, the message carried by the edge (u_4, t_i) is denoted by $Z_{4,i}$, and the message carried by the edge (u_5, t_i) is denoted by $Z_{5,i}$.

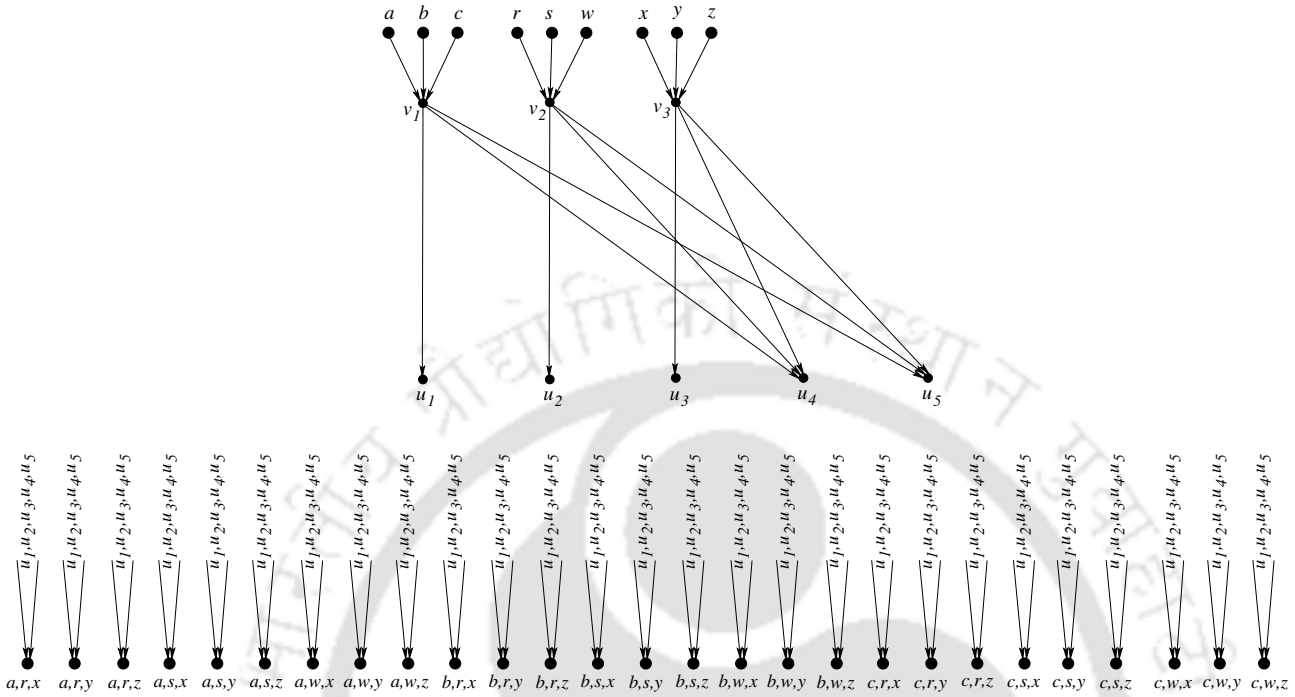

Figure 4.3: The generalized M-network $\mathcal{N}_m$ for $m = 3$.

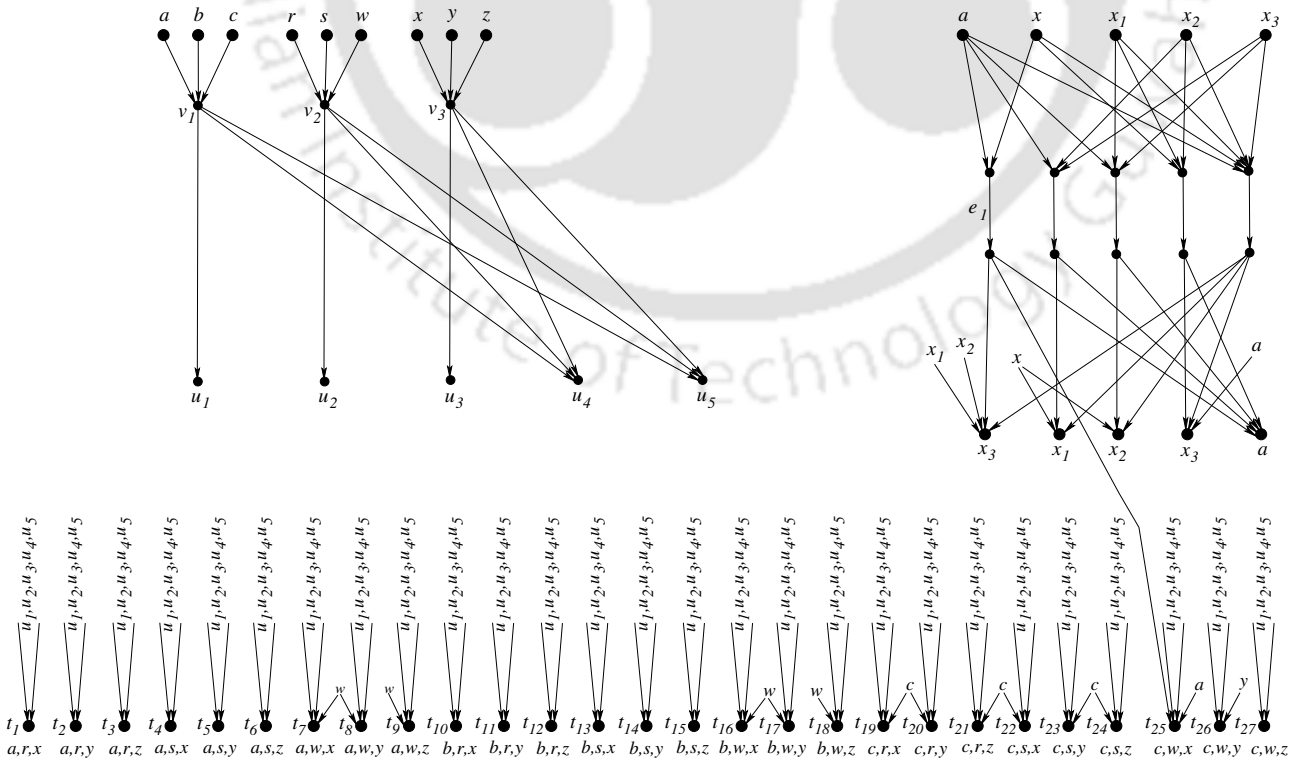

Figure 4.4: The network $\mathcal{G}_2$ for $q' = 2$.

The $q'+3$ source nodes of the Char-q'-x network are: $a, x, x_1, \ldots, x_{q'+1}$ (note that the $\mathcal{N}_3$ network and Char-q'-x network has sources a and x in common). Edge e_1 is the middle edge of the Char-q'-x network which has paths from a and x, but not from any other sources. The message carried by e_1 is denoted by Y_{e_1}.

The additional edges that are not part of $\mathcal{N}_3$ and Char-q'-x, are listed below:

- (w, t_7), (w, t_8), (w, t_9), (w, t_{16}), (w, t_{17}), (w, t_{18}).
- (c, t_{19}), (c, t_{20}), (c, t_{21}), (c, t_{22}), (c, t_{23}), (c, t_{24}).
- (a, t_{25}).
- (y, t_{26}).
- $(head(e_1), t_{25})$.

We first develop some general equations that hold for the network $\mathcal{G}_2$. Let f be the function that maps the network $\mathcal{G}_2$ to a discrete polymatrid $\mathbb{D}_2$ such that $\mathcal{G}_2$ is a discrete polymatroidal network with respect to $\mathbb{D}_2$. Let ρ be the rank function of $\mathbb{D}_2$, and let $\rho_{max} \leq d$. Now let $\mathsf{g} = \rho \circ f$. Then we have the following equations:

$$\begin{aligned}
&\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, r) + \mathsf{g}(Y_{33}, x) \\
&= \mathsf{g}(Y_{11}, a, Y_{22}, r, Y_{33}, x) \qquad \text{[using Lemma 5 repetitively]} \qquad (4.67) \\
&\leq \mathsf{g}(Y_{11}, a, Y_{22}, r, Y_{33}, x, Z_{4,1}, Z_{5,1}) \\
&\leq \mathsf{g}(Y_{11}, Y_{22}, Y_{33}, Z_{4,1}, Z_{5,1}) \qquad \text{[due the demands of } t_1\text{]} \\
&\leq 5d \qquad \text{[since rank of any element is less than or equal to } d\text{]}. \qquad (4.68)
\end{aligned}$$

Similar to equation (4.68), we have the following equations:

$$\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, r) + \mathsf{g}(Y_{33}, y) \leq 5d \qquad (4.69)$$

$$\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, r) + \mathsf{g}(Y_{33}, z) \leq 5d \qquad (4.70)$$

$$\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, s) + \mathsf{g}(Y_{33}, x) \leq 5d \qquad (4.71)$$

$$\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, s) + \mathsf{g}(Y_{33}, y) \leq 5d \qquad (4.72)$$

$$\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, s) + \mathsf{g}(Y_{33}, z) \leq 5d \qquad (4.73)$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, x) \leq 5d \tag{4.74}$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, y) \leq 5d \tag{4.75}$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, z) \leq 5d \tag{4.76}$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, x) \leq 5d \tag{4.77}$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, y) \leq 5d \tag{4.78}$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, z) \leq 5d \tag{4.79}$$

$$\mathrm{g}(Y_{11}, c) + \mathrm{g}(Y_{22}, w) + \mathrm{g}(Y_{33}, z) \leq 5d. \tag{4.80}$$

We also have the following inequalities:

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{11}, c) \geq 5d \tag{4.81}$$

$$\mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{22}, w) \geq 5d \tag{4.82}$$

$$\mathrm{g}(Y_{33}, x) + \mathrm{g}(Y_{33}, y) + \mathrm{g}(Y_{33}, z) \geq 5d. \tag{4.83}$$

We prove one of equations (4.81)-(4.83) and the rest can be prove similarly.

$$\begin{aligned}
&\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{11}, c) \\
&\geq \mathrm{g}(Y_{11}, a, b) + \mathrm{g}(Y_{11}) + \mathrm{g}(Y_{11}, c) \qquad \text{[applying rule [P3] of Definition 4]} \\
&\geq \mathrm{g}(Y_{11}, a, b, c) + 2\mathrm{g}(Y_{11}) \\
&= \mathrm{g}(a, b, c) + 2\mathrm{g}(Y_{11}) \\
&= 5d.
\end{aligned}$$

Adding equations (4.81)-(4.83), we have:

$$\begin{aligned}
&\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{11}, c) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{22}, w) + \mathrm{g}(Y_{33}, x) \\
&\qquad + \mathrm{g}(Y_{33}, y) + \mathrm{g}(Y_{33}, z) \geq 15d \\
&\text{or, } (\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, x)) + (\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, y)) + \mathrm{g}(Y_{11}, c) \\
&\qquad + \mathrm{g}(Y_{22}, w) + \mathrm{g}(Y_{33}, z) \geq 15d.
\end{aligned} \tag{4.84}$$

But as equations (4.68), (4.78) and (4.80) hold, from equation (4.84), we have:

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, x) = 5d \tag{4.85}$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, y) = 5d \tag{4.86}$$

$$\mathrm{g}(Y_{11}, c) + \mathrm{g}(Y_{22}, w) + \mathrm{g}(Y_{33}, z) = 5d. \tag{4.87}$$

Similarly, rearranging equation (4.84), we get the following equalities:

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, y) = 5d \tag{4.88}$$

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, x) = 5d \tag{4.89}$$

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, y) = 5d \tag{4.90}$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, x) = 5d \tag{4.91}$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, y) = 5d \tag{4.92}$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, x) = 5d. \tag{4.93}$$

Subtracting equations (4.85) from (4.91), we get:

$$\mathrm{g}(Y_{11}, a) = \mathrm{g}(Y_{11}, b). \tag{4.94}$$

Subtracting equations (4.85) from (4.89), we get:

$$\mathrm{g}(Y_{22}, r) = \mathrm{g}(Y_{22}, s). \tag{4.95}$$

Subtracting equations (4.85) from (4.88), we get:

$$\mathrm{g}(Y_{33}, x) = \mathrm{g}(Y_{33}, y). \tag{4.96}$$

As equations (4.68), (4.78) and (4.80) holds, from equation (4.84) we also have:

$$\begin{aligned}(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, x)) + (\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, y)) + \mathrm{g}(Y_{11}, c) \\ + \mathrm{g}(Y_{22}, w) + \mathrm{g}(Y_{33}, z) = 15d.\end{aligned} \tag{4.97}$$

Rearranging terms in equation (4.97), we have:

$$\begin{aligned}(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{11}, c)) + (\mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{22}, w)) + (\mathrm{g}(Y_{33}, x) \\ + \mathrm{g}(Y_{33}, y) + \mathrm{g}(Y_{33}, z)) = 15d.\end{aligned} \tag{4.98}$$

As equations (4.81)-(4.83) holds, we must have:

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{11}, c) = 5d \tag{4.99}$$

$$\mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{22}, w) = 5d \tag{4.100}$$

$$\mathrm{g}(Y_{33}, x) + \mathrm{g}(Y_{33}, y) + \mathrm{g}(Y_{33}, z) = 5d. \tag{4.101}$$

Applying equations (4.94)-(4.96) to equations (4.99)-(4.101), we have:

$$2\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{11}, c) = 5d \tag{4.102}$$

$$2\mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{22}, w) = 5d \tag{4.103}$$

$$2\mathrm{g}(Y_{33}, x) + \mathrm{g}(Y_{33}, z) = 5d. \tag{4.104}$$

Multiplying equation (4.70) by 2 and then adding to equation (4.87), we have:

$$\begin{aligned}
&2(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, z)) + \mathrm{g}(Y_{11}, c) + \mathrm{g}(Y_{22}, w) + \mathrm{g}(Y_{33}, z) \leq 15d \\
&\text{or, } 5d + 5d + 3\mathrm{g}(Y_{33}, z) \leq 15d \qquad \text{[substituting equations (4.102) and (4.103)]} \\
&\text{or, } 3\mathrm{g}(Y_{33}, z) \leq 5d \\
&\text{or, } \mathrm{g}(Y_{33}, z) \leq \frac{5d}{3}.
\end{aligned} \tag{4.105}$$

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 Y_{e_1} in the Char-q'-x network is independent of x (from Lemma 25), and is a function of only a. So due to the demands of terminal t_{25}, we have:

$$\begin{aligned}
&\mathrm{g}(Y_{11}, a, c) + \mathrm{g}(Y_{22}, w) + \mathrm{g}(Y_{33}, x) \\
&= \mathrm{g}(Y_{11}, Y_{22}, Y_{33}, a, c, w, x) \qquad \text{[using Lemma 5 repetitively]} \\
&\leq \mathrm{g}(Y_{11}, Y_{22}, Y_{33}, a, c, w, x, Z_{4,27}, Z_{5,27}) \\
&= \mathrm{g}(Y_{11}, Y_{22}, Y_{33}, a, c, w, x, Z_{4,27}, Z_{5,27}, Y_{e_1}) \\
&= \mathrm{g}(Y_{11}, Y_{22}, Y_{33}, a, Z_{4,27}, Z_{5,27}, Y_{e_1}) \qquad \text{[due to demands of } t_{25}\text{]} \\
&= \mathrm{g}(Y_{11}, Y_{22}, Y_{33}, a, Z_{4,27}, Z_{5,27}) \\
&= \mathrm{g}(Y_{22}, Y_{33}, Z_{4,27}, Z_{5,27}) + \mathrm{g}(Y_{11}, a | Y_{22}, Y_{33}, Z_{4,27}, Z_{5,27}) \\
&\leq \mathrm{g}(Y_{22}, Y_{33}, Z_{4,27}, Z_{5,27}) + \mathrm{g}(Y_{11}, a) \\
&\leq 4d + \mathrm{g}(Y_{11}, a).
\end{aligned} \tag{4.106}$$

It can be seen that due to terminals t_1, t_{14}, and t_{27} all of the source messages are to be retrieved from $\{Y_{ii}, Y_{ij} | i = 1, 2, 3 \text{ and } j = 4, 5\}$. Then like equation (3.7) it can be shown that $Y_{11} = d$. Then,

$$\begin{aligned}
&\mathsf{g}(Y_{11}, a, c) + \mathsf{g}(Y_{11}, a) \\
&= \mathsf{g}(Y_{11}, a, c) + \mathsf{g}(Y_{11}, b) && \text{[from equation (4.94)]} \\
&\geq \mathsf{g}(Y_{11}, a, c, b) + \mathsf{g}(Y_{11}) && \text{[using rule [P3] of Definition 4]} \\
&\geq 4d.
\end{aligned}$$

Then we have

$$\mathsf{g}(Y_{11}, a, c) \geq 4d - \mathsf{g}(Y_{11}, a). \tag{4.107}$$

Substituting equation (4.107) in equation (4.106), we have:

$$\mathsf{g}(Y_{11}, w) + \mathsf{g}(Y_{33}, x) \leq 2\mathsf{g}(Y_{11}, a). \tag{4.108}$$

We first show that $\mathcal{G}_2$ has no scalar linear solution.

Lemma 28. *The network $\mathcal{G}_2$ has no scalar linear solution over any finite field.*

Proof: Note that equations (4.106)-(4.108) cannot be used as they hold only if the characteristic of the finite field divides q'; and current lemma is to be shown to be true over all finite fields. Let us assume that the network has a scalar linear solution. Then, $\rho_{max} \leq 1$ where ρ is the rank function of $\mathbb{D}_2$, with respect to which $\mathcal{G}_2$ is a discrete polymatroidal network.

Since $d = 1$, and the rank function of a discrete polymatroid is always an integer, from equation (4.105) we have: $\mathsf{g}(Y_{33}, z) \leq 1$. Since $1 = \mathsf{g}(z) \leq \mathsf{g}(Y_{33}, z)$, we must have:

$$\mathsf{g}(Y_{33}, z) = 1. \tag{4.109}$$

Substituting equation (4.109) in equation (4.87), we have:

$$\mathsf{g}(Y_{11}, c) + \mathsf{g}(Y_{22}, w) = 4. \tag{4.110}$$

Since rank of any element is less than or equal to 1, we have $\mathsf{g}(Y_{11}, c) \leq 2$ and $\mathsf{g}(Y_{22}, w) \leq 2$. Then equation (4.110) implies:

$$\mathsf{g}(Y_{11}, c) = 2. \tag{4.111}$$

Substituting equation (4.111) in equation (4.102), we have:

$$\begin{aligned} 2\mathrm{g}(Y_{11}, a) &= 3 \\ \text{or, } \mathrm{g}(Y_{11}, a) &= \frac{3}{2}. \end{aligned} \tag{4.112}$$

Equation (4.112) is a contradiction as the rank function always outputs an integer. ■

We now prove the following lemma.

Lemma 29. *The network $\mathcal{G}_2$ has a 2-dimensional vector linear solution if and only if the characteristic of the finite field divides q'.*

Proof:

Consider the 'only if' part. We show that if the characteristic of the finite field does not divide q' then network $\mathcal{G}_2$ has no 2-dimensional vector linear solution. We prove this result by contradiction. Assume that $\mathcal{G}_2$ has a 2-dimensional vector linear solution even when the characteristic of the finite field does not divide q'. So we have $\rho_{max} = d = 2$ for the discrete polymatroid $\mathbb{D}_2$.

Since the rank function of a discrete polymatroid is integer valued, from equation (4.105), we have:

$$\mathrm{g}(Y_{33}, z) \leq 3. \tag{4.113}$$

Substituting equation (4.113) in equation (4.104), we have:

$$\mathrm{g}(Y_{33}, x) \geq \frac{7}{2}. \tag{4.114}$$

Then it mus that

$$\mathrm{g}(Y_{33}, x) \geq 4. \tag{4.115}$$

Since rank of an element is less than or equal to 2, we must have:

$$\mathrm{g}(Y_{33}, x) = 4. \tag{4.116}$$

Substituting equation (4.116) in equation (4.104), we have:

$$\mathrm{g}(Y_{33}, z) = 2. \tag{4.117}$$

Substituting equation (4.117) in equation (4.87), we have:

$$\mathrm{g}(Y_{11}, c) + \mathrm{g}(Y_{22}, w) = 8. \tag{4.118}$$

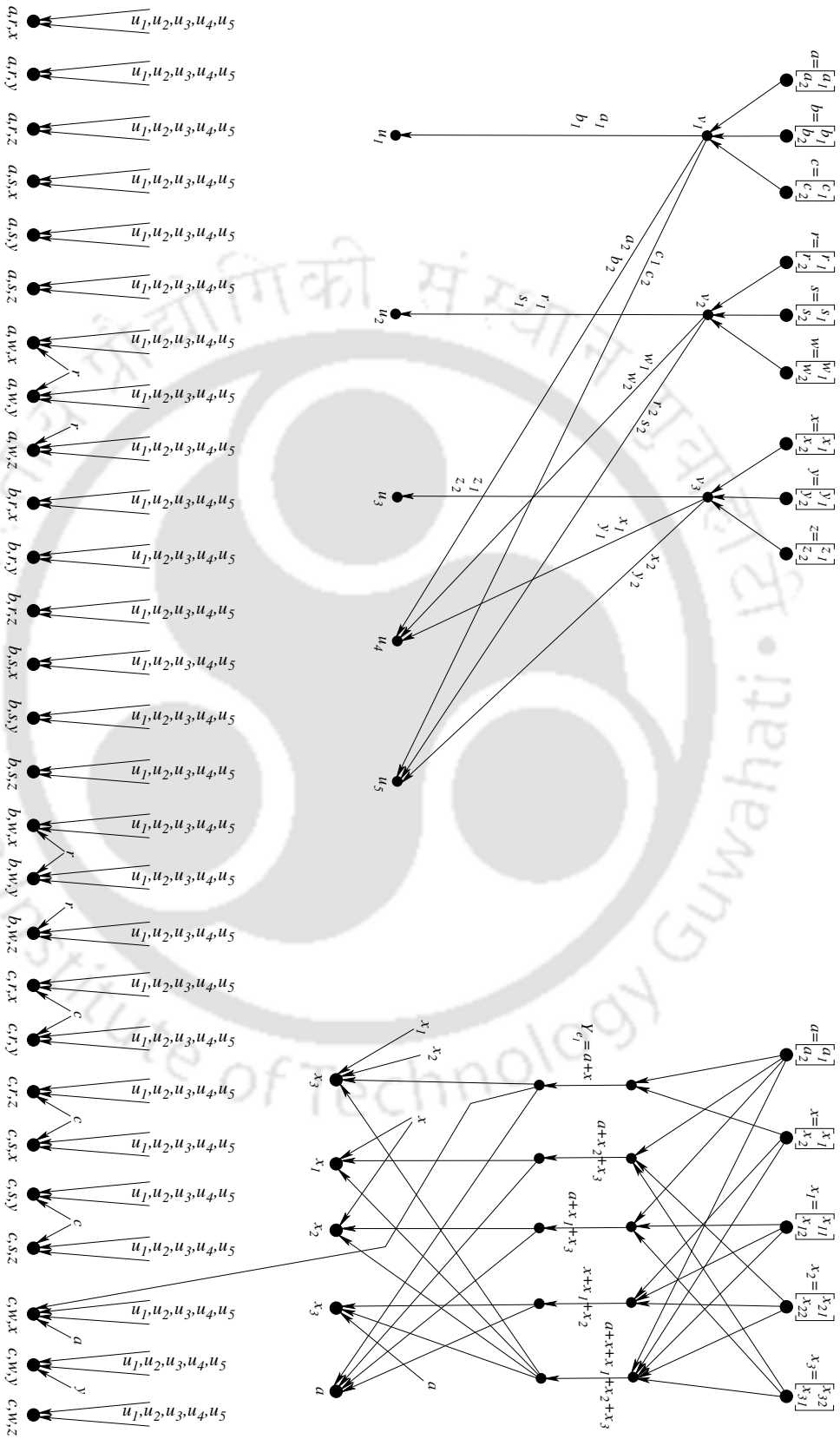

Figure 4.5: A 2-dimensional vector linear solution of $\mathcal{G}_2$ for $q' = 2$ when the characteristic divides q'.

Since rank of an element is less than or equal to 2, we must have:

$$\mathrm{g}(Y_{11}, c) = 4 \tag{4.119}$$

$$\mathrm{g}(Y_{22}, w) = 4. \tag{4.120}$$

Substituting equation (4.119) in equation (4.102), we have (note $d = 2$):

$$\mathrm{g}(Y_{11}, a) = 3. \tag{4.121}$$

Substituting equations (4.116), (4.120), and (4.121) in equation (4.108), we have: $8 \leq 6$, which is a contradiction.

To prove the 'if' part we present a 2-dimensional coding scheme over a finite field whose characteristic divides q'. In fig. 4.5 we show a 2-dimensional vector linear solution of $\mathcal{G}_2$ when $q' = 2$. This coding scheme can easily be extended for any value of q'. (For a different value of q', only a decoding matrix in the Char-q'-x network changes (see equation (4.49).) ■

Now, consider the following lemma.

Lemma 30. *The network $\mathcal{G}_2$ has a 5-dimensional vector linear solution if and only if the characteristic of the finite field divides q'.*

Proof: Consider the 'only if' part. We show that if the characteristic of the finite field does not divide q' then network $\mathcal{G}_2$ has no 5-dimensional vector linear solution. We prove this result by contradiction. Assume that $\mathcal{G}_2$ has a 5-dimensional vector linear solution when the characteristic of the finite field does not divide q'. So we have $d = 5$ for the discrete polymatroid $\mathcal{D}_2$.

Since the rank function of a discrete polymatroid is integer valued, from equation (4.105) we have:

$$\mathrm{g}(Y_{33}, z) \leq 8. \tag{4.122}$$

From equation (4.104) we get that $25 - \mathrm{g}(Y_{33}, z)$ must be divisible by 2 (otherwise $\mathrm{g}(Y_{33}, x)$ would not be an integer). Hence $\mathrm{g}(Y_{33}, z)$ must be an odd number. For similar reasoning, from equations (4.102) and (4.103) we get that $\mathrm{g}(Y_{11}, c)$ and $\mathrm{g}(Y_{22}, w)$ must be odd numbers.

Then, since $5 = \mathrm{g}(z) \leq \mathrm{g}(Y_{33}, z)$, either $\mathrm{g}(Y_{33}, z) = 5$ or $\mathrm{g}(Y_{33}, z) = 7$.

Case I: $\mathrm{g}(Y_{33}, z) = 5$.

Substituting $\mathsf{g}(Y_{33}, z) = 5$ in equation (4.87), we get:

$$\mathsf{g}(Y_{11}, c) + \mathsf{g}(Y_{22}, w) = 20. \tag{4.123}$$

Since rank of any union of two elements is less than or equal to 10, we must have

$$\mathsf{g}(Y_{11}, c) = \mathsf{g}(Y_{22}, w) = 10. \tag{4.124}$$

But equation (4.124) is a contradiction because as we have argued, $\mathsf{g}(Y_{11}, c)$ and $\mathsf{g}(Y_{22}, w)$ must be odd numbers.

Case II: $\mathsf{g}(Y_{33}, z) = 7$.

Substituting $\mathsf{g}(Y_{33}, z) = 7$ in equation (4.104) we have:

$$\mathsf{g}(Y_{33}, x) = 9. \tag{4.125}$$

Substituting $\mathsf{g}(Y_{33}, z) = 7$ in equation (4.87), we get:

$$\mathsf{g}(Y_{11}, c) + \mathsf{g}(Y_{22}, w) = 18. \tag{4.126}$$

Since neither of $\mathsf{g}(Y_{11}, c)$ and $\mathsf{g}(Y_{22}, w)$ can be equal to 10 (as 10 is an even number), we must have:

$$\mathsf{g}(Y_{11}, c) = 9 \tag{4.127}$$

$$\mathsf{g}(Y_{22}, w) = 9. \tag{4.128}$$

Substituting equation (4.127) in equation (4.102) we have:

$$\mathsf{g}(Y_{11}, a) = 8. \tag{4.129}$$

Substituting equations (4.125), (4.128), and (4.129) in equation (4.108), we have: $18 \leq 16$, which is a contradiction.

To prove the 'if' part we now design a 5-dimensional vector linear solution when the characteristic of the finite field divides q'. We first note that $\mathcal{G}_2$ has a 3-dimensional vector linear solution over all finite fields. This is because, from Theorem 11 of Chapter 3 we know that $\mathcal{N}_3$ has a 3-dimensional vector linear solution over all finite fields, and from Lemma 25 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'. Now, from Lemma 29 we get that $\mathcal{G}_2$ 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. ■

4.1.4 Network $\mathcal{G}_3$

We now present the final network of this section: $\mathcal{G}_3$. This network is a conjunction of one $\mathcal{N}_3$, one Char-q_1-s network, one Char-q_1-y network, one Char-q_2-b network, and some additional edges. We show the network $\mathcal{G}_3$ in Fig. 4.6 for $q_1 = 2$ and $q_2 = 3$.

The source nodes of $\mathcal{N}_3$ are: $a, b, c, r, s, w, x, y, z$. Some of the nodes of $\mathcal{N}_3$ are labelled as $v_1, v_2, v_3, u_1, u_2, u_3, u_4$, and u_5. The message carried by the edges (v_i, u_i) and (v_i, u_j) for $i = 1, 2, 3$ and $j = 4, 5$ are denoted by Y_{ii} and Y_{ij} respectively. For $1 \leq i \leq 27$, the message carried by the edge (u_4, t_i) is denoted by $Z_{4,i}$, and the message carried by the edge (u_5, t_i) is denoted by $Z_{5,i}$.
Nodes $a, s, x_1, x_2, \ldots, x_{q_1+1}$ are source nodes of the Char-q_1-s network, nodes $a, y, x_1, x_2, ..., x_{q_1+1}$ are the source nodes of the Char-q_1-y network, and $a, b, x_1, x_2, \ldots, x_{q_2+1}$ are the source nodes of the Char-q_2-b network. Note that the source a is common between all four networks ($\mathcal{N}_3$, Char-q_1-s, Char-q_1-y, Char-q_2-b). In Section 4.1.1 where we described the Char-q-y network, the middle edges of the Char-q-y were labelled as: $e_1, e_2, \ldots, e_{q+3}$. Since we have three networks of the same class, we name the middle edges of the Char-q_1-s network as: $e^s_1, e^s_2, \ldots, e^s_{q_1+3}$; the middle edges of the Char-q_1-y network as: $e^y_1, e^y_2, \ldots, e^y_{q_1+3}$, and the middle edges of the Char-q_2-b network as: $e^b_1, e^b_2, \ldots, e^b_{q_2+3}$. The message carried by the edge e^j_i is denoted by $Y_{e^j_i}$ for $1 \leq i \leq q+3$, $j \in \{s, y, b\}$. Also note that the the tail node of e^s_1 has paths from only two sources: a and s, $tail(e^y_1)$ has paths from only a and y; and $tail(e^b_1)$ has paths from only a and b.

The additional edges not contained in $\mathcal{N}_3$, or Char-q_1-s, or Char-q_1-y, or Char-q_2-b, are listed below:

(i) (y, t_5), (y, t_{11}), (y, t_{17}), (y, t_{23}).

(ii) (z, t_9), (z, t_{18}), (z, t_{21}), (z, t_{24}), (z, t_{27}).

(iii) (s, t_{13}), (s, t_{15}).

(iv) (w, t_{25}), (w, t_{26}), (w, t_{27}).

We show that $\mathcal{G}_3$ has a scalar linear solution if and only if the characteristic of the finite field divides q_1, and has a 2-dimensional vector linear solution if and only if the characteristic of the finite field divides at least one of q_1 and q_2.

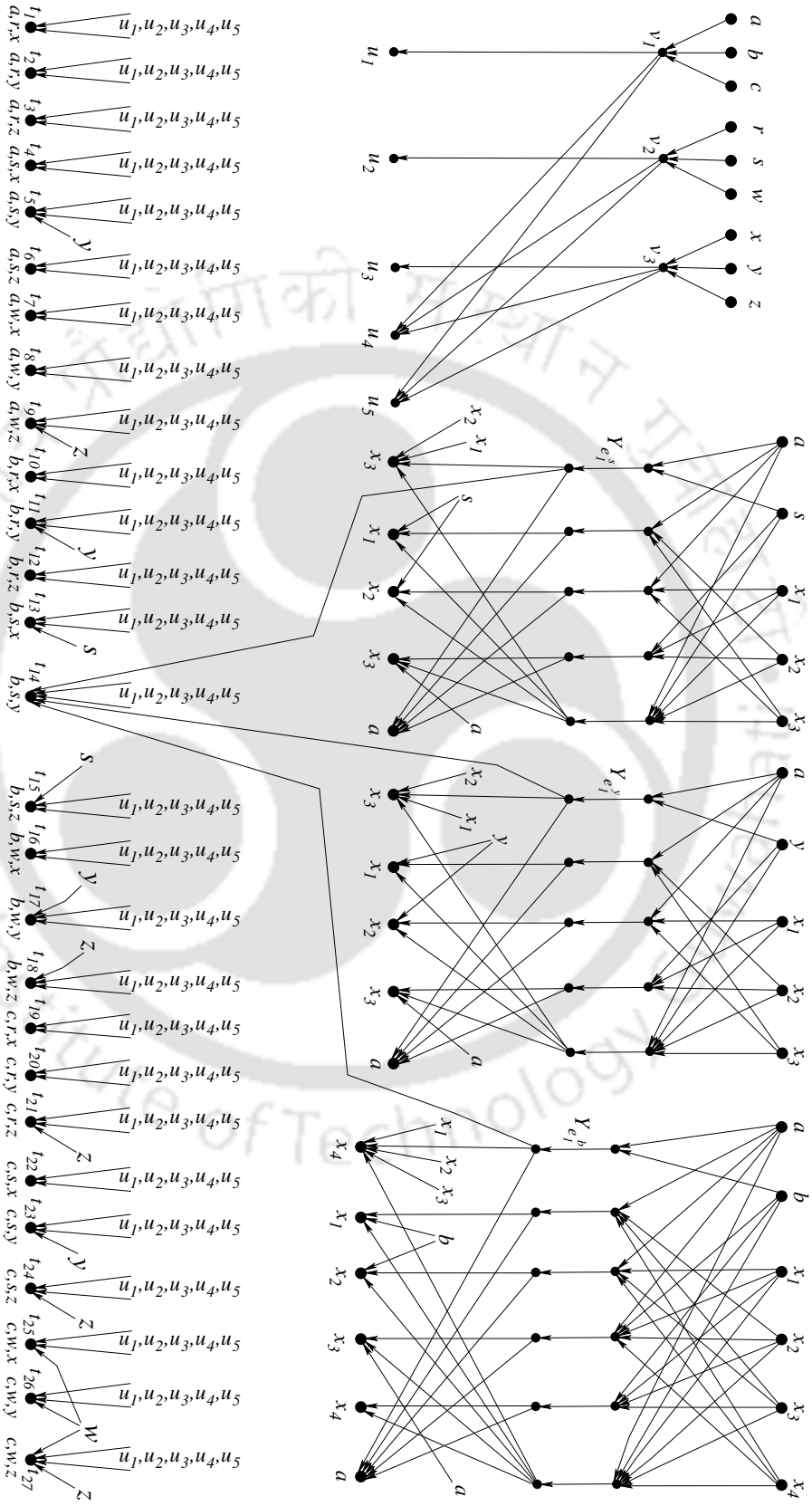

Figure 4.6: The network $\mathcal{G}_3$ for $q_1 = 2$ and $q_2 = 3$.

Let f be the function that maps the source nodes and the edges of $\mathcal{G}_3$ to the ground set of a discrete polymatroid $\mathbb{D}_3$ such that $\mathcal{G}_3$ is a discrete polymatroidal network associated with $\mathbb{D}_3$. Let ρ be the rank function of $\mathbb{D}_3$. Now let $\mathsf{g} = \rho \circ f$. As $\mathsf{g}()$ is a rank function of a discrete polymatroid, it obeys the rules given in Definition 4.

Lemma 31. *$\mathcal{G}_3$ has a scalar linear solution if and only if the characteristic of the finite field divides q_1.*

Proof: First we prove the 'only if' part. We show that if the characteristic of the finite field does not divide q_1, then $\mathcal{G}_3$ does not have a scalar linear solution. This is proved by contradiction. Assume that $\mathcal{G}_3$ have a scalar linear solution even when the characteristic of the finite field does not divide q_1. Using Lemma 5 we have:

$$\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, r) + \mathsf{g}(Y_{33}, x) = \mathsf{g}(Y_{11}, Y_{22}, Y_{33}, a, r, x). \tag{4.130}$$

Then,

$$\begin{aligned}
&\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, r) + \mathsf{g}(Y_{33}, x) \\
&= \mathsf{g}(Y_{11}, Y_{22}, Y_{33}, a, r, x) \\
&\leq \mathsf{g}(Y_{11}, Y_{22}, Y_{33}, a, r, x, Z_{4,1}, Z_{5,1}) \\
&= \mathsf{g}(Y_{11}, Y_{22}, Y_{33}, Z_{4,1}, Z_{5,1}) \qquad \text{[due to the demands of } t_1\text{]} \\
&\leq 5.
\end{aligned} \tag{4.131}$$

In equation 4.131 we have used the fact that for $\mathcal{N}_3$ to have a scalar linear solution, rank of any element of the ground set of $\mathbb{D}_3$ (with respect to which $\mathcal{G}_3$ is a discrete polymatroidal network) is less than or equal to 1 (see Definition 4).

Similarly we have:

$$\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, r) + \mathsf{g}(Y_{33}, y) \leq 5 \tag{4.132}$$

$$\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, r) + \mathsf{g}(Y_{33}, z) \leq 5 \tag{4.133}$$

$$\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, s) + \mathsf{g}(Y_{33}, x) \leq 5 \tag{4.134}$$

$$\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, s) + \mathsf{g}(Y_{33}, z) \leq 5 \tag{4.135}$$

$$\mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{22}, w) + \mathsf{g}(Y_{33}, x) \leq 5 \tag{4.136}$$

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, w) + \mathrm{g}(Y_{33}, y) \leq 5 \tag{4.137}$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, x) \leq 5 \tag{4.138}$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, z) \leq 5 \tag{4.139}$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, w) + \mathrm{g}(Y_{33}, x) \leq 5 \tag{4.140}$$

$$\mathrm{g}(Y_{11}, c) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, x) \leq 5 \tag{4.141}$$

$$\mathrm{g}(Y_{11}, c) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, y) \leq 5 \tag{4.142}$$

$$\mathrm{g}(Y_{11}, c) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, x) \leq 5. \tag{4.143}$$

We now show that $\mathrm{g}(Y_{ii}) = \mathrm{g}(Y_{ij}) = 1$ for $i = 1, 2, 3$ and $j = 4, 5$.

$$\begin{aligned}
9 &= \mathrm{g}(a, b, c, r, s, w, x, y, z) \\
&= \mathrm{g}(a, b, c, r, s, w, x, y, z, Y_{11}, Y_{14}, Y_{15}, Y_{22}, Y_{24}, Y_{25}, Y_{33}, Y_{34}, Y_{35}) \\
&= \mathrm{g}(Y_{11}, Y_{14}, Y_{15}, Y_{22}, Y_{24}, Y_{25}, Y_{33}, Y_{34}, Y_{35}) \\
&\leq \mathrm{g}(Y_{11}) + \mathrm{g}(Y_{14}) + \mathrm{g}(Y_{15}) + \mathrm{g}(Y_{22}) + \mathrm{g}(Y_{24}) + \mathrm{g}(Y_{25}) + \mathrm{g}(Y_{33}) + \mathrm{g}(Y_{34}) + \mathrm{g}(Y_{35}) \\
&\leq 9.
\end{aligned}$$

This indicates that

$$\mathrm{g}(Y_{11}) + \mathrm{g}(Y_{14}) + \mathrm{g}(Y_{15}) + \mathrm{g}(Y_{22}) + \mathrm{g}(Y_{24}) + \mathrm{g}(Y_{25}) + \mathrm{g}(Y_{33}) + \mathrm{g}(Y_{34}) + \mathrm{g}(Y_{35}) = 9. \tag{4.144}$$

Since the value of each of the terms in the left hand side of the above equation is less than or equal to 1, and since 9 of these terms must add up to 9, we must have

$$\mathrm{g}(Y_{ii}) = \mathrm{g}(Y_{ij}) = 1 \text{ for } i = 1, 2, 3 \text{ and } j = 4, 5. \tag{4.145}$$

Using the rule [P3] of Definition 4 we can show the following:

$$\begin{aligned}
&\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{11}, c) \\
&\geq \mathrm{g}(Y_{11}, a, b) + \mathrm{g}(Y_{11}) + \mathrm{g}(Y_{11}, c) \\
&\geq \mathrm{g}(Y_{11}, a, b, c) + 2\mathrm{g}(Y_{11}) \\
&= \mathrm{g}(a, b, c) + 2\mathrm{g}(Y_{11}) \\
&= 5 \qquad [Y_{11} = 1 \text{ from } (4.145)].
\end{aligned} \tag{4.146}$$

Similarly we have:

$$\mathrm{g}(Y_{11}, r) + \mathrm{g}(Y_{11}, s) + \mathrm{g}(Y_{11}, w) \geq 5 \tag{4.147}$$

$$\mathrm{g}(Y_{11}, x) + \mathrm{g}(Y_{11}, y) + \mathrm{g}(Y_{11}, z) \geq 5. \tag{4.148}$$

Adding equations (4.131), (4.132), and (4.133), we have:

$$3(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r)) + \mathrm{g}(Y_{33}, x) + \mathrm{g}(Y_{33}, y) + \mathrm{g}(Y_{33}, z) \leq 15$$

$$3(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r)) \leq 10 \qquad \text{[substituting from (4.148)]}$$

$$(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r) \leq 10/3. \tag{4.149}$$

Since rank of any element is less than or equal to 1 we have:

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, y) \leq 6. \tag{4.150}$$

From equations (4.134), (4.135), (4.150), and (4.148), we have:

$$3(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, s)) \leq 11. \tag{4.151}$$

Similarly from equations (4.136), (4.137), and (4.148), we have:

$$3(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, w)) \leq 11. \tag{4.152}$$

From equations (4.149), (4.151), and (4.152), we have:

$$3\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{22}, w) \leq 32/3. \tag{4.153}$$

Substituting equation (4.147), we have:

$$\mathrm{g}(Y_{11}, a) \leq 17/9. \tag{4.154}$$

As the value of a rank function is always an integer, we have $\mathrm{g}(Y_{11}, a) \leq 1$. As $\mathrm{g}(Y_{11}, a) \geq \mathrm{g}(a)$, we must have:

$$\mathrm{g}(Y_{11}, a) = 1. \tag{4.155}$$

Similarly it can be shown

$$\mathrm{g}(Y_{22}, r) = 1 \tag{4.156}$$

$$\mathrm{g}(Y_{33}, x) = 1. \tag{4.157}$$

Then, we have the following equations.

$$\mathrm{g}(Y_{11}|a) = \mathrm{g}(Y_{11}, a) - \mathrm{g}(a) = 1 - 1 = 0 \qquad \text{[see Sec. 2.5 for notation meaning]} \tag{4.158}$$

$$\mathrm{g}(Y_{22}|r) = \mathrm{g}(Y_{22}, r) - \mathrm{g}(r) = 1 - 1 = 0 \tag{4.159}$$

$$\mathrm{g}(Y_{33}|x) = \mathrm{g}(Y_{33}, x) - \mathrm{g}(x) = 1 - 1 = 0. \tag{4.160}$$

We also have:

$$\mathrm{g}(a|Y_{11}) = \mathrm{g}(a, Y_{11}) - \mathrm{g}(Y_{11}) = 1 - 1 = 0 \tag{4.161}$$

$$\mathrm{g}(r|Y_{22}) = \mathrm{g}(r, Y_{22}) - \mathrm{g}(Y_{22}) = 1 - 1 = 0 \tag{4.162}$$

$$\mathrm{g}(x|Y_{33}) = \mathrm{g}(x, Y_{33}) - \mathrm{g}(Y_{33}) = 1 - 1 = 0. \tag{4.163}$$

Case I: The characteristic of the finite field neither divides q_1 nor q_2.

Hence, the components of b,q, and y in $Y_{e_1^s}, Y_{e_1^y}$, and $Y_{e_1^b}$ respectively is zero; and, $Y_{e_1^s}, Y_{e_1^y}$, and $Y_{e_1^b}$ are functions of only a (this is due to Lemma 25).

Then,

$$\begin{aligned}
&5 \geq \mathrm{g}(a, r, x, Z_{4,14}, Z_{5,14}) \\
&= \mathrm{g}(a, r, x, Z_{4,14}, Z_{5,14}) + \mathrm{g}(Y_{11}|a) + \mathrm{g}(Y_{22}|r) + \mathrm{g}(Y_{33}|x) \qquad \text{[from (4.158), (4.159), and (4.160)]} \\
&\geq \mathrm{g}(a, r, x, Z_{4,14}, Z_{5,14}) + \mathrm{g}(Y_{11}|a, r, x, Z_{4,14}, Z_{5,14}) + \mathrm{g}(Y_{22}|a, r, x, Y_{11}, Z_{4,14}, Z_{5,14}) \\
&\qquad\qquad + \mathrm{g}(Y_{33}|a, r, x, Y_{11}, Y_{22}, Z_{4,14}, Z_{5,14}) \\
&= \mathrm{g}(a, r, x, Y_{11}, Y_{22}, Y_{33}, Z_{4,14}, Z_{5,14}) \\
&= \mathrm{g}(a, r, x, Y_{e_1^s}, Y_{e_1^y}, Y_{e_1^b}, Y_{11}, Y_{22}, Y_{33}, Z_{4,14}, Z_{5,14}) \qquad \text{[as } Y_{e_1^s}, Y_{e_1^y}, \text{ and } Y_{e_1^b} \text{ are functions of } a\text{]} \\
&= \mathrm{g}(a, r, x, Y_{e_1^s}, Y_{e_1^y}, Y_{e_1^b}, Y_{11}, Y_{22}, Y_{33}, Z_{4,14}, Z_{5,14}, b, s, y) \qquad \text{[due to the demands of } t_{14}\text{]} \\
&\geq \mathrm{g}(a, r, x, b, s, y) = 6.
\end{aligned}$$

which is a contradiction, and hence $\mathcal{G}_3$ does not have a scalar linear solution over such a finite field.

Case II: The characteristic of the finite field divides q_2 but it does not divide q_1.

Over such a finite field the component of b in $Y_{e_1^b}$ from Char-q_2-b network may be non-zero, but the components of s and y in $Y_{e_1^s}$ and $Y_{e_1^y}$ respectively is zero. Since **Case I** already handles the case

if the component of b in $Y_{e_1^b}$ is zero, we assume that the component of b in $Y_{e_1^b}$ is non-zero. We have:

$$\begin{aligned}
&\mathrm{g}(Y_{22}, Y_{24}) + 1 \\
&= \mathrm{g}(Y_{22}, Y_{24}) + \mathrm{g}(Y_{25}) \qquad \text{[from equation (4.145)]} \\
&\geq \mathrm{g}(Y_{22}, Y_{24}, Y_{25}) \\
&= \mathrm{g}(Y_{22}, Y_{24}, Y_{25}, r, s, w) \\
&= \mathrm{g}(r, s, w) + \mathrm{g}(Y_{22}, Y_{24}, Y_{25} | r, s, w) = 3.
\end{aligned}$$

Then we have, $\mathrm{g}(Y_{22}, Y_{24}) \geq 2$. But as rank of any element is less than or equal to 1 (for a scalar solution to exist), we have: $\mathrm{g}(Y_{22}, Y_{24}) \leq 2$. So we must have:

$$\mathrm{g}(Y_{22}, Y_{24}) = 2. \tag{4.164}$$

Similarly we have:

$$\mathrm{g}(Y_{11}, Y_{14}) = 2 \tag{4.165}$$

$$\mathrm{g}(Y_{33}, Y_{34}) = 2. \tag{4.166}$$

Since $\mathrm{g}(Y_{11}, Y_{14}, b) \geq \mathrm{g}(Y_{11}, Y_{14})$ and $\mathrm{g}(Y_{11}, Y_{14}, b) \leq 3$, $\mathrm{g}(Y_{11}, Y_{14}, b)$ is either equal to 2 or 3.

Case IIa: $\mathrm{g}(Y_{11}, Y_{14}, b) = 3$.

At terminal t_{16} we have:

$$\begin{aligned}
&\mathrm{g}(Y_{11}, Y_{14}, b) + \mathrm{g}(Y_{22}, Y_{24}, w) + \mathrm{g}(Y_{33}, Y_{34}, x) \\
&= \mathrm{g}(Y_{11}, Y_{14}, b, Y_{22}, Y_{24}, w, Y_{33}, Y_{34}, x) \qquad \text{[reasoning is similar to equation (4.130)]} \\
&= \mathrm{g}(Y_{11}, Y_{14}, b, Y_{22}, Y_{24}, w, Y_{33}, Y_{34}, x, Z_{4,16}) \\
&\leq \mathrm{g}(Y_{11}, Y_{14}, b, Y_{22}, Y_{24}, w, Y_{33}, Y_{34}, x, Z_{4,16}, Z_{5,16}) \\
&= \mathrm{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, Z_{4,16}, Z_{5,16}) \qquad \text{[due to the demands of } t_{16}\text{]} \\
&= \mathrm{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, Z_{5,16}) \\
&\leq 7.
\end{aligned} \tag{4.167}$$

Similarly we have:

$$\mathrm{g}(Y_{11}, Y_{15}, b) + \mathrm{g}(Y_{22}, Y_{25}, w) + \mathrm{g}(Y_{33}, Y_{35}, x) \leq 7. \tag{4.168}$$

From equation (4.155), we have:

$$\begin{aligned}
&\mathsf{g}(Y_{33}, Y_{34}, x) && (4.169)\\
&= \mathsf{g}(Y_{33}, x) + \mathsf{g}(Y_{34}|Y_{33}, x) && (4.170)\\
&= 1 + \mathsf{g}(Y_{34}|Y_{33}, x) \qquad \text{[from equation (4.157)]} && (4.171)\\
&\leq 2. && (4.172)
\end{aligned}$$

We also have:

$$\mathsf{g}(Y_{33}, Y_{34}, x) = \mathsf{g}(Y_{33}, Y_{34}) + \mathsf{g}(x|Y_{33}, Y_{34}) \geq 2. \tag{4.173}$$

From equations (4.173) and (4.172), we have:

$$\mathsf{g}(Y_{33}, Y_{34}, x) = 2. \tag{4.174}$$

Substituting equation (4.174) in equation (4.167) we have:

$$\mathsf{g}(Y_{11}, Y_{14}, b) + \mathsf{g}(Y_{22}, Y_{24}, w) \leq 5. \tag{4.175}$$

Since by assumption of the case condition $\mathsf{g}(Y_{11}, Y_{14}, b) = 3$, we have:

$$\mathsf{g}(Y_{22}, Y_{24}, w) \leq 2. \tag{4.176}$$

We now have:

$$\begin{aligned}
&\mathsf{g}(Y_{22}, Y_{24}, s) + \mathsf{g}(Y_{22}, Y_{24}, w)\\
&\geq \mathsf{g}(Y_{22}, Y_{24}, s, w) + \mathsf{g}(Y_{22}, Y_{24}) \qquad \text{[using rule [P3] of Def. 4]}\\
&\geq \mathsf{g}(Y_{22}, Y_{24}, s, w) + \mathsf{g}(r|Y_{22}) + \mathsf{g}(Y_{22}, Y_{24}) \qquad \text{[using equation (4.162)]}\\
&\geq \mathsf{g}(Y_{22}, Y_{24}, s, w) + \mathsf{g}(r|Y_{22}, Y_{24}, s, w) + \mathsf{g}(Y_{22}, Y_{24})\\
&= \mathsf{g}(Y_{22}, Y_{24}, s, r, w) + \mathsf{g}(Y_{22}, Y_{24})\\
&\geq 3 + 2 = 5 \qquad \text{[using equation (4.164)].} && (4.177)
\end{aligned}$$

Substituting equation (4.176) in equation (4.177), we get:

$$\mathsf{g}(Y_{22}, Y_{24}, s) \geq 3. \tag{4.178}$$

Then we must have:

$$\mathsf{g}(Y_{22}, Y_{24}, s) = 3. \tag{4.179}$$

Now, due to the demands of terminal t_{14}, we have:

$$\begin{aligned}
&\mathsf{g}(Y_{11}, Y_{14}, b) + \mathsf{g}(Y_{22}, Y_{24}, s) + \mathsf{g}(Y_{33}, Y_{34}, y) \\
&= \mathsf{g}(Y_{11}, Y_{14}, b, Y_{22}, Y_{24}, s, Y_{33}, Y_{34}, y) \\
&= \mathsf{g}(Y_{11}, Y_{14}, b, Y_{22}, Y_{24}, s, Y_{33}, Y_{34}, y, Z_{4,14}) \\
&\geq \mathsf{g}(Y_{11}, Y_{14}, b, Y_{22}, Y_{24}, s, Y_{33}, Y_{34}, y, Z_{4,14}, Z_{5,14}, a) \\
&= \mathsf{g}(Y_{11}, Y_{14}, b, Y_{22}, Y_{24}, s, Y_{33}, Y_{34}, y, Z_{4,14}, Z_{5,14}, a, Y_{e_1^s}, Y_{e_1^y}, Y_{e_1^b}) \\
&= \mathsf{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, Z_{4,14}, Z_{5,14}, a, Y_{e_1^s}, Y_{e_1^y}, Y_{e_1^b}) \\
&= \mathsf{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, Z_{5,14}, a, Y_{e_1^b}) \\
&\leq \mathsf{g}(Y_{11}, a) + \mathsf{g}(Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, Z_{5,14}, Y_{e_1^b}) \\
&\leq 1 + 7 = 8 \qquad \text{[using equation (4.155)].}
\end{aligned} \tag{4.180}$$

Substituting equation (4.179) and noting that $\mathsf{g}(Y_{11}, Y_{14}, b) = 3$ as per the case condition, from equation (4.180), we have:

$$\mathsf{g}(Y_{33}, Y_{34}, y) \leq 2. \tag{4.181}$$

Now, due to the demands of terminal t_{15}, we have:

$$\begin{aligned}
&\mathsf{g}(Y_{11}, Y_{14}, b) + \mathsf{g}(Y_{22}, Y_{24}, s) + \mathsf{g}(Y_{33}, Y_{34}, z) \\
&= \mathsf{g}(Y_{11}, Y_{14}, b, Y_{22}, Y_{24}, s, Y_{33}, Y_{34}, z) \\
&= \mathsf{g}(Y_{11}, Y_{14}, b, Y_{22}, Y_{24}, s, Y_{33}, Y_{34}, z, Z_{4,15}) \\
&\geq \mathsf{g}(Y_{11}, Y_{14}, b, Y_{22}, Y_{24}, s, Y_{33}, Y_{34}, z, Z_{4,15}, Z_{5,15}) \\
&= \mathsf{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, z, Z_{4,15}, Z_{5,15}) \\
&= \mathsf{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, z, Z_{5,15}) \\
&\leq 8.
\end{aligned} \tag{4.182}$$

Substituting equation (4.179) and noting that $\mathsf{g}(Y_{11}, Y_{14}, b) = 3$ as per the case condition, from equation (4.182), we have:

$$\mathsf{g}(Y_{33}, Y_{34}, z) \leq 2. \tag{4.183}$$

We now have:

$$\begin{aligned}
&\mathsf{g}(Y_{33}, Y_{34}, x) + \mathsf{g}(Y_{33}, Y_{34}, y) + \mathsf{g}(Y_{33}, Y_{34}, z) \\
&\geq \mathsf{g}(Y_{33}, Y_{34}, x, y) + \mathsf{g}(Y_{33}, Y_{34}) + \mathsf{g}(Y_{33}, Y_{34}, z) \\
&\geq \mathsf{g}(Y_{33}, Y_{34}, x, y, z) + 2\mathsf{g}(Y_{33}, Y_{34}) \\
&= 3 + 4 = 7. \qquad \text{[from equation (4.166)]}
\end{aligned} \tag{4.184}$$

However, substituting equations (4.174), (4.181), and (4.183) in equation (4.184), we have: $6 \geq 7$, which is a contradiction.

Case IIb: $\mathsf{g}(Y_{11}, Y_{14}, b) = 2$.

We have:

$$\begin{aligned}
&\mathsf{g}(Y_{11}, Y_{14}, b) + \mathsf{g}(Y_{11}, Y_{15}, b) \\
&\geq \mathsf{g}(Y_{11}, Y_{14}, Y_{15}, b) + \mathsf{g}(Y_{11}, b) \\
&= 3 + \mathsf{g}(Y_{11}, b) + \mathsf{g}(a|Y_{11}) \qquad \text{[using equations (4.145) and (4.161)]} \\
&\geq 3 + \mathsf{g}(Y_{11}, b) + \mathsf{g}(a|Y_{11}, b) \\
&= 3 + \mathsf{g}(Y_{11}, a, b) \\
&= 3 + \mathsf{g}(a, b) + \mathsf{g}(Y_{11}|a, b) \\
&\geq 5.
\end{aligned} \tag{4.185}$$

Substituting the case condition $\mathsf{g}(Y_{11}, Y_{14}, b) = 2$ in equation (4.185), we get:

$$\mathsf{g}(Y_{11}, Y_{15}, b) \geq 3. \tag{4.186}$$

We also know that $\mathsf{g}(Y_{11}, Y_{15}, b) \leq 3$. So we must have:

$$\mathsf{g}(Y_{11}, Y_{15}, b) = 3. \tag{4.187}$$

Note that equation (4.187) is very similar to the case condition of **Case IIa**. Like equation (4.174) it can be shown that

$$\mathsf{g}(Y_{33}, Y_{35}, x) = 2. \tag{4.188}$$

Substituting equation (4.188) and equation (4.187) in equation (4.168), which holds in this case as

well, we get:

$$\mathrm{g}(Y_{22}, Y_{25}, w) \leq 2. \tag{4.189}$$

Similar to equation (4.177) the following can be shown:

$$\mathrm{g}(Y_{22}, Y_{25}, s) + \mathrm{g}(Y_{22}, Y_{25}, w) \geq 5. \tag{4.190}$$

Using the fact that $\mathrm{g}(Y_{22}, Y_{25}, w) \leq 2$ (from (4.189)), from equation (4.190), we have:

$$\mathrm{g}(Y_{22}, Y_{25}, s) = 3. \tag{4.191}$$

Similar to equation (4.180), we get:

$$\mathrm{g}(Y_{11}, Y_{15}, b) + \mathrm{g}(Y_{22}, Y_{25}, s) + \mathrm{g}(Y_{33}, Y_{35}, y) \leq 8. \tag{4.192}$$

Substitution equations (4.191) and (4.187) in equation (4.192), we get:

$$\mathrm{g}(Y_{33}, Y_{35}, y) \leq 2. \tag{4.193}$$

Similar to equation (4.182), we have:

$$\mathrm{g}(Y_{11}, Y_{15}, b) + \mathrm{g}(Y_{22}, Y_{25}, s) + \mathrm{g}(Y_{33}, Y_{35}, z) \leq 8. \tag{4.194}$$

Substituting equations (4.191) and (4.187) in equation (4.194), we have:

$$\mathrm{g}(Y_{33}, Y_{35}, z) \leq 2. \tag{4.195}$$

Similar to equation (4.184) we also have:

$$\mathrm{g}(Y_{33}, Y_{35}, x) + \mathrm{g}(Y_{33}, Y_{35}, y) + \mathrm{g}(Y_{33}, Y_{35}, z) \geq 7. \tag{4.196}$$

However, substituting equations (4.188), (4.193) and (4.195) in equation (4.196), we have: $6 \leq 7$, which is a contradiction.

We no consider the 'if' part. We show that there is a scalar linear solution if the characteristic of the finite field divides q_1. The solution when $q_1 = 2$ is shown in Fig 4.7. The solution can be easily extended to all values of q_1.

■

Lemma 32. *$\mathcal{G}_3$ has a 2-dimensional vector linear solution if and only if the characteristic of the finite*

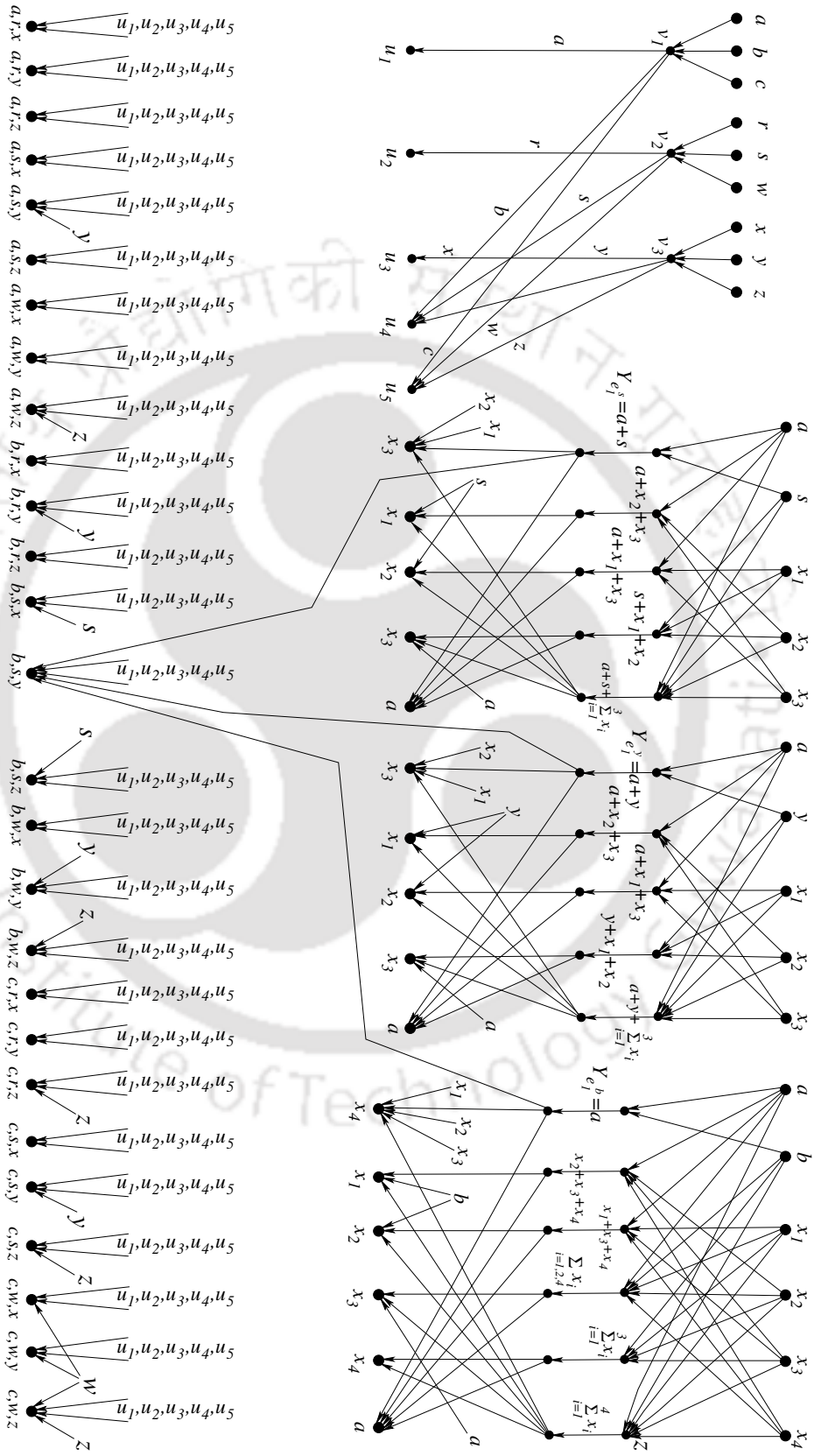

Figure 4.7: A scalar linear solution of $\mathcal{G}_3$ for $q_1 = 2$ and $q_2 = 3$ when the characteristic divides q_1.

field divides q_1 *or* q_2.

Proof: Consider the 'only if' part. We show that if the characteristic of the finite field divides neither of q_1 or q_2 then there exists no 2-dimensional vector linear solution of $\mathcal{G}_3$. Assume otherwise. Note that in such a case $Y_{e_1^b}, Y_{e_1^s}$ and $Y_{e_1^y}$ are not a function of b, s, and y respectively (Lemma 25). Also note that rank of any element is less than or equal to 2 (for the network to have a 2-dimensional vector linear solution). We have:

$$\begin{aligned}
&\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, x) \\
&= \mathrm{g}(Y_{11}, Y_{22}, Y_{33}, a, r, x) \qquad \text{[using Lemma 5 repetitively]} \\
&\leq \mathrm{g}(Y_{11}, Y_{22}, Y_{33}, a, r, x, Z_{4,1}, Z_{5,1}) \\
&= \mathrm{g}(Y_{11}, Y_{22}, Y_{33}, Z_{4,1}, Z_{5,1}) \\
&\leq 10. \qquad (4.197)
\end{aligned}$$

Similarly we have:

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, y) \leq 10 \qquad (4.198)$$

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, z) \leq 10 \qquad (4.199)$$

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, x) \leq 10 \qquad (4.200)$$

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, z) \leq 10 \qquad (4.201)$$

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, w) + \mathrm{g}(Y_{33}, x) \leq 10 \qquad (4.202)$$

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, w) + \mathrm{g}(Y_{33}, y) \leq 10 \qquad (4.203)$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, x) \leq 10 \qquad (4.204)$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, z) \leq 10 \qquad (4.205)$$

$$\mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{22}, w) + \mathrm{g}(Y_{33}, x) \leq 10 \qquad (4.206)$$

$$\mathrm{g}(Y_{11}, c) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, x) \leq 10 \qquad (4.207)$$

$$\mathrm{g}(Y_{11}, c) + \mathrm{g}(Y_{22}, r) + \mathrm{g}(Y_{33}, y) \leq 10 \qquad (4.208)$$

$$\mathrm{g}(Y_{11}, c) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, x) \leq 10. \qquad (4.209)$$

Proceeding similarly to how equation (4.145) was obtained in the previous Lemma, it can be show

that

$$\mathrm{g}(Y_{ii}) = \mathrm{g}(Y_{ij}) = 2 \text{ for } i = 1, 2, 3 \text{ and } j = 4, 5. \tag{4.210}$$

In the same way equation (4.146) was proved, the following equations can be proved:

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{11}, b) + \mathrm{g}(Y_{11}, c) \geq 10 \tag{4.211}$$

$$\mathrm{g}(Y_{11}, r) + \mathrm{g}(Y_{11}, s) + \mathrm{g}(Y_{11}, w) \geq 10 \tag{4.212}$$

$$\mathrm{g}(Y_{11}, x) + \mathrm{g}(Y_{11}, y) + \mathrm{g}(Y_{11}, z) \geq 10. \tag{4.213}$$

Adding equations (4.197), (4.198), and (4.199), we have:

$$3(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r)) + \mathrm{g}(Y_{33}, x) + \mathrm{g}(Y_{33}, y) + \mathrm{g}(Y_{33}, z) \leq 30$$

$$3(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r)) \leq 20 \qquad \text{[from equation (4.211)]}$$

$$(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, r) \leq 20/3. \tag{4.214}$$

Since rank of each element is less than or equal to 2, we have

$$\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, s) + \mathrm{g}(Y_{33}, y) \leq 12. \tag{4.215}$$

From equations (4.200), (4.201), (4.215), and (4.211), we have:

$$3(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, s)) \leq 22. \tag{4.216}$$

Similarly we have:

$$3(\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, w)) \leq 22. \tag{4.217}$$

From equations (4.214), (4.216), and (4.217), we have:

$$3\mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{11}, r) + \mathrm{g}(Y_{11}, s) + \mathrm{g}(Y_{11}, w) \leq 64/3. \tag{4.218}$$

Substituting equation (4.212), we have:

$$\mathrm{g}(Y_{11}, a) \leq 34/9. \tag{4.219}$$

As the output of a rank function is always an integer, the rank of $\mathrm{g}(Y_{11}, a)$ must be either 1, 2, or 3. However, as $\mathrm{g}(a) = 2$, $\mathrm{g}(Y_{11}, a)$ is either equal to 2 or 3. Similarly it can be shown that either $\mathrm{g}(Y_{22}, r) = 2$ or $\mathrm{g}(Y_{22}, r) = 3$; and either $\mathrm{g}(Y_{33}, x) = 2$ or $\mathrm{g}(Y_{33}, x) = 3$.

We will now consider many several cases that may arise. In Fig. 4.8 we present these cases for the purpose of easy following.

Case I: $\mathsf{g}(Y_{11}, a) = 3$.

From equation (4.211), we get the following possibilities: $\mathsf{g}(Y_{11}, b) = 3$ and $\mathsf{g}(Y_{11}, c) = 4$; $\mathsf{g}(Y_{11}, b) = 4$ and $\mathsf{g}(Y_{11}, c) = 3$; $\mathsf{g}(Y_{11}, b) = 4$ and $\mathsf{g}(Y_{11}, c) = 4$.

Case I.1: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 3$, $\mathsf{g}(Y_{11}, c) = 4$.

Case I.1.1: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 3$, $\mathsf{g}(Y_{11}, c) = 4$, $\mathsf{g}(Y_{22}, r) = 3$.

From equation (4.212), we get the following possibilities: $\mathsf{g}(Y_{22}, s) = 3$ and $\mathsf{g}(Y_{22}, w) = 4$; $\mathsf{g}(Y_{22}, s) = 4$ and $\mathsf{g}(Y_{22}, w) = 3$; $\mathsf{g}(Y_{22}, s) = 4$ and $\mathsf{g}(Y_{22}, w) = 4$.

Case I.1.1.1: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 3$, $\mathsf{g}(Y_{11}, c) = 4$, $\mathsf{g}(Y_{22}, r) = 3$, $\mathsf{g}(Y_{22}, s) = 3$, $\mathsf{g}(Y_{22}, w) = 4$.

Substituting the values set by the case condition in equation (4.203), we get $\mathsf{g}(Y_{33}, y) \leq 3$. Now as equation (4.213) holds, it must be that $\mathsf{g}(Y_{33}, x) = 3$, $\mathsf{g}(Y_{33}, y) = 3$, and $\mathsf{g}(Y_{33}, z) = 4$.

We then have:

$$\begin{aligned}\mathsf{g}(Y_{33}, Y_{34}, x) &= \mathsf{g}(Y_{33}, x) + \mathsf{g}(Y_{34}|Y_{33}, x) \\ &= 3 + \mathsf{g}(Y_{34}|Y_{33}, x) \leq 5. \end{aligned} \tag{4.220}$$

Similarly we can show the following equations.

$$\mathsf{g}(Y_{11}, Y_{14}, a) \leq 5 \tag{4.221}$$

$$\mathsf{g}(Y_{11}, Y_{15}, a) \leq 5 \tag{4.222}$$

$$\mathsf{g}(Y_{11}, Y_{14}, b) \leq 5 \tag{4.223}$$

$$\mathsf{g}(Y_{11}, Y_{15}, b) \leq 5 \tag{4.224}$$

$$\mathsf{g}(Y_{22}, Y_{24}, r) \leq 5 \tag{4.225}$$

$$\mathsf{g}(Y_{22}, Y_{25}, r) \leq 5 \tag{4.226}$$

$$\mathsf{g}(Y_{22}, Y_{24}, s) \leq 5 \tag{4.227}$$

$$\mathsf{g}(Y_{22}, Y_{25}, s) \leq 5 \tag{4.228}$$

$$\mathsf{g}(Y_{33}, Y_{35}, x) \leq 5 \tag{4.229}$$

$$\mathsf{g}(Y_{33}, Y_{34}, y) \leq 5 \tag{4.230}$$

$$\mathsf{g}(Y_{33}, Y_{35}, y) \leq 5. \tag{4.231}$$

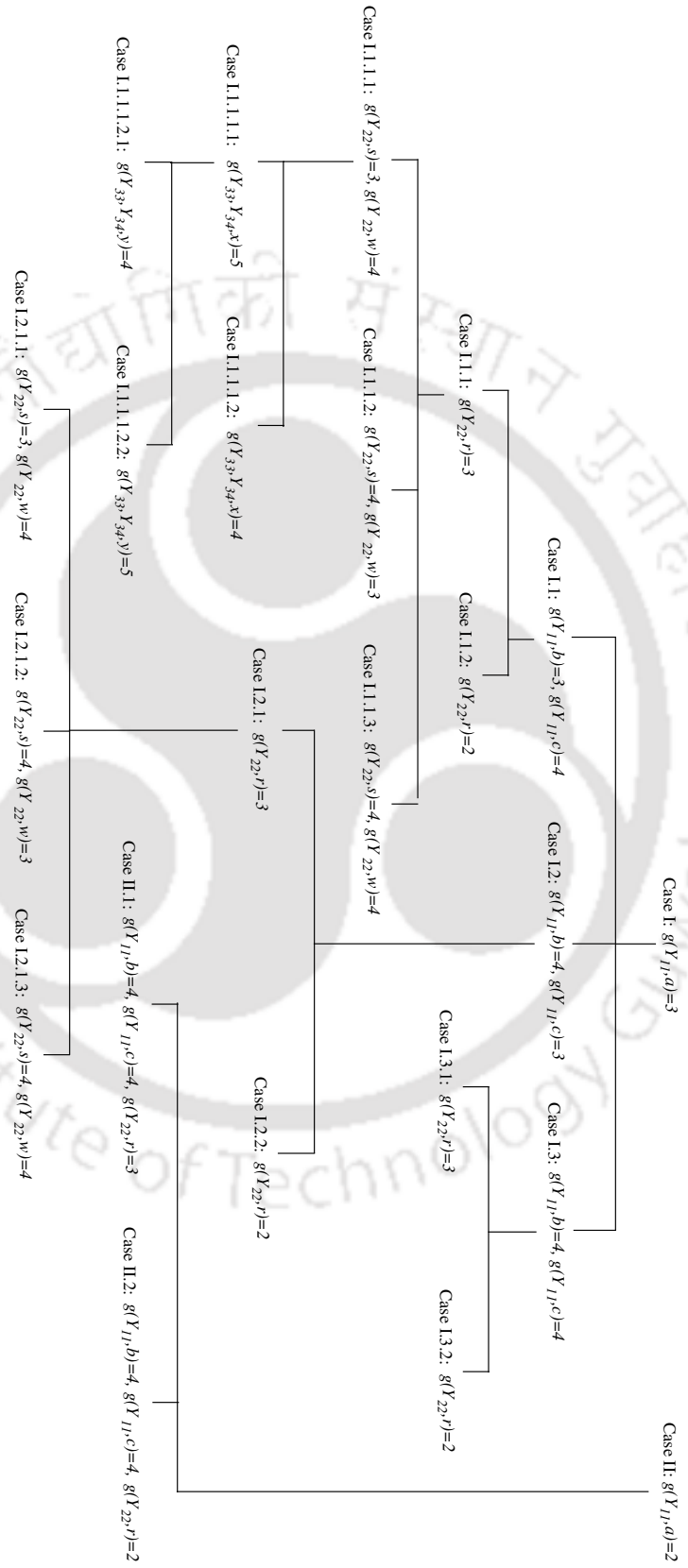

Figure 4.8: The case divisions in the proof of Lemma 32.

We also have the following:

$$\begin{aligned}
&\mathsf{g}(Y_{11}, Y_{14}, a) + \mathsf{g}(Y_{11}, Y_{14}, b) + \mathsf{g}(Y_{11}, Y_{14}, c) \\
&\geq \mathsf{g}(Y_{11}, Y_{14}, a, b) + \mathsf{g}(Y_{11}, Y_{14}) + \mathsf{g}(Y_{11}, Y_{14}, c) \\
&\geq \mathsf{g}(Y_{11}, Y_{14}, a, b, c) + 2\mathsf{g}(Y_{11}, Y_{14}) \\
&\geq 6 + 8 = 14. \qquad \text{[from equation (4.210)]}
\end{aligned}$$

Similarly it can be shown that:

$$\mathsf{g}(Y_{11}, Y_{15}, a) + \mathsf{g}(Y_{11}, Y_{15}, b) + \mathsf{g}(Y_{11}, Y_{15}, c) \geq 14 \tag{4.232}$$

$$\mathsf{g}(Y_{22}, Y_{24}, r) + \mathsf{g}(Y_{22}, Y_{24}, s) + \mathsf{g}(Y_{22}, Y_{24}, w) \geq 14 \tag{4.233}$$

$$\mathsf{g}(Y_{22}, Y_{25}, r) + \mathsf{g}(Y_{22}, Y_{25}, s) + \mathsf{g}(Y_{22}, Y_{25}, w) \geq 14 \tag{4.234}$$

$$\mathsf{g}(Y_{33}, Y_{34}, x) + \mathsf{g}(Y_{33}, Y_{34}, y) + \mathsf{g}(Y_{33}, Y_{34}, z) \geq 14 \tag{4.235}$$

$$\mathsf{g}(Y_{33}, Y_{35}, x) + \mathsf{g}(Y_{33}, Y_{35}, y) + \mathsf{g}(Y_{33}, Y_{35}, z) \geq 14. \tag{4.236}$$

Similar to equation (4.166) it can be shown that $\mathsf{g}(Y_{33}, Y_{34}) = 4$. Then because of equation (4.220) and that $\mathsf{g}(Y_{33}, Y_{34}, x) \geq \mathsf{g}(Y_{33}, Y_{34})$, we have either $\mathsf{g}(Y_{33}, Y_{34}, x) = 4$ or $\mathsf{g}(Y_{33}, Y_{34}, x) = 5$.

Case I.1.1.1.1: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 3$, $\mathsf{g}(Y_{11}, c) = 4$, $\mathsf{g}(Y_{22}, r) = 3$, $\mathsf{g}(Y_{22}, s) = 3$, $\mathsf{g}(Y_{22}, w) = 4$, $\mathsf{g}(Y_{33}, Y_{34}, x) = 5$.

Due to the demands of terminal t_1, we have:

$$\begin{aligned}
&\mathsf{g}(Y_{11}, Y_{14}, a) + \mathsf{g}(Y_{22}, Y_{24}, r) + \mathsf{g}(Y_{33}, Y_{34}, x) \\
&= \mathsf{g}(Y_{11}, Y_{14}, a, Y_{22}, Y_{24}, r, Y_{33}, Y_{34}, x) \qquad \text{[reasoning is similar to equation (4.130)]} \\
&= \mathsf{g}(Y_{11}, Y_{14}, a, Y_{22}, Y_{24}, r, Y_{33}, Y_{34}, x, Z_{4,1}) \\
&\leq \mathsf{g}(Y_{11}, Y_{14}, a, Y_{22}, Y_{24}, r, Y_{33}, Y_{34}, x, Z_{4,1}, Z_{5,1}) \\
&= \mathsf{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, Z_{4,1}, Z_{5,1}) \\
&= \mathsf{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, Z_{5,1}) \\
&\leq 14.
\end{aligned} \tag{4.237}$$

Similarly, due to the demands of terminals t_4 and t_7 respectively the following equations can be

determined.

$$\mathsf{g}(Y_{11}, Y_{14}, a) + \mathsf{g}(Y_{22}, Y_{24}, s) + \mathsf{g}(Y_{33}, Y_{34}, x) \leq 14 \tag{4.238}$$

$$\mathsf{g}(Y_{11}, Y_{14}, a) + \mathsf{g}(Y_{22}, Y_{24}, w) + \mathsf{g}(Y_{33}, Y_{34}, x) \leq 14. \tag{4.239}$$

Adding equations (4.237), (4.238), and (4.239), we have:

$$3\mathsf{g}(Y_{11}, Y_{14}, a) + \mathsf{g}(Y_{22}, Y_{24}, r) + \mathsf{g}(Y_{22}, Y_{24}, s) + \mathsf{g}(Y_{22}, Y_{24}, w) + 3\mathsf{g}(Y_{33}, Y_{34}, x) \leq 42. \tag{4.240}$$

Substituting the case condition and equation (4.233) in equation (4.240), we have:

$$\mathsf{g}(Y_{11}, Y_{14}, a) \leq 13/3. \tag{4.241}$$

Since the rank function is always an integer, and that $\mathsf{g}(Y_{11}, Y_{14}) = 4$ (the latter can be proved similarly to equation (4.165)), we have:

$$\mathsf{g}(Y_{11}, Y_{14}, a) = 4. \tag{4.242}$$

We now have:

$$\begin{aligned} &\mathsf{g}(Y_{11}, Y_{14}, a) + \mathsf{g}(Y_{11}, Y_{15}, a) \\ &\geq \mathsf{g}(Y_{11}, Y_{14}, Y_{15}, a) + \mathsf{g}(Y_{11}, a). \end{aligned} \tag{4.243}$$

We also have:

$$\begin{aligned} 6 &= \mathsf{g}(a, b, c) \\ &\leq \mathsf{g}(a, b, c, Y_{11}, Y_{14}, Y_{15}) \\ &= \mathsf{g}(Y_{11}, Y_{14}, Y_{15}) \\ &\leq \mathsf{g}(Y_{11}) + \mathsf{g}(Y_{14}) + \mathsf{g}(Y_{15}) \\ &\leq 6. \end{aligned} \tag{4.244}$$

Equation (4.244) indicates that

$$\mathsf{g}(Y_{11}, Y_{14}, Y_{15}) = \mathsf{g}(Y_{11}) + \mathsf{g}(Y_{14}) + \mathsf{g}(Y_{15}) = 6. \tag{4.245}$$

Substituting equation (4.245) and the case condition $\mathsf{g}(Y_{11}, a) = 3$ in equation (4.243), we have:

$$\mathsf{g}(Y_{11}, Y_{14}, a) + \mathsf{g}(Y_{11}, Y_{15}, a) \geq 9. \tag{4.246}$$

Substituting equation (4.242) in equation (4.246), we get

$$\mathsf{g}(Y_{11}, Y_{15}, a) \geq 5. \tag{4.247}$$

As equation (4.222) holds, we have:

$$\mathsf{g}(Y_{11}, Y_{15}, a) = 5. \tag{4.248}$$

Similarly to equation (4.237), due to terminals t_{10} and t_{19}, we have:

$$\mathsf{g}(Y_{11}, Y_{14}, b) + \mathsf{g}(Y_{22}, Y_{24}, r) + \mathsf{g}(Y_{33}, Y_{34}, x) \leq 14 \tag{4.249}$$

$$\mathsf{g}(Y_{11}, Y_{14}, c) + \mathsf{g}(Y_{22}, Y_{24}, r) + \mathsf{g}(Y_{33}, Y_{34}, x) \leq 14. \tag{4.250}$$

Adding equations (4.237), (4.249), and (4.250), we get:

$$\mathsf{g}(Y_{11}, Y_{14}, a) + \mathsf{g}(Y_{11}, Y_{14}, b) + \mathsf{g}(Y_{11}, Y_{14}, c) + 3\mathsf{g}(Y_{22}, Y_{24}, r) + 3\mathsf{g}(Y_{33}, Y_{34}, x) \leq 42. \tag{4.251}$$

Substituting equation (4.232) and the case condition $\mathsf{g}(Y_{33}, Y_{34}, x) = 5$, we get:

$$\mathsf{g}(Y_{22}, Y_{24}, r) \leq 13/3. \tag{4.252}$$

Since like equation (4.164) it can be shown that $\mathsf{g}(Y_{22}, Y_{24}) = 4$, and that rank function is integer valued, we must have:

$$\mathsf{g}(Y_{22}, Y_{24}, r) = 4. \tag{4.253}$$

Similar to equation (4.246), it can be shown that:

$$\mathsf{g}(Y_{22}, Y_{24}, r) + \mathsf{g}(Y_{22}, Y_{25}, r) \geq 9. \tag{4.254}$$

Substituting equation (4.253) in equation (4.254) and noting equation (4.226), we have:

$$\mathsf{g}(Y_{22}, Y_{25}, r) = 5. \tag{4.255}$$

Like equation (4.237), dues to terminals t_1, t_2 and t_3, the following equations hold true.

$$\mathsf{g}(Y_{11}, Y_{15}, a) + \mathsf{g}(Y_{22}, Y_{25}, r) + \mathsf{g}(Y_{33}, Y_{35}, x) \leq 14 \tag{4.256}$$

$$\mathsf{g}(Y_{11}, Y_{15}, a) + \mathsf{g}(Y_{22}, Y_{25}, r) + \mathsf{g}(Y_{33}, Y_{35}, y) \leq 14 \tag{4.257}$$

$$\mathsf{g}(Y_{11}, Y_{15}, a) + \mathsf{g}(Y_{22}, Y_{25}, r) + \mathsf{g}(Y_{33}, Y_{35}, z) \leq 14. \tag{4.258}$$

Substituting equations (4.248) and (4.255) in equations (4.256), (4.257) and (4.258) respectively, we get the following:

$$\mathsf{g}(Y_{33}, Y_{35}, x) \leq 4 \tag{4.259}$$

$$\mathsf{g}(Y_{33}, Y_{35}, y) \leq 4 \tag{4.260}$$

$$\mathsf{g}(Y_{33}, Y_{35}, z) \leq 4. \tag{4.261}$$

Substituting equations (4.259), (4.260), and (4.261) in equation (4.236) we get $12 \geq 14$, which is a contradiction. Hence, $\mathcal{N}_3$ does not have a 2-dimensional vector linear solution under this case.

Case I.1.1.1.2: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 3$, $\mathsf{g}(Y_{11}, c) = 4$, $\mathsf{g}(Y_{22}, r) = 3$, $\mathsf{g}(Y_{22}, s) = 3$, $\mathsf{g}(Y_{22}, w) = 4$, $\mathsf{g}(Y_{33}, Y_{34}, x) = 4$.

We show that this case condition leads to $\mathsf{g}(Y_{11}, Y_{15}, a) = 4$. We know:

$$\begin{aligned} 6 &= \mathsf{g}(x, y, z) \\ &\leq \mathsf{g}(x, y, z, Y_{33}, Y_{34}, Y_{35}) \\ &= \mathsf{g}(Y_{33}, Y_{34}, Y_{35}) \\ &\leq \mathsf{g}(Y_{33}) + \mathsf{g}(Y_{34}) + \mathsf{g}(Y_{35}) \\ &\leq 6. \end{aligned} \tag{4.262}$$

Equation (4.262) indicates that

$$\mathsf{g}(Y_{33}, Y_{34}, Y_{35}) = \mathsf{g}(Y_{33}) + \mathsf{g}(Y_{34}) + \mathsf{g}(Y_{35}) = 6. \tag{4.263}$$

We also have:

$$\begin{aligned} &\mathsf{g}(Y_{33}, Y_{34}, x) + \mathsf{g}(Y_{33}, Y_{35}, x) \\ &\geq \mathsf{g}(Y_{33}, Y_{34}, Y_{35}, x) + \mathsf{g}(Y_{33}, x) \\ &\geq 6 + 3 = 9 \qquad [\text{using equation (4.263) and that } \mathsf{g}(Y_{33}, x) = 3]. \end{aligned} \tag{4.264}$$

Substituting the case condition $\mathsf{g}(Y_{33}, Y_{34}, x) = 4$ and equation (4.229) in equation (4.264), we have:

$$\mathsf{g}(Y_{33}, Y_{35}, x) = 5. \tag{4.265}$$

Due to the demands of terminal t_1, we have:

$$\begin{aligned}
&\mathrm{g}(Y_{11}, Y_{15}, a) + \mathrm{g}(Y_{22}, Y_{25}, r) + \mathrm{g}(Y_{33}, Y_{35}, x) \\
&= \mathrm{g}(Y_{11}, Y_{15}, a, Y_{22}, Y_{25}, r, Y_{33}, Y_{35}, x) \qquad \text{[reasoning is similar to equation (4.130)]} \\
&= \mathrm{g}(Y_{11}, Y_{15}, a, Y_{22}, Y_{25}, r, Y_{33}, Y_{35}, x, Z_{5,1}) \\
&\leq \mathrm{g}(Y_{11}, Y_{15}, a, Y_{22}, Y_{25}, r, Y_{33}, Y_{35}, x, Z_{5,1}, Z_{4,1}) \\
&= \mathrm{g}(Y_{11}, Y_{15}, Y_{22}, Y_{25}, Y_{33}, Y_{35}, Z_{5,1}, Z_{4,1}) \\
&= \mathrm{g}(Y_{11}, Y_{15}, Y_{22}, Y_{25}, Y_{33}, Y_{35}, Z_{4,1}) \\
&\leq 14. \qquad (4.266)
\end{aligned}$$

Similarly due to the demands of terminals t_4 and t_7 respectively the following equations can be determined.

$$\mathrm{g}(Y_{11}, Y_{15}, a) + \mathrm{g}(Y_{22}, Y_{25}, s) + \mathrm{g}(Y_{33}, Y_{35}, x) \leq 14 \qquad (4.267)$$

$$\mathrm{g}(Y_{11}, Y_{15}, a) + \mathrm{g}(Y_{22}, Y_{25}, w) + \mathrm{g}(Y_{33}, Y_{35}, x) \leq 14. \qquad (4.268)$$

Adding equations (4.266), (4.267), and (4.268), we have:

$$3\mathrm{g}(Y_{11}, Y_{15}, a) + \mathrm{g}(Y_{22}, Y_{25}, r) + \mathrm{g}(Y_{22}, Y_{25}, s) + \mathrm{g}(Y_{22}, Y_{25}, w) + 3\mathrm{g}(Y_{33}, Y_{35}, x) \leq 42. \qquad (4.269)$$

Substituting equations (4.234) and (4.265) in equation (4.269), we have:

$$\mathrm{g}(Y_{11}, Y_{15}, a) \leq 13/3. \qquad (4.270)$$

Since the rank function is always an integer, and that $\mathrm{g}(Y_{11}, Y_{15}) = 2$ (the latter can be proved similarly to equation (4.165)), we have:

$$\mathrm{g}(Y_{11}, Y_{15}, a) = 4. \qquad (4.271)$$

Case I.1.1.1.2.1: $\mathrm{g}(Y_{11}, a) = 3$, $\mathrm{g}(Y_{11}, b) = 3$, $\mathrm{g}(Y_{11}, c) = 4$, $\mathrm{g}(Y_{22}, r) = 3$, $\mathrm{g}(Y_{22}, s) = 3$, $\mathrm{g}(Y_{22}, w) = 4$, $\mathrm{g}(Y_{33}, Y_{34}, x) = 4$ and $\mathrm{g}(Y_{33}, Y_{34}, y) = 4$.

Substituting the case conditions in equation (4.235) we have: $\mathrm{g}(Y_{33}, Y_{34}, z) \geq 6$. Since, as per the lemma we intend to prove, the rank of an element is less than or equal to 2, we have:

$$\mathrm{g}(Y_{33}, Y_{34}, z) = 6. \qquad (4.272)$$

Due to the demands of the terminal t_6, we have:

$$\begin{aligned}
&\mathsf{g}(Y_{11}, Y_{14}, a) + \mathsf{g}(Y_{22}, Y_{24}, r) + \mathsf{g}(Y_{33}, Y_{34}, z) \\
&= \mathsf{g}(Y_{11}, Y_{14}, a, Y_{22}, Y_{24}, r, Y_{33}, Y_{34}, z) \qquad \text{[reasoning is similar to equation (4.130)]} \\
&= \mathsf{g}(Y_{11}, Y_{14}, a, Y_{22}, Y_{24}, r, Y_{33}, Y_{34}, z, Z_{4,6}) \\
&\leq \mathsf{g}(Y_{11}, Y_{14}, a, Y_{22}, Y_{24}, r, Y_{33}, Y_{34}, z, Z_{4,6}, Z_{5,6}) \\
&= \mathsf{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, Z_{4,6}, Z_{5,6}) \\
&= \mathsf{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, Z_{5,6}) \\
&\leq 14. \qquad (4.273)
\end{aligned}$$

Substituting equation (4.272) in equation (4.273), we have:

$$\mathsf{g}(Y_{11}, Y_{14}, a) + \mathsf{g}(Y_{22}, Y_{24}, r) \leq 8. \qquad (4.274)$$

Now, similar to equations (4.165) and (4.164) it can be shown that $\mathsf{g}(Y_{11}, Y_{14}) = 4$ and $\mathsf{g}(Y_{22}, Y_{24}) = 4$. Then we have:

$$\mathsf{g}(Y_{11}, Y_{14}, a) \geq 4 \qquad (4.275)$$

$$\mathsf{g}(Y_{22}, Y_{24}, r) \geq 4. \qquad (4.276)$$

Substituting equations (4.275) and (4.276) in equation (4.274), we must have:

$$\mathsf{g}(Y_{11}, Y_{14}, a) = 4. \qquad (4.277)$$

Similar to equation (4.264) it can be shown that

$$\mathsf{g}(Y_{11}, Y_{14}, a) + \mathsf{g}(Y_{11}, Y_{15}, a) \geq 9. \qquad (4.278)$$

Substituting equations (4.277) and (4.271) in equation (4.278), we have $8 \geq 9$, which is a contradiction. So $\mathcal{N}_3$ does not have a 2-dimensional vector linear solution under this case.

Case I.1.1.1.2.2: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 3$, $\mathsf{g}(Y_{11}, c) = 4$, $\mathsf{g}(Y_{22}, r) = 3$, $\mathsf{g}(Y_{22}, s) = 3$, $\mathsf{g}(Y_{22}, w) = 4$, $\mathsf{g}(Y_{33}, Y_{34}, x) = 4$ and $\mathsf{g}(Y_{33}, Y_{34}, y) = 5$.

Due to the demands of the terminal t_5, we have:

$$\begin{aligned}
&\mathrm{g}(Y_{11}, Y_{14}, a) + \mathrm{g}(Y_{22}, Y_{24}, s) + \mathrm{g}(Y_{33}, Y_{34}, y) \\
&= \mathrm{g}(Y_{11}, Y_{14}, a, Y_{22}, Y_{24}, s, Y_{33}, Y_{34}, y) \qquad \text{[reasoning is similar to equation (4.130)]} \\
&= \mathrm{g}(Y_{11}, Y_{14}, a, Y_{22}, Y_{24}, s, Y_{33}, Y_{34}, y, Z_{4,5}) \\
&\leq \mathrm{g}(Y_{11}, Y_{14}, a, Y_{22}, Y_{24}, s, Y_{33}, Y_{34}, y, Z_{4,5}, Z_{5,5}) \\
&= \mathrm{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, y, Z_{4,5}, Z_{5,5}) \\
&= \mathrm{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Y_{33}, Y_{34}, y, Z_{5,5}) \\
&= \mathrm{g}(Y_{33}, Y_{34}, y) + \mathrm{g}(Y_{11}, Y_{14}, Y_{22}, Y_{24}, Z_{5,5} | Y_{33}, Y_{34}, y) \\
&\leq 5 + 10 = 15 \qquad \text{[using the case codnition]}.
\end{aligned} \tag{4.279}$$

Similar to equations (4.267) and (4.268) the following equations can be shown to hold:

$$\mathrm{g}(Y_{11}, Y_{14}, a) + \mathrm{g}(Y_{22}, Y_{24}, r) + \mathrm{g}(Y_{33}, Y_{34}, y) \leq 14 \tag{4.280}$$

$$\mathrm{g}(Y_{11}, Y_{14}, a) + \mathrm{g}(Y_{22}, Y_{24}, w) + \mathrm{g}(Y_{33}, Y_{34}, y) \leq 14. \tag{4.281}$$

Adding equations (4.279), (4.280), and (4.281), we get:

$$3\mathrm{g}(Y_{11}, Y_{14}, a) + \mathrm{g}(Y_{22}, Y_{24}, r) + \mathrm{g}(Y_{22}, Y_{24}, s) + \mathrm{g}(Y_{22}, Y_{24}, w) + 3\mathrm{g}(Y_{33}, Y_{34}, y) \leq 43. \tag{4.282}$$

Substituting equation (4.233) in equation (4.282), we get:

$$3\mathrm{g}(Y_{11}, Y_{14}, a) + 3\mathrm{g}(Y_{33}, Y_{34}, y) \leq 29. \tag{4.283}$$

Substituting the case condition $\mathrm{g}(Y_{33}, Y_{34}, y) = 5$ in equation (4.283), we get:

$$\mathrm{g}(Y_{11}, Y_{14}, a) \leq 14/3. \tag{4.284}$$

Now, similar to equation (4.165) it can be shown that $\mathrm{g}(Y_{11}, Y_{14}) = 4$. Then, as the rank function is integer valued and as equation (4.284) holds, we must have:

$$\mathrm{g}(Y_{11}, Y_{14}, a) = 4. \tag{4.285}$$

Substituting equations (4.285) and (4.271) in equation (4.278), which holds in this case as well, we have $8 \leq 9$, which is a contradiction.

Case I.1.1.2: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 3$, $\mathsf{g}(Y_{11}, c) = 4$, $\mathsf{g}(Y_{22}, r) = 3$, $\mathsf{g}(Y_{22}, s) = 4$, $\mathsf{g}(Y_{22}, w) = 3$.

Substituting the case conditions in equation (4.209), we have $\mathsf{g}(Y_{33}, x) \leq 2$. However, as $\mathsf{g}(x) = 2$, we must have $\mathsf{g}(Y_{33}, x) = 2$. Substituting this value in equation (4.213), we must have $\mathsf{g}(Y_{33}, y) = 4$ and $\mathsf{g}(Y_{33}, z) = 4$. Substituting the latter value along with the case conditions in equation (4.201), we have $11 \leq 10$, which is a contradiction.

Case I.1.1.3: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 3$, $\mathsf{g}(Y_{11}, c) = 4$, $\mathsf{g}(Y_{22}, r) = 3$, $\mathsf{g}(Y_{22}, s) = 4$, $\mathsf{g}(Y_{22}, w) = 4$.

The proof that $\mathcal{N}_3$ does not have a 2-dimensional vector linear solution under case is same as that of **Case I.1.1.2**.

Case I.1.2: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 3$, $\mathsf{g}(Y_{11}, c) = 4$, $\mathsf{g}(Y_{22}, r) = 2$.

From equation (4.212), we have: $\mathsf{g}(Y_{22}, s) = 4$ and $\mathsf{g}(Y_{22}, w) = 4$. Substituting values in equation (4.209), we get: $\mathsf{g}(Y_{33}, x) = 2$. Then, from equation (4.213), we have $\mathsf{g}(Y_{33}, y) = \mathsf{g}(Y_{33}, z) = 4$. Substituting these values and the case conditions in equation (4.203), we get: $11 \leq 10$, which is a contradiction.

Case I.2: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 4$, $\mathsf{g}(Y_{11}, c) = 3$.

Case I.2.1: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 4$, $\mathsf{g}(Y_{11}, c) = 3$, $\mathsf{g}(Y_{22}, r) = 3$.

Case I.2.1.1: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 4$, $\mathsf{g}(Y_{11}, c) = 3$, $\mathsf{g}(Y_{22}, r) = 3$, $\mathsf{g}(Y_{22}, s) = 3$, $\mathsf{g}(Y_{22}, w) = 4$.

From equation (4.206) we get that $\mathsf{g}(Y_{33}, x) \leq 2$. Then due to equation (4.213) it must be that $\mathsf{g}(Y_{33}, y) = 4$ and $\mathsf{g}(Y_{33}, z) = 4$. However then equation (4.205) cannot be satisfied.

Case I.2.1.2: $\mathsf{g}(Y_{11}, a) = 3$, $\mathsf{g}(Y_{11}, b) = 4$, $\mathsf{g}(Y_{11}, c) = 3$, $\mathsf{g}(Y_{22}, r) = 3$, $\mathsf{g}(Y_{22}, s) = 4$, $\mathsf{g}(Y_{22}, w) = 3$.

Substituting $\mathsf{g}(Y_{11}, a) = 3$ and $\mathsf{g}(Y_{22}, s) = 4$ in equation (4.200), we get:

$$\mathsf{g}(Y_{33}, x) \leq 3. \tag{4.286}$$

Similarly from equation (4.201), we get:

$$\mathsf{g}(Y_{33}, z) \leq 3. \tag{4.287}$$

Due to the demands of the terminal t_{14}, we have:

$$\begin{aligned}
&\mathsf{g}(Y_{11}, b) + \mathsf{g}(Y_{22}, s) + \mathsf{g}(Y_{33}, y) \\
&= \mathsf{g}(Y_{11}, b, Y_{22}, s, Y_{33}, y) \qquad \text{[reasoning is similar to equation (4.130)]} \\
&\leq \mathsf{g}(Y_{11}, b, Y_{22}, s, Y_{33}, y, Z_{4,14}, Z_{5,14}, Y_{e_1^s}, Y_{e_1^y}, Y_{e_1^b}, a)
\end{aligned}$$

$$
\begin{aligned}
&= \mathrm{g}(Y_{11}, Y_{22}, Y_{33}, Z_{4,14}, Z_{5,14}, Y_{e_1^s}, Y_{e_1^y}, Y_{e_1^b}, a) \\
&= \mathrm{g}(Y_{11}, Y_{22}, Y_{33}, Z_{4,14}, Z_{5,14}, a) \qquad [Y_{e_1^s}, Y_{e_1^y}, Y_{e_1^b} \text{ are functions of } a] \\
&= \mathrm{g}(Y_{11}, a) + \mathrm{g}(Y_{22}, Y_{33}, Z_{4,14}, Z_{5,14} | Y_{11}, a) \\
&\leq 3 + 8 = 11. \qquad (4.288)
\end{aligned}
$$

Substituting $\mathrm{g}(Y_{11}, b) = 4$ and $\mathrm{g}(Y_{22}, s) = 4$ in equation (4.288), we get:

$$\mathrm{g}(Y_{33}, y) \leq 3. \qquad (4.289)$$

Substituting equations (4.286), (4.287), and (4.289) in equation (4.213) we get $9 \geq 10$, which is a contradiction.

Case I.2.1.3: $\mathrm{g}(Y_{11}, a) = 3$, $\mathrm{g}(Y_{11}, b) = 4$, $\mathrm{g}(Y_{11}, c) = 3$, $\mathrm{g}(Y_{22}, r) = 3$, $\mathrm{g}(Y_{22}, s) = 4$, $\mathrm{g}(Y_{22}, w) = 4$.

The proof that under this case $\mathcal{N}_3$ does not have a 2-dimensional vector linear solution is similar to that of **Case I.2.1.2**.

Case I.2.2: $\mathrm{g}(Y_{11}, a) = 3$, $\mathrm{g}(Y_{11}, b) = 4$, $\mathrm{g}(Y_{11}, c) = 3$, $\mathrm{g}(Y_{22}, r) = 2$.

As rank of any element is less than or equal to 2, substituting $\mathrm{g}(Y_{22}, r) = 2$ in equation (4.212), we get: $\mathrm{g}(Y_{22}, s) = 4$ and $\mathrm{g}(Y_{22}, w) = 4$. Then, similar to Case I.2.1.2 it can be proved that $\mathcal{N}_3$ does not have a 2-dimensional vector linear solution under this case.

Case I.3: $\mathrm{g}(Y_{11}, a) = 3$, $\mathrm{g}(Y_{11}, b) = 4$, $\mathrm{g}(Y_{11}, c) = 4$.

Case I.3.1: $\mathrm{g}(Y_{11}, a) = 3$, $\mathrm{g}(Y_{11}, b) = 4$, $\mathrm{g}(Y_{11}, c) = 4$, $\mathrm{g}(Y_{22}, r) = 3$.

From equation (4.204), we have $\mathrm{g}(Y_{33}, x) \leq 3$; from equation (4.205), we have $\mathrm{g}(Y_{33}, z) \leq 3$; and from equation (4.208), we have $\mathrm{g}(Y_{33}, y) \leq 3$. Substituting these values in equation (4.213), we get $9 \geq 10$, which is a contradiction.

Case I.3.2: $\mathrm{g}(Y_{11}, a) = 3$, $\mathrm{g}(Y_{11}, b) = 4$, $\mathrm{g}(Y_{11}, c) = 4$, $\mathrm{g}(Y_{22}, r) = 2$.

In this case, due to equation (4.212), we have $\mathrm{g}(Y_{22}, s) = 4$ and $\mathrm{g}(Y_{22}, w) = 4$. Then, similar to **Case I.2.1.2** it can be proved that $\mathcal{N}_3$ does not have a 2-dimensional vector linear solution under this case.

Case II: $\mathrm{g}(Y_{11}, a) = 2$.

Then, form equation (4.211), we have $\mathrm{g}(Y_{11}, b) = 4$ and $\mathrm{g}(Y_{11}, c) = 4$.

Case II.1: $\mathrm{g}(Y_{11}, a) = 2$, $\mathrm{g}(Y_{11}, b) = 4$, $\mathrm{g}(Y_{11}, c) = 4$, $\mathrm{g}(Y_{22}, r) = 3$.

Using the values set by the case condition, from equation (4.204), we have $\mathrm{g}(Y_{33}, x) \leq 3$, from

equation (4.205), we have $\mathsf{g}(Y_{33}, z) \leq 3$, and from equation (4.208), we have $\mathsf{g}(Y_{33}, y) \leq 3$. Substituting these values in equation (4.213) we get $9 \geq 10$, which is a contradiction.

Case II.2: $\mathsf{g}(Y_{11}, a) = 2$, $\mathsf{g}(Y_{11}, b) = 4$, $\mathsf{g}(Y_{11}, c) = 4$, $\mathsf{g}(Y_{22}, r) = 2$.

Then, from equation (4.212), we have $\mathsf{g}(Y_{22}, s) = 4$ and $\mathsf{g}(Y_{22}, w) = 4$. So substituting $\mathsf{g}(Y_{11}, b) = 4$ and $\mathsf{g}(Y_{22}, w) = 4$ in equation (4.206), we have: $\mathsf{g}(Y_{33}, x) = 2$. Then, from equation (4.213), we have $\mathsf{g}(Y_{33}, y) = 4$ and $\mathsf{g}(Y_{33}, z) = 4$. Substituting $\mathsf{g}(Y_{11}, b) = 4$, $\mathsf{g}(Y_{22}, s) = 4$, and $\mathsf{g}(Y_{33}, y) = 4$ in equation (4.288) we get: $12 \leq 11$, which is a contradiction.

To prove the if part we show a 2-dimensional vector linear coding scheme over a finite field whose characteristic divides either of q_1 or q_2. Since $\mathcal{G}_3$ already has a scalar linear solution over finite fields whose characteristic divides q_1, it also has a vector linear solution over the same field for any message dimension. In Fig. 4.9 we show a 2-dimensional vector linear solution when the characteristic of the finite field divides $q_2 = 3$. The coding scheme can be easily extended for all values of q_2. ■

4.2 Main Results

First we describe what is meant by union of two networks.

Definition 8. *Let $\mathcal{K}_1$ be a network, and let V_1 be the set of all nodes in $\mathcal{K}_1$ and let E_1 be the set of all edges in $\mathcal{K}_1$. Similarly, let $\mathcal{K}_2$ be a network whose set of nodes is denoted by V_2 and set of edges is denoted by E_2. The union of networks $\mathcal{K}_1$ and $\mathcal{K}_2$ is a network whose node set is $V_1 \cup V_2$, and edge set is $E_1 \cup E_2$.*

The next two theorems shows that by *increasing* the message dimension just by 1, the set of characteristics over which a vector linear solution exists may get arbitrarily larger.

Theorem 33. *For any finite non-empty 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 $P = \{p_1, p_2, \ldots, p_l\}$. We show that the network $\mathcal{G}_1$ for $q = p_1 \times p_2 \times \cdots \times p_l$ is such a network. From Lemma 27 we know that $\mathcal{G}_1$ has a scalar linear solution if and only if characteristic of the finite field divides q. Becasue of our chosen value of q, the characteristic divides q if and only if it belongs to P. So $\mathcal{G}_1$ has a scalar linear solution if and only if the characteristic of the finite field belongs to P.

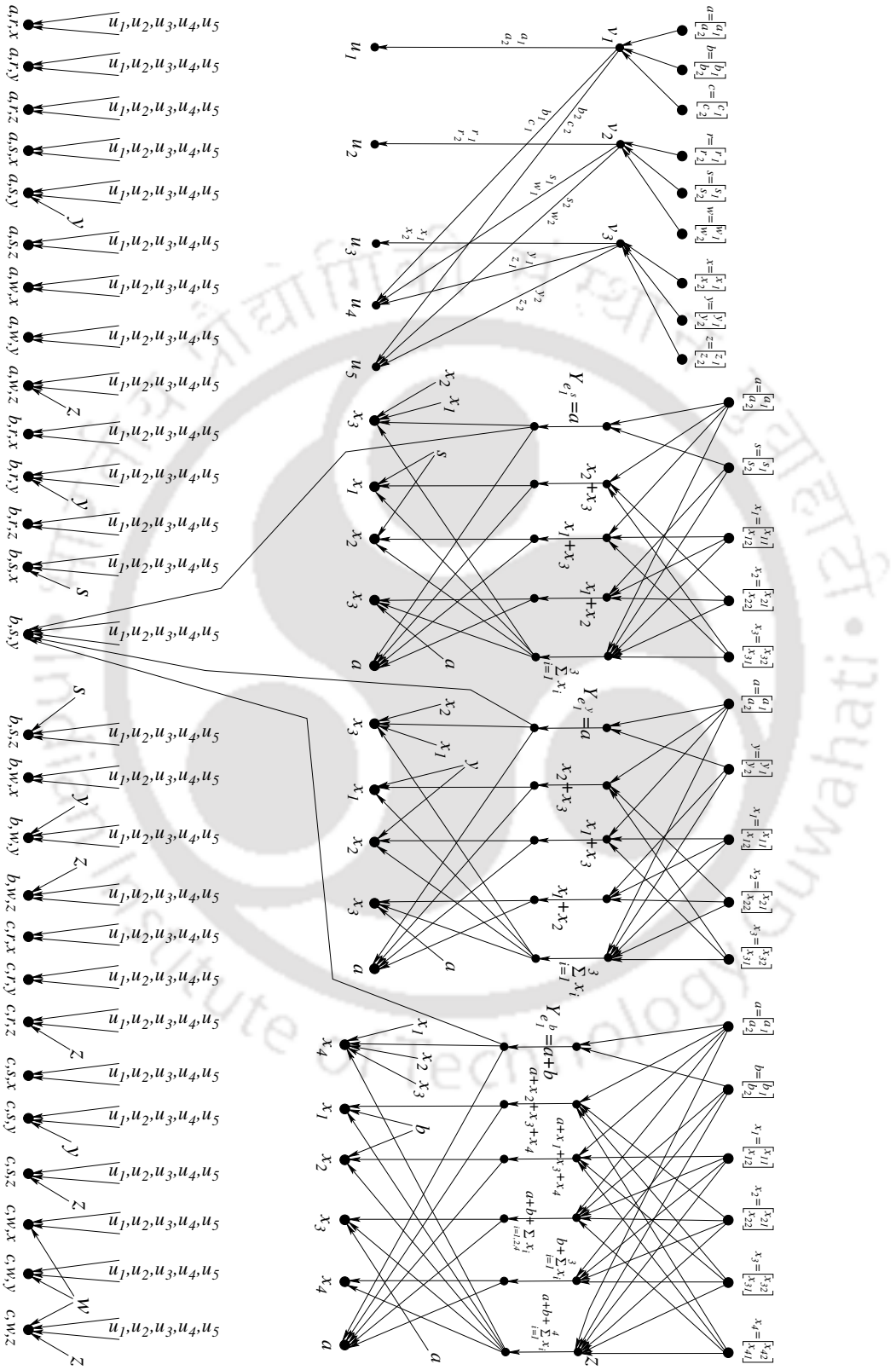

Figure 4.9: A 2-dimensional vector linear solution of $\mathcal{G}_3$ for $q_1 = 2$ and $q_2 = 3$ when the characteristic divides q_2.

We now show a 2-dimensional vector linear solution over all finite fields. The M-network part of $\mathcal{G}_1$ has a 2-dimensional vector linear solution over all finite fields. In Lemma 25 the Char-q-$\bar{y}$ part of $\mathcal{G}_1$ was shown to have a scalar linear solution over all finite fields when its middle edges do not carry any information about $\bar{y}$. Since, the M-network part is already solved, the middle edges of the Char-q-$\bar{y}$ network do not need the carry any information about $\bar{y}$. So $\mathcal{G}_1$ has a 2-dimensional vector linear solution over all finite fields. ■

Theorem 34. *For any three finite non-empty sets of primes P_1, P_2, and P_3, there exists a network which has a scalar linear solution if and only if the characteristic of the finite field belongs to P_1, has a 2-dimensional vector linear solution if and only if the characteristic of the finite field belongs to $\{P_1, P_2\}$, and has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to $\{P_1, P_2, P_3\}$.*

Proof: Consider the union of the networks $\mathcal{G}_1$ (presented in Section 4.1.2) and $\mathcal{G}_3$ (presented in Section 4.1.4), and name the resultant network as $\mathcal{G}_{13}$. Let the value of q in $\mathcal{G}_1$ be equal to the product of the primes contained in $P_1 \cup P_2 \cup P_3$. Then according to Lemma 27, $\mathcal{G}_1$ has a vector linear solution for any odd message dimension if and only if the characteristic of the finite field belongs to $P_1 \cup P_2 \cup P_3$.

In the $\mathcal{G}_3$ network let q_1 be equal to the product of the primes contained in P_1, and let q_2 be equal to the product of the primes contained in P_2. Then, from Lemma 31 we get that $\mathcal{G}_3$ has a scalar linear solution if and only if the characteristic of the finite field belongs to P_1, and has a 2-dimensional vector linear solution if and only if the characteristic of the finite field is in $P_1 \cup P_2$.

Now, for the scalar case, since $\mathcal{G}_1$ has a scalar linear solution only over finite fields whose characteristic belongs to $P_1 \cup P_2 \cup P_3$, and $\mathcal{G}_3$ has a scalar linear solution only over finite fields whose characteristic belongs to P_1, $\mathcal{G}_{13}$ (union of the two networks) has a scalar linear solution if and only if the characteristic of the finite field belongs to P_1.

For the case when message dimension is equal to 2, we first note that as shown in Theorem 33 $\mathcal{G}_1$ has a 2-dimensional vector linear solution over all finite fields. Then, since $\mathcal{G}_3$ has a 2-dimensional vector linear solution if and only if the characteristic of the finite field is in $P_1 \cup P_2$, network $\mathcal{G}_{13}$ has a 2-dimensional vector linear solution if and only if the characteristic of the finite field is in $P_1 \cup P_2$.

For the case when message dimension is equal to 3, we note that part of the $\mathcal{G}_3$ network which is the generalized M-network for $m = 3$ (shown as network $\mathcal{N}_3$ in Chapter 3) has a 3-dimensional vector

linear solution over all finite fields. Since the middle edges of Char-q_1-s, Char-q_1-y, and Char-q_2-b do not need carry any symbols of s, y, and b respectively (because the the generalized M-network for $m = 3$ already has a solution), as shown in Lemma 25 they have a scalar linear solution over all finite fields. But $\mathcal{G}_1$ has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to $P_1 \cup P_2 \cup P_3$. So the network $\mathcal{G}_{13}$ has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to $P_1 \cup P_2 \cup P_3$. ■

Note: For any given positive integer n, if $|P_3| > |P_2|+n$, then Theorem 34 shows that there exists a network which has the 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.

Theorems 33 and 34 may indicate that a higher message dimension is superior to a lower message dimension in terms of achieving a vector linear solution over a larger set of characteristics. But the next theorem shows that such a hierarchy does not exist between two message dimensions greater than 1; it shows that there also exists a network where by *increasing* the message dimension just by 1, the set of characteristics over which a vector linear solution exists may get smaller.

Theorem 35. *For any two finite non-empty 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.*

Proof: Consider the union of the networks $\mathcal{G}_1$ and $\mathcal{G}_2$ and denote it by $\mathcal{G}_{12}$. Let the value of q in network $\mathcal{G}_1$ be equal to the product of the primes contained in P_2 and let the value of q' in $\mathcal{G}_2$ be equal to the product of the primes contained in $\{P_1, P_2\}$.

Since $\mathcal{G}_2$ does not have a scalar linear solution over any finite field (Lemma 28), the network $\mathcal{G}_{12}$ does not have a scalar linear solution over any finite field.

As shown in Theorem 33 $\mathcal{G}_1$ has a 2-dimensional vector linear solution over all finite fields. But due to Lemma 29, $\mathcal{G}_2$ has a 2-dimensional vector linear solution if and only if the characteristic of the finite field divides q'. This implies that $\mathcal{G}_2$ has a 2-dimensional vector linear solution if and only if the characteristic of the finite field belongs to $\{P_1, P_2\}$. So the network $\mathcal{G}_{12}$ has a 2-dimensional vector linear solution if and only if the characteristic of the finite field belongs to $\{P_1, P_2\}$.

The part of the network $\mathcal{G}_2$ which is the generalized M-network for $m = 3$ (shown as $\mathcal{N}_3$ in

Chapter 3) has a 3-dimensional vector linear solution over all finite fields. Hence, as the Char-q-x part of $\mathcal{G}_2$ does not have to carry any symbols of x (because the $\mathcal{N}_3$ is already having a 3-dimensional vector linear solution), Char-q-x has a scalar linear solution over all finite fields (shown in Lemma 25). Hence $\mathcal{G}_2$ has a 3-dimensional vector linear solution over all finite fields. But from Lemma 27 we know that $\mathcal{G}_1$ has a 3-dimensional vector linear solution if and only if the characteristic of the finite field divides q. Then network $\mathcal{G}_{12}$ 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 $|P_1|$ is such that $|P_1| > |P_2| + n$, then Theorem 35 shows that there exists a network which has the 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.

The next theorem shows that if a network has vector linear solutions for two different message dimensions, then it does not necessarily mean that the set of characteristics over which the network has the vector linear solution for the higher message dimension is a superset of the set of characteristics over which the network has the vector linear solution for the lower message dimension, and vice versa.

Theorem 36. *For any two finite non-empty 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, and has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to P_2.*

Proof: The proof is similar to Theorem 35. (replace $\{P_1, P_2\}$ of Theorem 35 by P_1, *i.e.*, the value of q' in $\mathcal{G}_2$ is be equal to the product of the primes contained in P_1). ■

Theorem 37. *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 $\mathcal{G}_1$ for $q = p$ is such a network. Lemma 25 shows that $\mathcal{G}_1$ 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 [13] and [44]. In [44], it has been shown that all networks which 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 25 it can

be seen that only addition and subtraction operations required to achieve a scalar linear solution of the Char-q-$\bar{y}$. Hence the same solution would also work over any ring. Since both the M-network and the Char-q-$\bar{y}$ network have a scalar linear solution over the non-commutative ring of size 16, $\mathcal{G}_1$ 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 $\mathcal{G}_1$ has that property that the size of the alphabet required to achieve a scalar linear solution over a finite field is arbitrary larger than the size of the alphabet required to achieve a scalar linear solution over a non-commutative ring.

Lemma 38. *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 that the network $\mathcal{G}_{12}$ shown in the proof of Theorem 36 is such a network when the sets P_1 and P_2 are disjoint. We have shown that $\mathcal{G}_{12}$ has a 2-dimensional vector linear solution if and only if the characteristic of the finite field belongs to P_1. We have also shown that $\mathcal{G}_{12}$ has a 3-dimensional vector linear solution if and only if the characteristic of the finite field belongs to P_2.

In Lemma 30 we showed that the network $\mathcal{G}_2$ has a 5-dimensional vector linear solution if and only if the characteristic of the finite field divides q' (where q' is the product of primes contained in P_1). Then, for $\mathcal{G}_2$ to have a 5-dimensional vector linear solution, the characteristic of the finite field must belong to P_1. But as shown in Lemma 27, for our selected value of q (where q is the product of primes contained in P_2), $\mathcal{G}_1$ has a 5-dimensional vector linear solution if and only if the characteristic of the finite field belongs to P_2. Since P_1 and P_2 are disjoint, $\mathcal{G}_{12}$ has no 5-dimensional vector linear solution. □

Due to Lemma 38, we have the following theorem. Note that the 'if' part of the theorem is trivial to prove.

Theorem 39. *For a network, existences 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 if and only if the m_1 and m_2 dimensional vector linear solutions exists over the same finite field.*

4.3 Discussion

Recently it has been shown in [12] that linear coding capacity is dependent only on the characteristic of the finite field. This chapter 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 $\mathcal{G}_1$ is 1 and it can be achieved over all finite fields. But we now know that a rate 1 linear solution can be achieved over all finite fields if and only if the message dimension is even; for odd message dimensions, a rate 1 linear solution can be achieved if and only if the characteristic of the finite field divides q.

It has been shown that there exists characteristic-dependent linear rank inequalities that produce different upper-bounds on the linear coding capacity over different finite fields. Now as we have shown that the set of characteristics over which a network has an m-dimensional vector linear solution depends upon m, can characteristic-dependent linear rank inequalities capture this fact.

5

Characteristic-dependent linear rank inequalities

Contents

In the literature, it has been shown that the rate achievable using linear network coding depends upon the characteristic of the finite field. For example, it has been shown that for a network named as the Fano network, over finite fields of even characteristic, rate 1 is achievable using linear network coding, but if the characteristic of the finite field is not 2, then no rate higher than 4/5 is achievable. For such networks, the tightest upper-bound produced by Shannon information inequalities and non-Shannon information inequalities is 1, and neither of these two types of inequalities can produce different upper-bounds for different characteristics (somewhat obvious). For such networks, characteristic-dependent linear rank inequalities (a class of linear rank inequalities) can used to produce different upper-bounds for different characteristics. For example, for the Fano network, using a characteristic-dependent linear rank inequality, the 4/5 upper-bound over finite fields of odd characteristic can be obtained [32].

For any given vector space, the subspaces of the vector space obey a set of inequalities known as linear rank inequalities. For example, $dim(V_1) + dim(V_2) = dim(V_1 \cup V_2) + dim(V_1 \cap V_2)$ is a linear rank inequality ($dim(V)$ denotes the dimension of V). It has been shown that for each rate achievable using linear network coding, there exists a corresponding set of vector subspaces ([35] showed that linear solvability guarantees the existence of a representable discrete polymatroid, which can be seen as a set of vector subspaces). Any bound on the dimensions of these vector subspaces also results in a bound on the rates achievable using linear network coding.

It has been shown in [26] that all information inequalities (Shannon inequalities and non-Shannon inequalities) are also linear rank inequalities if the entropy function is replaced by the dimension function and the variables represent vector spaces. But there also exist linear rank inequalities that are not information inequalities. This indicates that the upper-bounds obtained using linear rank inequalities may be lesser than the upper-bounds obtained using Shannon information inequalities and non-Shannon information inequalities (because no. of linear rank inequalities = number of Shannon information inequalities + number of non-Shannon information inequalities + number of linear rank inequalities that are not information inequalities).

Hammer *et al.* showed that for upto three variables, there exists no linear rank inequality which is not an information inequality (Theorem 3 of [26]). The Ingleton inequality: $dim(A) + dim(B) + dim(A, B, C) + dim(A, B, D) + dim(C, D) \leq dim(A, B) + dim(A, C) + dim(A, D) + dim(B, C) + dim(B, D)$, was proved in 1969 by A. W. Ingleton [45]. The proof of this inequality can also be found

in [26] and [8]. This inequality has been used in [8] to find an upper-bound on the linear coding capacity of the *Vámos* network. Hammer *et al.* showed that for four variables, the only linear rank inequality that is not an information inequality is the Ingleton inequality and permutations of its variables (Theorem 5 of [26]).

Dougherty *et al.* presented a list of twenty four new linear rank inequalities on five variables, which are not information inequalities [29]. In [30] it has been shown that even an incomplete list of six variable linear rank inequalities cross one billion. For seven or more variables, Blasiak *et al.* showed that there exist linear rank inequalities that hold if the characteristic of the field is among a certain set of primes, but may not hold otherwise. Such an inequality is called as a characteristic-dependent linear rank inequality. Blasiak *et al.* showed two such seven variable inequalities: one holds over finite fields of even characteristic, and the other holds over finite fields of odd characteristic.

In [32], Dougherty *et al.* developed a novel method where characteristic-dependent linear rank inequalities were developed from networks which do not have a linear solution over one set of characteristics but has a linear solution over another (complement of the first) set of characteristics. We name this method as the *DFZ Method* based on the initials of the authors. In reference [32] they used this method to develop two new seven variable characteristic-dependent linear rank inequalities: one holds over all finite fields of odd characteristic but may not hold otherwise (produced from the Fano network); and another holds over all finite fields of even characteristic but may not hold otherwise (produced from the non-Fano network).

In [33], Dougherty *et al.* developed two new eight variable characteristic-dependent linear rank inequalities. First inequality holds over all finite fields of characteristic not equal to 3 but may not hold otherwise (this is produced from the T8 network, which is constructed from the T8 matroid); and the second inequality holds over all finite fields of characteristic equal to 3 but may not hold otherwise (this is produced from the non-T8 network, which is constructed from the non-T8 matroid).

Eric Freiling – in his thesis – showed that for any finite or co-finite set of primes numbers, there exists a characteristic-dependent linear rank inequality that holds if the characteristic of the finite field belongs to the given set, but may not hold otherwise [34].

In the fifth chapter, we – independently of the work of [34] – produce three new sets of linear rank inequalities for any set of primes P. For any given set of primes P, the inequalities in the first set hold if the characteristic of the finite field does not belong to P, and the inequalities in the second

and third set hold if the characteristic of the finite field belongs to P. We also show the application of these inequalities in computing upper-bounds on the linear coding capacity of networks.

5.1 Three New Sets of Characteristic-Dependent Linear Rank Inequalities

In this section, we present three new sets of characteristic-dependent linear rank inequalities. For each set of primes there exists one characteristic-dependent linear rank inequality in each of the sets. We present these inequalities in the next three theorems.

5.1.1 First Set of Inequalities

Theorem 40. *For any given set of primes $\{p_1, p_2, \ldots, p_l\}$, let $A, B_1, B_2, \ldots, B_{q-1}, C, V_1, V_2, \ldots, V_{q-1}, W, X, Y, Z$ be vector subspaces of a finite dimensional vector space V where $q = p_1 \times p_2 \times \cdots \times p_l$. Then the following linear rank inequality holds if V is a vector space over a finite field whose characteristic does not belong to $\{p_1, p_2, \ldots, p_l\}$, but may not hold otherwise:*

$$
\begin{aligned}
&(2q-1)dim(A) + \sum_{i=1}^{q-1} 2dim(B_i) + (2q-2)dim(C) \leq (q-1)(dim(W) + dim(X) + dim(Y) \\
&+ 2dim(Z)) + \sum_{i=1}^{q-1} dim(V_i) + (7q-6)dim(W|A, B_1, \ldots, B_{q-1}) + (6q-5)dim(X|B_1, \ldots, B_{q-1}, C) \\
&+ \sum_{i=1}^{q-1} (2q)dim(V_i|X, B_1, .., B_{i-1}, B_{i+1}, .., B_{q-1}) + (3q-3)dim(Y|W, X) + (4q-3)dim(Z|W, C) \\
&+ (2q-1)dim(A|Z, V_1, \ldots, V_{q-1}) + (q-1)dim(C|A, Y) \\
&+ \sum_{i=1}^{q-1} 2dim(B_i|B_1, \ldots, B_{i-1}, B_{i+1}, \ldots, B_{q-1}, Y, Z) + \sum_{i=1}^{q-1} dim(C|V_i, B_i) \\
&+ (5q-4)(dim(A) + \sum_{i=1}^{q-1} dim(B_i) + dim(C) - dim(A, B_1, \ldots, B_{q-1}, C)) \\
&+ (q-1)(\sum_{i=1}^{q-1} dim(B_i) + dim(C) - dim(B_1, \ldots, B_{q-1}, C). \qquad (5.1)
\end{aligned}
$$

The proof of the truth of this inequality is given in Section 5.3. Note that the linear rank inequality in equation (5.1) has $2q + 4$ number of variables. Before we present the proof we show that this inequality may not hold if $q = 0$ over the finite field (note $q = 0$ when the characteristic belong to the given set of primes). Let V be $q+1$ dimensional vector space over $\mathbb{F}_{p^\alpha}$ where $p \in \{p_1, p_2, \ldots, p_l\}$ and α

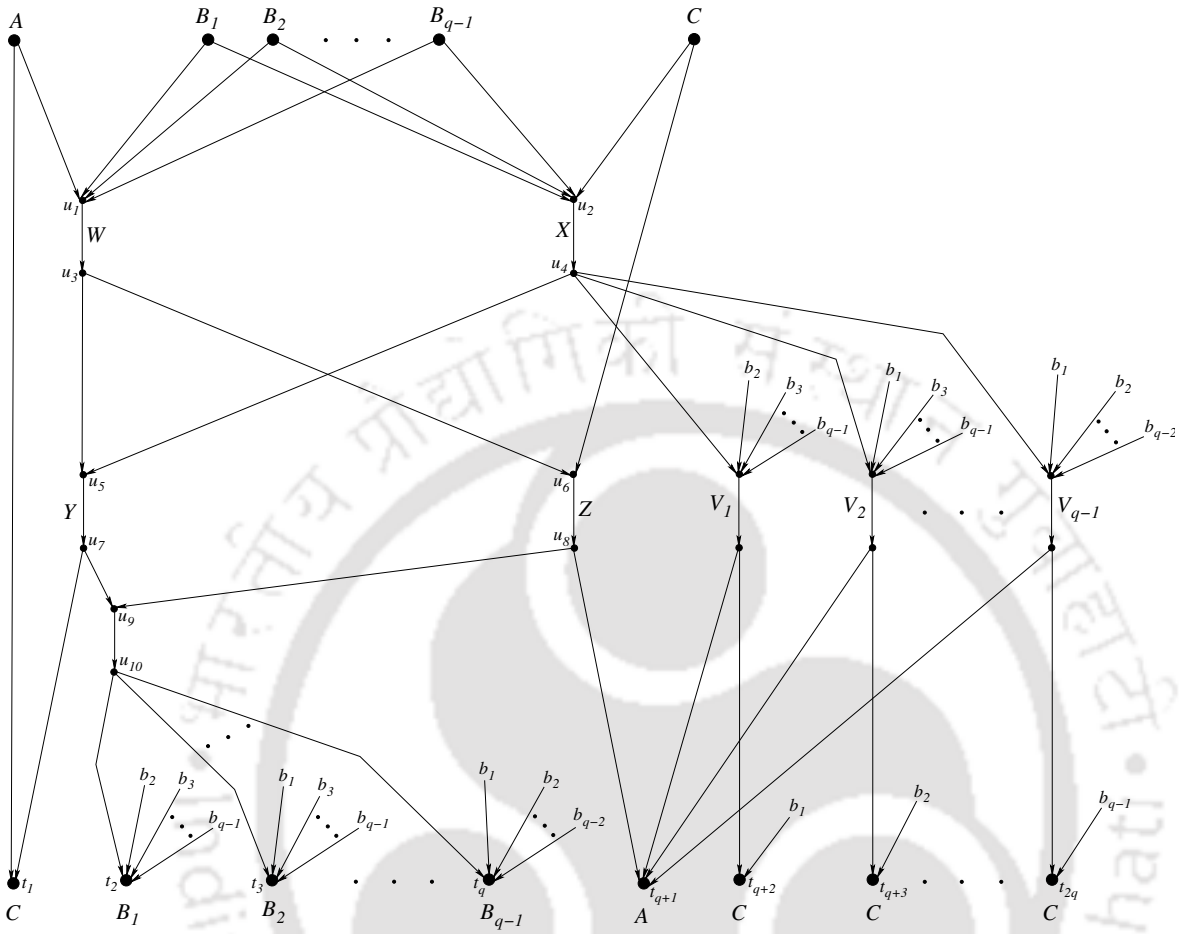

Figure 5.1: The characteristic-dependent linear rank inequality shown in equation (5.1) shows that the linear coding capacity of this network over finite fields whose characteristic does not divide q can be no more than $\frac{6(q-1)}{6(q-1)+1}$.

is some positive integer. Let u_i be the 1 dimensional vector space spanned by the $q+1$-length vector whose i^{th} element is 1 and all other elements are zero. Now, consider the following vector subspaces of V.

$$A = u_1 \qquad \text{for } 1 \le i \le q-1 : \; B_i = u_{i+1}$$

$$C = u_{q+1} \qquad W = \sum_{i=1}^{q} u_i$$

$$X = \sum_{i=2}^{q+1} u_i \qquad Y = u_1 - u_{q+1}$$

$$Z = \sum_{i=1}^{q} u_i - u_{q+1} \qquad \text{for } 1 \le i \le q-1 : \; V_i = u_{i+1} + u_{q+1}.$$

Now note that

$$V_i = X - \sum_{j=1, j\neq i}^{q} B_j \qquad Y = W - X \qquad Z = W - C \qquad C = V_i - B_i$$

$$A = A - qC = Z - \sum_{i=1}^{q-1} V_i \qquad C = A - Y \qquad B_i = Z - Y - \sum_{j=1, j\neq i}^{q-1} B_j.$$

With this setting, all the conditional terms in equation (5.1) becomes zero; and the inequality returns $(6q-5) \leq (6q-6)$, or, $6 \leq 5$, which is a contradiction. Hence the inequality in equation (5.1) is not valid over such a finite field.

5.1.1.1 Application of Inequality in Equation (5.1)

Consider the network shown in Fig. 5.1. Let us say that the network shown in Fig. 5.1 has a (k, n) fractional linear network coding solution over a finite field whose characteristic does not belong to $\{p_1, p_2, \ldots, p_l\}$. Then applying the characteristic-dependent linear rank inequality shown in equation (5.1), we have the following equation, (Fig. 5.1 shows the variables corresponding to the sources and the edges)

$$\begin{aligned} &(2q-1)k + \sum_{i=1}^{q-1} 2k + (2q-2)k \leq (q-1)(n+n+n+2n) + \sum_{i=1}^{q-1} n \\ &\text{or, } (6q-5)k \leq 6(q-1)n \\ &\text{or, } \frac{k}{n} \leq \frac{6(q-1)}{6(q-1)+1}. \end{aligned}$$

However, we do not know the tightness of this bound. For the case of $q = 2$, the network shown in Fig. 5.1 reduces to the well known Fano network, whose linear coding capacity over finite fields of odd characteristics is equal to 4/5 (proof given in [4] and [32]). But inequality (5.1) results an upper-bound equal to $\frac{6}{7}$.

5.1.2 Second Set of Inequalities

Theorem 41. *For any given set of primes $\{p_1, p_2, \ldots, p_l\}$, let $A, B_1, B_2, \ldots, B_q, V_1, V_2, \ldots, V_q, X, Y$ be vector subspaces of a finite dimensional vector space V where $q = p_1 \times p_2 \times \cdots \times p_l$. Then the following linear rank inequality holds if V is a vector space over a finite field whose characteristic*

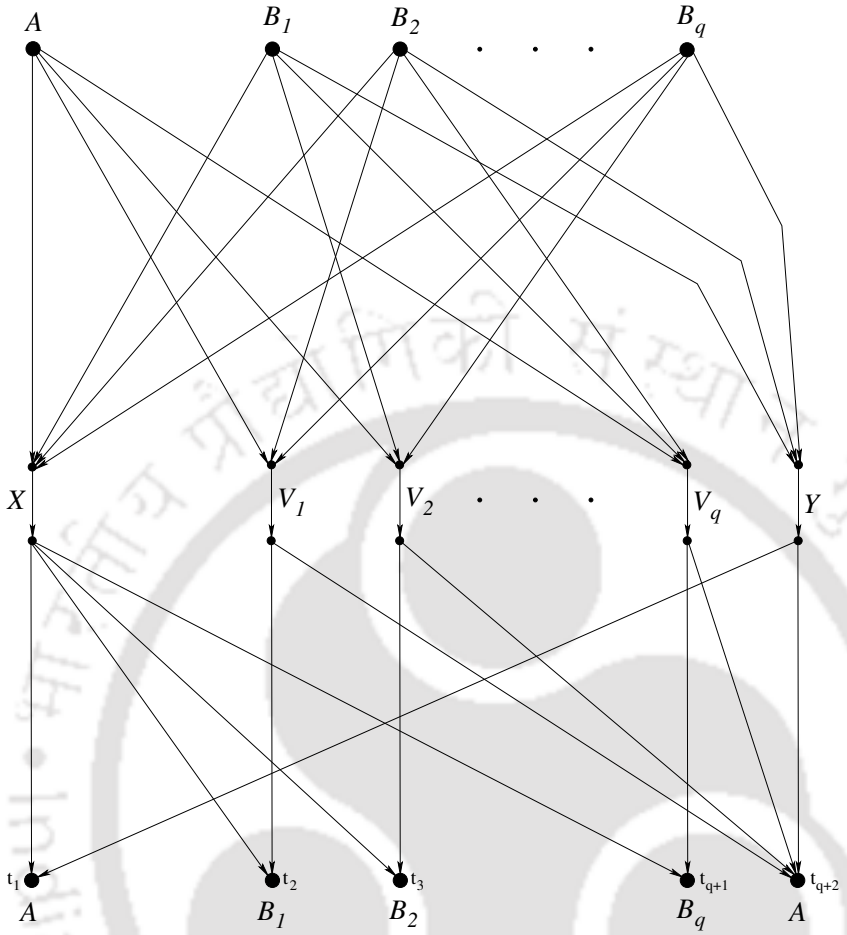

Figure 5.2: The characteristic-dependent linear rank inequality shown in equation (5.2) shows that the linear coding capacity of this network over finite fields whose characteristic divides q can be no more than $\frac{3q}{3q+1}$.

belongs to $\{p_1, p_2, \ldots, p_l\}$*, but may not hold otherwise:*

$$
\begin{aligned}
&2dim(A) + (q+1)dim(B_1) + \sum_{i=2}^{q} 2dim(B_i) \leq (2q-1)dim(X) + dim(Y) + \sum_{i=1}^{q} dim(V_i) \\
&+ dim(A|X,Y) + dim(A|V_1,\ldots,V_q,Y) + (q+1)dim(B_1|X,V_1) + \sum_{i=2}^{q} 2dim(B_i|X,V_i) \\
&+ (3q)dim(X|A,B_1,\ldots,B_q) + 2dim(Y|B_1,\ldots,B_q) + (q+2)dim(V_1|A,B_2,B_3,\ldots,B_q) \\
&+ \sum_{i=2}^{q} 3dim(V_i|A,B_1,\ldots,B_{i-1},B_{i+1},\ldots,B_q) \\
&+ (3q+1)(dim(A) + \sum_{j=1}^{q} dim(B_j) - dim(A,B_1,\ldots,B_q)). \qquad (5.2)
\end{aligned}
$$

The proof of the existence of the inequality is shown in Section 5.4. Note that the linear rank

inequality in equation (5.2) has $2q+3$ number of variables.

We here show that this inequality may not hold if q has an inverse over the finite field (which is equivalent to stating that the characteristic of the finite field does not belong to $\{p_1, p_2, \ldots, p_l\}$). Let V be $q+1$ dimensional vector space over $\mathbb{F}_{p^\alpha}$ where $p \notin \{p_1, p_2, \ldots, p_l\}$ and α is some positive integer. Let u_i be the 1 dimensional vector space spanned by the $q+1$-length vector whose i^{th} element is equal to 1 and all other elements are zero. Now, consider the following vector subspaces of V.

$$\text{for } 1 \leq i \leq q: \; B_i = u_{i+1} \qquad X = \sum_{i=1}^{q+1} u_i \qquad A = u_1$$

$$\text{for } 1 \leq i \leq q: \; V_i = \sum_{j=1, j\neq(i+1)}^{q+1} u_j \qquad Y = \sum_{i=2}^{q+1} u_i.$$

Now note

$$X = A + \sum_{i=1}^{q} B_i \qquad V_i = A + \sum_{j=1, j\neq i}^{q} B_i \qquad Y = \sum_{i=1}^{q} B_i$$

$$A = q^{-1}(\sum_{i=1}^{q} V_i - (q-1)Y) \qquad A = X - Y \qquad B_i = X - V_i.$$

Hence all the conditional terms in equation (5.2) becomes zero; and the inequality returns $(3q+1) \leq (3q)$, or, $1 \leq 0$, which is a contradiction.

5.1.2.1 Application of Inequality in Equation (5.2)

Consider the network shown in Fig. 5.2. Let us say that the network shown in Fig. 5.2 has a (k, n) fractional linear network coding solution over a finite field whose characteristic belongs to $\{p_1, p_2, \ldots, p_l\}$. Then applying the characteristic-dependent linear rank inequality shown in equation (5.2), we have the following equation, (Fig. 5.2 shows the variables corresponding to the sources and the edges)

$$\begin{aligned} & 2k + (q+1)k + \sum_{i=2}^{q} 2k \leq (2q-1)n + n + \sum_{i=1}^{q} n \\ & \text{or, } (3q+1)k \leq 3qn \\ & \text{or, } \frac{k}{n} \leq \frac{3q}{3q+1}. \end{aligned}$$

We do not know however how much tight this bound is. For the case of $q = 2$, the network shown in Fig. 5.2 reduces to the well known non-Fano network, whose linear coding capacity over finite fields

of even characteristics is equal to 5/6 (proved in [32]). But inequality (5.1) results an upper-bound equal to $\frac{6}{7}$.

5.1.3 Third Set of Inequalities

Theorem 42. *For any given set of primes $\{p_1, p_2, \ldots, p_l\}$, let $A, B_1, B_2, \ldots, B_q, V_1, V_2, \ldots, V_q$, X, Y be vector subspaces of a finite dimensional vector space V where $q = p_1 \times p_2 \times \cdots \times p_l$. Then the following linear rank inequality holds if V is a vector space over a finite field whose characteristic belongs to $\{p_1, p_2, \ldots, p_l\}$, but may not hold otherwise:*

$$\begin{aligned}
&(q+2)dim(A) + \sum_{i=1}^{q} 3dim(B_i) \leq (3q)dim(X) + dim(Y) + \sum_{i=1}^{q} dim(V_i) \\
&+ \sum_{i=1}^{q} 4dim(V_i|A, B_1, \ldots, B_{i-1}, B_{i+1}, \ldots, B_q) + (q+3)dim(Y|B_1, B_2, \ldots, B_q) \\
&+ dim(A|V_1, \ldots, V_q, Y) + (4q+2)dim(X|A, B_1, \ldots, B_q) + (q+2)dim(A|X, Y) \\
&+ \sum_{i=1}^{q} 3dim(B_i|X, V_i) + (4q+3)(dim(A) + \sum_{j=1}^{q} dim(B_j) - dim(A, B_1, \ldots, B_q)). \qquad (5.3)
\end{aligned}$$

The proof of the existence of the inequality is shown in Section 5.5. Note that the linear rank inequality in equation (5.3) has $2q+3$ number of variables. Let us show here this inequality may not hold if q has an inverse over the finite field (which is equivalent to stating that the characteristic of the finite field does not belong to $\{p_1, p_2, \ldots, p_l\}$). Let V be $q+1$ dimensional vector space over $\mathbb{F}_{p^\alpha}$ where $p \notin \{p_1, p_2, \ldots, p_l\}$ and α is some positive integer. Let u_i be the 1 dimensional vector space spanned by the $q+1$-length vector whose i^{th} element is equal to 1 and all other elements are zero. Now, consider the following vector subspaces of V.

$$A = u_1 \qquad \text{for } 1 \leq i \leq q: \ B_i = u_{i+1} \qquad Y = \sum_{i=2}^{q+1} u_i$$

$$X = \sum_{i=1}^{q+1} u_i \qquad \text{for } 1 \leq i \leq q: \ V_i = \sum_{j=1, j\neq(i+1)}^{q+1} u_j.$$

Now note

$$X = A + \sum_{i=1}^{q} B_i \qquad V_i = A + \sum_{j=1, j\neq i}^{q} B_i \qquad Y = \sum_{i=1}^{q} B_i$$

$$A = q^{-1}(\sum_{i=1}^{q} V_i - (q-1)Y) \qquad A = X - Y \qquad B_i = X - V_i.$$

Hence all the conditional terms in equation (5.2) becomes zero; and the inequality returns $(4q+2) \leq$

$(4q+1)$, or, $2 \leq 1$, which is a contradiction.

5.1.3.1 Application of Inequality in Equation (5.2)

Let us say that the network shown in Fig. 5.2 has a (k, n) fractional linear network coding solution over a finite field whose characteristic belongs to $\{p_1, p_2, \ldots, p_l\}$. Then applying the characteristic-dependent linear rank inequality shown in equation (5.2), we have the following equation: (Fig. 5.2 shows the variables corresponding to the sources and the edges)

$$\begin{aligned}
&(q+2)dim(A) + \sum_{i=1}^{q} 3dim(B_i) \leq (3q)dim(X) + dim(Y) + \sum_{i=1}^{q} dim(V_i) \\
&\text{or, } (4q+2)k \leq (4q+1)n \\
&\text{or, } \frac{k}{n} \leq \frac{4q+1}{4q+2}.
\end{aligned}$$

Note: In [32] the authors presented two characteristic-dependent linear rank inequalities. The second characteristic-dependent linear rank inequality inequality shown in [32] that holds over finite fields whose characteristic is equal to 2 is reproduced below in equation (5.4):

$$\begin{aligned}
&2H(A) + 3H(B) + 2H(C) \leq H(W) + H(X) + H(Y) + 3H(Z) + 2H(A|Y,Z) + 3H(B|X,Z) \\
&+ H(C|W,Z) + 2H(W|A,B) + 4H(X|A,C) + 3H(Y|B,C) + 6H(Z|A,B,C) + H(C|W,X,Y) \\
&+ 7(H(A) + H(B) + H(C)H(A,B,C)).
\end{aligned} \tag{5.4}$$

Over finite fields of characteristic 2, the characteristic-dependent linear rank inequality obtained from equation (5.2) is as follows:

$$\begin{aligned}
&2dim(A) + 3dim(B_1) + 2dim(B_2) \leq 3dim(X) + dim(Y) + dim(V_1) + dim(V_2) + dim(A|X,Y) \\
&+ dim(A|V_1,V_2,Y) + 3dim(B_1|X,V_1) + 2dim(B_2|X,V_2) + 6dim(X|A,B_1,B_2) + 2dim(Y|B_1,B_2) \\
&+ 4dim(V_1|A,B_2) + 3dim(V_2|A,B_1) + 7(dim(A) + dim(B_1) + dim(B_2) - dim(A,B_1,B_2)).
\end{aligned} \tag{5.5}$$

It can be seen that equation (5.5) is the same as equation (5.4) when in equation (5.4): A is replaced by B_2, B is replaced by B_1, C is replaced by A, Z is replaced by X, W is replaced by Y, X is replaced by V_1, and Y is replaced by V_2. As we will show, the proof of equation (5.2) is a generalization of the proof of equation (5.4).

5.2 A Note on the Proofs of the Inequalities (5.1), (5.2), and (5.3)

The authors of [32] developed a novel method where characteristic-dependent linear rank inequalities were yielded from the networks whose linear coding capacity is equal to 1 over some characteristics, but less than 1 over other characteristics. Hereafter, we will refer this method as the *DFZ method*. All of the inequalities in this chapter is derived using the DFZ method.

The idea behind the DFZ method is as follows. First - in accordance with the topology of the network - a set of vector subspaces, and a set of linear functions - that maps the aforementioned vector subspaces one to another - are constructed. Now, the network not having a rate 1 linear solution over a finite field means that if the dimensions of all the above considered vector subspaces are equal, then such a functional assignment won't exist (because if it had existed then the network would have a rate 1 linear solution). The DFZ method starts with these linear functions and tries to find an equation – relating the dimensions of the corresponding vector subspaces – that must hold true for such a functional assignment to exist over the finite filed. This equation is the desired inequality.

Now to obtain this equation, the DFZ method requires to find a subspace (denoted by S) that becomes a zero subspaces over the given finite field. This subspace must also be expressible as an intersection of other subspaces. Then, applying Lemma 6 (shown in Chapter 2) on S results the desired inequality. At present, all the steps of the DFZ method sans finding the set S is algorithmic. Intuitively, when S becomes the zero subspace, the dimension of the union of the subspaces whose intersection is equal to S increases (because the common set is null); thereby meaning that more information has to be sent. This 'more' information results the rate to be less than 1.

5.3 Proof of Inequality Shown in 5.1

Let V be a finite dimensional vector space and let $A, B_1, B_2, \ldots, B_{q-1}, C, V_1, V_2, \ldots, V_{q-1}, W$, X, Y, Z be subspaces of V for some positive integer q. We now list a set of functions that maps these subspaces one to another. The mapping of these functions is shown pictorially in Fig. 5.3.

for $1 \leq i \leq q-1 : f_{AV_i} : A \to V_i$

$f_{AZ} : A \to Z$

for $1 \leq i, j \leq q-1, j \neq i : f_{B_iB_j} B_i \to B_j$

for $1 \leq i \leq q-1 : f_{B_iY} : B_i \to Y$

for $1 \leq i \leq q-1 : f_{B_iZ} : B_i \to Z$

$f_{CA} : C \to A$

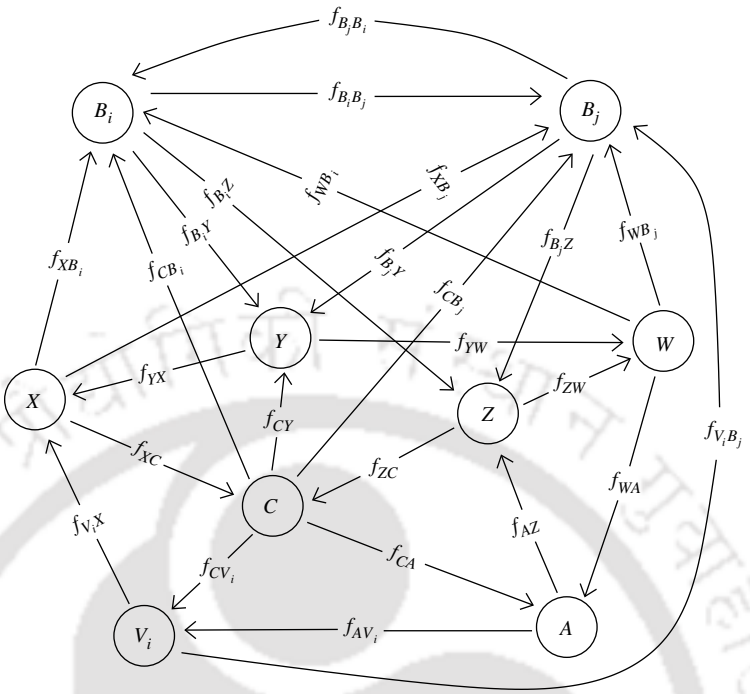

Figure 5.3: In this figure each circle with a label inside represents a vector subspace. We assume a set of mappings between these subspaces; these mappings are shown with an arrow directed from the domain to the co-domain (the mappings are shown for one particular values of i and j where $1 \leq i, j \leq q-1$, $i \neq j$).

for $1 \leq i \leq q-1 : f_{CB_i} : C \to B_i$

$f_{CY} : C \to Y$

for $1 \leq i \leq q-1 : f_{V_iX} : V_i \to X$

$f_{WA} : W \to A$

$f_{XC} : X \to C$

$f_{YX} : Y \to X$

$f_{ZW} : Z \to W.$

for $1 \leq i \leq q-1 : f_{CV_i} : C \to V_i$

for $1 \leq i, j \leq q-1, j \neq i : f_{V_iB_j} : V_i \to B_j$

for $1 \leq i \leq q-1 : f_{WB_i} : W \to B_i$

for $1 \leq i \leq q-1 : f_{XB_i} : X \to B_i$

$f_{YW} : Y \to W$

$f_{ZC} : Z \to C$

Due to Lemma 8, we have the following results.

(i) $\sum_{i=1}^{q-1} f_{AV_i} + f_{AZ} = I$ over a subspace A' of A where

$$codim_A(A') \leq dim(A|V_1, V_2, \ldots, V_{q-1}, Z) \tag{5.6}$$

(ii) for $1 \leq i \leq q-1$: $\sum_{j=1,j\neq i}^{q-1} f_{B_iB_j} + f_{B_iY} + f_{B_iZ} = I$ over a subspace B_i' of B_i where

$$codim_{B_i}(B_i') \leq dim(B_i|B_1, \ldots, B_{i-1}, B_{i+1}, \ldots, B_{q-1}, Y, Z) \tag{5.7}$$

(iii) $f_{CA} + f_{CY} = I$ over a subspace C' of C where

$$codim_C(C') \leq dim(C|A, Y) \tag{5.8}$$

(iv) for $1 \leq i \leq q-1$: $f_{CB_i} + f_{CV_i} = I$ over a subspace C_i of C where

$$codim_C(C_i) \leq dim(C|B_i, V_i) \tag{5.9}$$

(v) for $1 \leq i \leq q-1$: $\sum_{j=1,j\neq i}^{q-1} f_{V_iB_j} + f_{V_iX} = I$ over a subspace V_i' of V_i where

$$codim_{V_i}(V_i') \leq dim(V_i|B_1, \ldots, B_{i-1}, B_{i+1}, \ldots, B_{q-1}, X) \tag{5.10}$$

(vi) $f_{WA} + \sum_{i=1}^{q-1} f_{WB_i} = I$ over a subspace W' of W where

$$codim_W(W') \leq dim(W|A, B_1, B_2, \ldots, B_{q-1}) \tag{5.11}$$

(vii) $\sum_{i=1}^{q-1} f_{XB_i} + f_{XC} = I$ over a subspace X' of X where

$$codim_X(X') \leq dim(X|B_1, B_2, \ldots, B_{q-1}, C) \tag{5.12}$$

(viii) $f_{YW} + f_{YX} = I$ over a subspace Y' of Y where

$$codim_Y(Y') \leq dim(Y|W, X) \tag{5.13}$$

(ix) $f_{ZC} + f_{ZW} = I$ over a subspace Z' of Z where

$$codim_Z(Z') \leq dim(Z|C, W) \tag{5.14}$$

Now, let's consider the following composite functions:

$$f_{CA} + f_{WA}f_{YW}f_{CY} : C \to A \tag{5.15}$$

$$\text{for } 1 \leq i \leq q-1 : (f_{WB_i}f_{YW} + f_{XB_i}f_{YX})f_{CY} : C \to B_i \tag{5.16}$$

$$f_{XC}f_{YX}f_{CY} : C \to C. \tag{5.17}$$

Using (5.11), we have:

$$f_{WA}f_{YW}f_{CY} + \sum_{i=1}^{q-1} f_{WB_i}f_{YW}f_{CY} = f_{YW}f_{CY} \text{ over a subspace } f_{CY}^{-1}f_{YW}^{-1}(W') \text{ of } C. \tag{5.18}$$

Using (5.12), we have:

$$f_{XC}f_{YX}f_{CY} + \sum_{i=1}^{q-1} f_{XB_i}f_{YX}f_{CY} = f_{YX}f_{CY} \text{ over a subspace } f_{CY}^{-1}f_{YX}^{-1}(X') \text{ of } C. \tag{5.19}$$

Using (5.13), we have:

$$f_{YW}f_{CY} + f_{YX}f_{CY} = f_{CY} \text{ over a subspace } f_{CY}^{-1}(Y') \text{ of } C. \tag{5.20}$$

We now add functions shown in (5.15)-(5.17) and use equations (5.8), (5.18), (5.19), and (5.20).

$$\begin{aligned} & f_{WA}f_{YW}f_{CY} + \sum_{i=1}^{q-1} f_{WB_i}f_{YW}f_{CY} + f_{XC}f_{YX}f_{CY} + \sum_{i=1}^{q-1} f_{XB_i}f_{YX}f_{CY} + f_{CA} \\ &= f_{YW}f_{CY} + f_{YX}f_{CY} + f_{CA} \\ &= f_{CY} + f_{CA} \\ &= I \text{ over a subspace: } C'' = f_{CY}^{-1}f_{YW}^{-1}(W') \cap f_{CY}^{-1}f_{YX}^{-1}(X') \cap f_{CY}^{-1}(Y') \cap C' \text{ of } C. \end{aligned}$$

Using Lemma 6, we get:

$$codim_C(C'') \leq codim_C(f_{CY}^{-1}f_{YW}^{-1}(W')) + codim_C(f_{CY}^{-1}f_{YX}^{-1}(X')) + codim_C(f_{CY}^{-1}(Y')) + codim_C(C')$$

Using (7), we have:

$$codim_C(C'') \leq codim_W(W') + codim_X(X') + codim_Y(Y') + codim_C(C'). \tag{5.21}$$

Now, according to Lemma 9 there exists a subspace $\bar{C}$ of C'' over which:

$$f_{CA} + f_{WA}f_{YW}f_{CY} = 0 \tag{5.22}$$

$$\text{for } 1 \leq i \leq q-1 : (f_{WB_i}f_{YW} + f_{XB_i}f_{YX})f_{CY} = 0 \tag{5.23}$$

$$f_{XC}f_{YX}f_{CY} = -I. \tag{5.24}$$

$$\text{where } codim_{C''}(\bar{C}) \leq dim(A) + \sum_{i=1}^{q-1} dim(B_i) + dim(C) - dim(A, B_1, B_2, \ldots, B_{q-1}, C). \tag{5.25}$$

As $codim_C(\bar{C}) = codim_C C'' + codim_{C''}\bar{C}$, we have:

$$codim_C(\bar{C}) \leq codim_W(W') + codim_X(X') + codim_Y(Y') + codim_C(C') + dim(A) + \sum_{i=1}^{q-1} dim(B_i) + dim(C) - dim(A, B_1, B_2, \ldots, B_{q-1}, C). \tag{5.26}$$

Now, let's consider the following composite functions:

$$f_{WA}(f_{YW}f_{B_iY} + f_{ZW}f_{B_iZ}) : B_i \to A \tag{5.27}$$

$$(f_{WB_i}f_{YW} + f_{XB_i}f_{YX})f_{B_iY} + f_{WB_i}f_{ZW}f_{B_iZ} : B_i \to B_i \tag{5.28}$$

$$\text{for } 1 \leq j \leq q-1, j \neq i : (f_{WB_j}f_{YW} + f_{XB_j}f_{YX})f_{B_iY} + f_{WB_j}f_{ZW}f_{B_iZ} + f_{B_iB_j} : B_i \to B_j \tag{5.29}$$

$$f_{XC}f_{YX}f_{B_iY} + f_{ZC}f_{B_iZ} : B_i \to C. \tag{5.30}$$

Using equation (5.11), we have:

$$f_{WA}f_{YW}f_{B_iY} + \sum_{i=j}^{q-1} f_{WB_j}f_{YW}f_{B_iY} = f_{YW}f_{B_iY} \text{ over a subspace } f_{B_iY}^{-1}f_{YW}^{-1}(W') \text{ of } B_i. \tag{5.31}$$

Using equation (5.11), we have:

$$f_{WA}f_{ZW}f_{B_iZ} + \sum_{j=1}^{q-1} f_{WB_j}f_{ZW}f_{B_iZ} = f_{ZW}f_{B_iZ} \text{ over a subspace } f_{B_iZ}^{-1}f_{ZW}^{-1}(W') \text{ of } B_i. \tag{5.32}$$

Using equation (5.12), we have:

$$f_{XC}f_{YX}f_{B_iY} + \sum_{j=1}^{q-1} f_{XB_j}f_{YX}f_{B_iY} = f_{YX}f_{B_iY} \text{ over a subspace } f_{B_iY}^{-1}f_{YX}^{-1}(X') \text{ of } B_i. \tag{5.33}$$

Using equation (5.13), we have:

$$f_{YW}f_{B_iY} + f_{YX}f_{B_iY} = f_{B_iY} \text{ over a subspace } f_{B_iY}^{-1}(Y') \text{ of } B_i. \tag{5.34}$$

Using equation (5.13), we have:

$$f_{ZW}f_{B_iZ} + f_{ZC}f_{B_iZ} = f_{B_iZ} \text{ over a subspace } f_{B_iZ}^{-1}(Z') \text{ of } B_i. \tag{5.35}$$

Consider the subspace B_i'' of B_i where:

$$B_i'' = f_{B_iY}^{-1}f_{YW}^{-1}(W') \cap f_{B_iZ}^{-1}f_{ZW}^{-1}(W') \cap f_{B_iY}^{-1}f_{YX}^{-1}(X') \cap f_{B_iY}^{-1}(Y') \cap f_{B_iZ}^{-1}(Z') \cap B_i'. \tag{5.36}$$

Adding functions shown in (5.27)-(5.30) over B_i'' and using equations (5.7) and (5.31)-(5.35), we get:

$$\begin{aligned}
&f_{WA}(f_{YW}f_{B_iY} + f_{ZW}f_{B_iZ}) + sum_{j=1}^{q-1} f_{WB_j}f_{YW}f_{B_iY} + sum_{j=1}^{q-1} f_{XB_j}f_{YX}f_{B_iY} \\
&+ sum_{j=1}^{q-1} f_{WB_j}f_{ZW}f_{B_iZ} + sum_{j=1,j\neq i}^{q-1} f_{B_iB_j} + f_{XC}f_{YX}f_{B_iY} + f_{ZC}f_{B_iZ} \\
&= f_{YW}f_{B_iY} + f_{ZW}f_{B_iZ} + sum_{j=1,j\neq i}^{q-1} f_{B_iB_j} + f_{YX}f_{B_iY} + f_{ZC}f_{B_iZ} \\
&= f_{B_iY} + f_{B_iZ} + sum_{j=1,j\neq i}^{q-1} f_{B_iB_j} = I.
\end{aligned}$$

Then, according to Lemma 9 there exists a subspace $\bar{B}_i$ of B_i'' over which:

$$f_{WA}(f_{YW}f_{B_iY} + f_{ZW}f_{B_iZ}) = 0 \tag{5.37}$$

$$(f_{WB_i}f_{YW} + f_{XB_i}f_{YX})f_{B_iY} + f_{WB_i}f_{ZW}f_{B_iZ} - I = 0 \tag{5.38}$$

$$\text{for } 1 \leq j \leq q-1, j \neq i : (f_{WB_j}f_{YW} + f_{XB_j}f_{YX})f_{B_iY} + f_{WB_j}f_{ZW}f_{B_iZ} + f_{B_iB_j} = 0 \tag{5.39}$$

$$f_{XC}f_{YX}f_{B_iY} + f_{ZC}f_{B_iZ} = 0. \tag{5.40}$$

such that

$$codim_{B_i''}(\bar{B}_i) \leq dim(A) + \sum_{i=1}^{q-1} dim(B_i) + dim(C) - dim(A, B_1, B_2, \ldots, B_{q-1}, C). \tag{5.41}$$

Applying Lemma 6 to equation (5.36), we get:

$$\begin{aligned}
codim_{B_i}(B_i'') \leq\ & codim_{B_i}(f_{B_iY}^{-1}f_{YW}^{-1}(W')) + codim_{B_i}(f_{B_iZ}^{-1}f_{ZW}^{-1}(W')) + codim_{B_i}(f_{B_iY}^{-1}f_{YX}^{-1}(X')) \\
&+ codim_{B_i}(f_{B_iY}^{-1}(Y')) + codim_{B_i}(f_{B_iZ}^{-1}(Z')) + codim_{B_i}(B_i').
\end{aligned} \tag{5.42}$$

Applying Lemma 7 to equation (5.42), we get:

$$\begin{aligned}
codim_{B_i}(B_i'') \leq\ & codim_W(W') + codim_W(W') + codim_X(X') + codim_Y(Y') + codim_Z(Z') \\
&+ codim_{B_i}(B_i').
\end{aligned} \tag{5.43}$$

From equations (5.41) and (5.43), we get:

$$codim_{B_i}(\bar{B}_i) = codim_{B_i}(B_i'') + codim_{B_i''}(\bar{B}_i) \tag{5.44}$$

$$\leq 2codim_W(W') + codim_X(X') + codim_Y(Y') + codim_Z(Z') + codim_{B_i}(B_i') \tag{5.45}$$

$$+ dim(A) + \sum_{i=1}^{q-1} dim(B_i) + dim(C) - dim(A, B_1, B_2, \ldots, B_{q-1}, C). \tag{5.46}$$

Consider the following composite functions.

$$f_{WA}f_{ZW}f_{AZ} : A \to A \tag{5.47}$$

$$\text{for } 1 \leq i \leq q-1 : f_{WB_i}f_{ZW}f_{AZ} + f_{XB_i}f_{V_iX}f_{AV_i} + \sum_{j=1,j\neq i}^{q-1}(f_{XB_i}f_{V_jX} + f_{V_jB_i})f_{AV_j} : A \to B_i \tag{5.48}$$

$$f_{ZC}f_{AZ} + \sum_{j=1}^{q-1} f_{XC}f_{V_jX}f_{AV_j} : A \to C. \tag{5.49}$$

Using equation (5.11), we get:

$$f_{WA}f_{ZW}f_{AZ} + \sum_{i=1}^{q-1} f_{WB_i}f_{ZW}f_{AZ} = f_{ZW}f_{AZ} \text{ over a subspace } f_{AZ}^{-1}f_{ZW}^{-1}(W') \text{ of } A. \tag{5.50}$$

Using equation (5.12), we get:

$$\begin{aligned}
&\sum_{j=1}^{q-1} f_{XC}f_{V_jX}f_{AV_j} + \sum_{i=1}^{q-1}(f_{XB_i}(\sum_{j=1}^{q-1} f_{V_jX}f_{AV_j})) \\
&= f_{XC}\sum_{j=1}^{q-1} f_{V_jX}f_{AV_j} + (\sum_{i=1}^{q-1} f_{XB_i})(\sum_{j=1}^{q-1} f_{V_jX}f_{AV_j}) \\
&= \sum_{j=1}^{q-1} f_{V_jX}f_{AV_j} \text{ over a subspace}(\sum_{j=1}^{q-1} f_{V_jX}f_{AV_j})^{-1}(X') \text{ of } A.
\end{aligned} \tag{5.51}$$

Using equation (5.10), we get:

$$\begin{aligned}
&\sum_{j=1}^{q-1} f_{V_jX}f_{AV_j} + \sum_{i=1}^{q-1}\sum_{j=1,j\neq i}^{q-1} f_{V_jB_i}f_{AV_j} \\
&= \sum_{j=1}^{q-1} f_{V_jX}f_{AV_j} + \sum_{j=1}^{q-1}\sum_{i=1,i\neq j}^{q-1} f_{V_jB_i}f_{AV_j} \\
&= \sum_{j=1}^{q-1}(f_{V_jX} + \sum_{i=1,i\neq j}^{q-1} f_{V_jB_i})f_{AV_j} \\
&= \sum_{j=1}^{q-1} f_{AV_j} \text{ over a subspace } f_{AV_1}^{-1}(V_1') \cap f_{AV_2}^{-1}(V_2') \cap \cdots \cap f_{AV_{q-1}}^{-1}(V_{q-1}') \text{ of } A.
\end{aligned} \tag{5.52}$$

Using equation (5.14), we get:

$$f_{ZW}f_{AZ} + f_{ZC}f_{AZ} = f_{AZ} \text{ over a subspace } f_{AZ}^{-1}(Z') \text{ of } A. \tag{5.53}$$

Consider the following subspace A'' of A.

$$A'' = f_{AZ}^{-1}f_{ZW}^{-1}(W') \cap (\sum_{j=1}^{q-1} f_{V_jX}f_{AV_j})^{-1}(X') \cap f_{AV_1}^{-1}(V_1') \cap \cdots \cap f_{AV_{q-1}}^{-1}(V_{q-1}') \cap f_{AZ}^{-1}(Z') \cap A'. \tag{5.54}$$

Now adding the functions shown in equations (5.47)-(5.49) over A'' and using equations (5.6), (5.50), (5.51), (5.52), and (5.53), we get:

$$f_{WA}f_{ZW}f_{AZ} + \sum_{i=1}^{q-1}(f_{WB_i}f_{ZW}f_{AZ} + f_{XB_i}f_{V_iX}f_{AV_i} + \sum_{j=1,j\neq i}^{q-1}(f_{XB_i}f_{V_jX} + f_{V_jB_i})f_{AV_j}) + f_{ZC}f_{AZ} + \sum_{j=1}^{q-1} f_{XC}f_{V_jX}f_{AV_j}$$

$$= f_{ZW}f_{AZ} + \sum_{j=1}^{q-1} f_{V_jX}f_{AV_j} + \sum_{i=1}^{q-1}\sum_{j=1,j\neq i}^{q-1} f_{V_jB_i}f_{AV_j} + f_{ZC}f_{AZ}$$

$$= f_{AZ} + \sum_{j=1}^{q-1} f_{AV_j} = I. \tag{5.55}$$

Then, according to Lemma 9 there exists a subspace $\bar{A}$ of A'' over which:

$$f_{WA}f_{ZW}f_{AZ} - I = 0 \tag{5.56}$$

$$\text{for } 1 \leq i \leq q-1: \; f_{WB_i}f_{ZW}f_{AZ} + f_{XB_i}f_{V_iX}f_{AV_i} + \sum_{j=1,j\neq i}^{q-1}(f_{XB_i}f_{V_jX} + f_{V_jB_i})f_{AV_j} = 0 \tag{5.57}$$

$$f_{ZC}f_{AZ} + \sum_{j=1}^{q-1} f_{XC}f_{V_jX}f_{AV_j} = 0. \tag{5.58}$$

such that

$$codim_{A''}(\bar{A}) \leq dim(A) + dim(B_1) + dim(B_2) + \cdots + dim(B_{q-1}) + dim(C) - dim(A, B_1, B_2, \ldots, B_{q-1}, C). \tag{5.59}$$

Applying Lemma 6 to equation (5.54), we get:

$$codim_A(A'') \leq codim_A(f_{AZ}^{-1}f_{ZW}^{-1}(W')) + codim_A((\sum_{j=1}^{q-1} f_{V_jX}f_{AV_j})^{-1}(X')) + codim_A(f_{AV_1}^{-1}(V_1')) + \cdots + codim_A(f_{AV_{q-1}}^{-1}(V_{q-1}')) + codim_A(f_{AZ}^{-1}(Z')) + codim_A(A'). \tag{5.60}$$

Applying Lemma 7 to equation (5.60), we get:

$$codim_A(A'') \leq codim_W(W') + codim_X(X') + codim_{V_1}V_1') + \cdots + codim_{V_{q-1}}(V_{q-1}') + codim_Z(Z') + codim_A(A')$$

$$= codim_W(W') + codim_X(X') + \sum_{i=1}^{q-1} codim_{V_i}V_i') + codim_Z(Z') + codim_A(A'). \tag{5.61}$$

From equation (5.61) and (5.59), we have:

$$\begin{aligned} &codim_A(\bar{A}) = codim_A(A'') + codim_{A''}(\bar{A}) \\ &\leq codim_W(W') + codim_X(X') + \sum_{i=1}^{q-1} codim_{V_i} V_i') + codim_Z(Z') + codim_A(A') + dim(A) \\ &+ dim(B_1) + dim(B_2) + \cdots + dim(B_{q-1}) + dim(C) - dim(A, B_1, B_2, \ldots, B_{q-1}, C). \end{aligned} \tag{5.62}$$

For $1 \leq i \leq q-1$ consider the following composite functions. (note that these equations hold for each different values of i in the given range)

$$f_{XB_i} f_{V_iX} f_{CV_i} + f_{CB_i} : C \to B_i \tag{5.63}$$

$$\text{for } 1 \leq j \leq (q-1), j \neq i : \ (f_{XB_j} f_{V_iX} + f_{V_iB_j}) f_{CV_i} : C \to B_j \tag{5.64}$$

$$f_{XC} f_{V_iX} f_{CV_i} : C \to C. \tag{5.65}$$

Using equations (5.12), we have:

$$f_{XC} f_{V_iX} f_{CV_i} + \sum_{j=1}^{q-1} f_{XB_j} f_{V_iX} f_{CV_i} = f_{V_iX} f_{CV_i} \text{ over a subspace } f_{CV_i}^{-1} f_{V_iX}^{-1}(X') \text{ of } C. \tag{5.66}$$

Using equations (5.10), we have:

$$f_{V_iX} f_{CV_i} + \sum_{j=1, j\neq i}^{q-1} f_{V_iB_j} f_{CV_i} = f_{CV_i} \text{ over a subspace } f_{CV_i}^{-1}(V_i') \text{ of } C. \tag{5.67}$$

Consider a subspace C_i' where

$$C_i' = f_{CV_i}^{-1} f_{V_iX}^{-1}(X') \cap f_{CV_i}^{-1}(V_i') \cap C_i. \tag{5.68}$$

Over C_i' adding the functions shown in equations (5.63)-(5.65) and using equations (5.9), (5.66) and (5.67), we get:

$$\begin{aligned} &f_{XB_i} f_{V_iX} f_{CV_i} + f_{CB_i} + \sum_{j=1, j\neq i}^{q-1} (f_{XB_j} f_{V_iX} + f_{V_iB_j}) f_{CV_i} + f_{XC} f_{V_iX} f_{CV_i} \\ &= f_{V_iX} f_{CV_i} + f_{CB_i} + \sum_{j=1, j\neq i}^{q-1} f_{V_iB_j} f_{CV_i} \\ &= f_{CV_i} + f_{CB_i} = I. \end{aligned} \tag{5.69}$$

Applying Lemma 9 to equation (5.69), we get that over a subspace $\bar{C}_i$ we have:

$$f_{XB_i} f_{V_iX} f_{CV_i} + f_{CB_i} = 0 \tag{5.70}$$

$$\text{for } 1 \leq j \leq (q-1), j \neq i: \ (f_{XB_j} f_{V_iX} + f_{V_iB_j}) f_{CV_i} = 0 \tag{5.71}$$

$$f_{XC} f_{V_iX} f_{CV_i} - I = 0. \tag{5.72}$$

such that

$$codim_{C_i'}(\bar{C}_i) \leq dim(B_1) + dim(B_2) + \cdots + dim(B_{q-1}) + dim(C) - dim(B_1, B_2, \ldots, B_{q-1}, C). \tag{5.73}$$

Applying Lemma 6 to equation (5.68), we get:

$$codim_C(C_i') \leq codim_C(f_{CV_i}^{-1} f_{V_iX}^{-1}(X')) + codim_C(f_{CV_i}^{-1}(V_i')) + codim_C(C_i). \tag{5.74}$$

Applying Lemma 7 to equation (5.74), we get:

$$codim_C(C_i') \leq codim_X(X') + codim_{V_i}(V_i') + codim_C(C_i). \tag{5.75}$$

From equations (5.73) and (5.75), we get:

$$codim_C(\bar{C}_i) = codim_C(C_i') + codim_{C_i'}(\bar{C}_i) \leq codim_X(X') + codim_{V_i}(V_i') + codim_C(C_i) + dim(B_1) + dim(B_2) + \cdots + dim(B_{q-1}) + dim(C) - dim(B_1, B_2, \ldots, B_{q-1}, C). \tag{5.76}$$

Consider the following vector subspaces.

$$\text{for } 1 \leq i \leq q-1: \ S_{B_i} = \{u \in B_i | f_{B_iY}(u) \in f_{CY}(\bar{C})\}. \tag{5.77}$$

Hence, equation (5.23) holds over S_{B_i} when f_{CY} is replaced by f_{B_iY}. So over S_{B_i} we have:

$$\text{for } 1 \leq i \leq (q-1): (f_{WB_i} f_{YW} + f_{XB_i} f_{YX}) f_{B_iY} = 0 \tag{5.78}$$

Since equation (5.38) holds over $\bar{B}_i$, from equations (5.38) and (5.78), over a subspace $\bar{B}_i \cap S_{B_i}$ we have:

$$f_{WB_i} f_{ZW} f_{B_iZ} = I \tag{5.79}$$

Now consider the following subspaces.

$$\text{for } 1 \leq i \leq q-1: \ R_{B_i} = \{u \in B_i | f_{B_iZ}(u) \in f_{AZ}(\bar{A})\}$$

$$\text{for } 1 \leq i \leq q-1: \ L_{B_i} = \{u \in B_i | f_{YW} f_{B_iY}(u) \in f_{ZW} f_{AZ}(\bar{A})\}.$$

So $f_{B_iZ}(R_{B_i})$ is a subspace of $f_{AZ}(\bar{A})$. Then, since from equation (5.56) f_{WA} is invertible over $f_{ZW}f_{AZ}(\bar{A})$; f_{WA} is also invertible over $f_{ZW}f_{B_iZ}(R_{B_i})$. Similarly, $f_{YW}f_{B_iY}(L_{B_i})$ is a subspace of $f_{ZW}f_{AZ}(\bar{A})$. Hence f_{WA} is also invertible over $f_{YW}f_{B_iY}(L_{B_i})$. Hence over a subspace $R_{B_i} \cap L_{B_i}$ from equation (5.37) we have:

$$f_{YW}f_{B_iY} + f_{ZW}f_{B_iZ} = 0 \tag{5.80}$$

Applying this equation in equation (5.38), over a subspace $\bar{B}_i \cap R_{B_i} \cap L_{B_i}$ we have:

$$f_{XB_i}f_{YX}f_{B_iY} = I \tag{5.81}$$

Now consider the following subspace:

$$\text{for } 1 \leq i \leq q-1 : \; S_{A_i} = \{u \in A | f_{AV_i}(u) \in f_{CV_i}(\bar{C}_i)\}.$$

Hence for $1 \leq i,j \leq (q-1), j \neq i$, $(f_{XB_j}f_{V_iX} + f_{V_iB_j})f_{AV_i}(S_{A_i})$ is a subspace of $(f_{XB_j}f_{V_iX} + f_{V_iB_j})f_{CV_i}(\bar{C}_i)$. Hence from equation (5.71), over S_{A_i} we have:

$$\text{for } 1 \leq j \leq (q-1), j \neq i : \; (f_{XB_j}f_{V_iX} + f_{V_iB_j})f_{AV_i} = 0 \tag{5.82}$$

Applying equation (5.82) on equation (5.57), over a subspace $\cap_{i=1}^{q-1} S_{A_i} \cap \bar{A}$ we have:

$$\text{for } 1 \leq j \leq q-1 : \; f_{WB_j}f_{ZW}f_{AZ} + f_{XB_j}f_{V_jX}f_{AV_j} = 0 \tag{5.83}$$

Let us now consider the following subspaces:

$$\text{for } 1 \leq i \leq q-1 : \; L_{A_i} = \{u \in A | f_{AZ}(u) \in (\bar{B}_i \cap S_{B_i})\} \tag{5.84}$$

$$\text{for } 1 \leq i \leq q-1 : \; R_{A_i} = \{u \in A | f_{V_iX}f_{AV_i}(u) \in f_{YX}f_{B_iY}(\bar{B}_i \cap R_{B_i} \cap L_{B_i})\} \tag{5.85}$$

$$S = \bar{A} \cap (\cap_{i=1}^{q-1} L_{A_i}) \cap (\cap_{i=1}^{q-1} R_{A_i}) \cap (\cap_{i=1}^{q-1} S_{A_i}). \tag{5.86}$$

For any $a \in S$, from equation (5.58), we have:

$$f_{ZC}f_{AZ}(a) + \sum_{i=1}^{q-1} f_{XC}f_{V_iX}f_{AV_i}(a) = 0$$

From (5.85) we know there exists a $b_i \in (\bar{B}_i \cap R_{B_i} \cap L_{B_i})$ such that $f_{V_iX}f_{R_i}(a) = f_{YX}f_{B_iY}(b_i)$

So, $f_{ZC}f_{AZ}(a) + \sum_{i=1}^{q-1} f_{XC}f_{YX}f_{B_iY}(b_i) = 0$

From equation (5.81) we know that $b_i = f_{XB_i}f_{YX}f_{B_iY}(b_i)$ for any $b_i \in (\bar{B}_i \cap R_{B_i} \cap L_{B_i})$. So,

$$f_{ZC}f_{AZ}(a) + \sum_{i=1}^{q-1} f_{XC}f_{YX}f_{B_iY}f_{XB_i}f_{YX}f_{B_iY}(b_i) = 0$$

or, $f_{ZC}f_{AZ}(a) + \sum_{i=1}^{q-1} f_{XC}f_{YX}f_{B_iY}f_{XB_i}f_{V_iX}f_{AV_i}(a) = 0$

Using equation (5.83), we have:

$$f_{ZC}f_{AZ}(a) - \sum_{i=1}^{q-1} f_{XC}f_{YX}f_{B_iY}f_{WB_i}f_{ZW}f_{AZ}(a) = 0$$

From (5.84) we know there exists a $b_i' \in (\bar{B}_i \cap S_{B_i})$ such that $f_{AZ}(a) = f_{B_iZ}(b_i')$. So,

$$f_{ZC}f_{AZ}(a) - \sum_{i=1}^{q-1} f_{XC}f_{YX}f_{B_iY}f_{WB_i}f_{ZW}f_{B_iZ}(b_i') = 0$$

From equation (5.79) we know that $b_i' = f_{WB_i}f_{ZW}f_{B_iZ}(b_i')$ for any $b_i' \in (\bar{B}_i \cap S_{B_i})$. So,

$$f_{ZC}f_{AZ}(a) - \sum_{i=1}^{q-1} f_{XC}f_{YX}f_{B_iY}(b_i') = 0. \tag{5.87}$$

Since $b_i' \in \bar{B}_i$, using equation (5.40) in equation (5.87), we have:

$$f_{ZC}f_{AZ}(a) + \sum_{i=1}^{q-1} f_{ZC}f_{B_iZ}(b_i') = 0$$

$$\text{or, } f_{ZC}f_{AZ}(a) + \sum_{i=1}^{q-1} f_{ZC}f_{AZ}(a) = 0$$

$$qf_{ZC}f_{AZ}(a) = 0. \tag{5.88}$$

We now argue that for equation (5.88) to hold for any $a \in S$, S must be a zero subspace. From equation (5.56) we know that f_{AZ} is one-to-one over $\bar{A}$. From equation (5.77) we know that $f_{B_iY}(S_{B_i})$ for $1 \leq i \leq (q-1)$ is a subspace of $f_{CY}(\bar{C})$. Because of equation (5.24), $f_{XC}f_{YX}$ is one-to-one over $f_{CY}(\bar{C})$. So $f_{XC}f_{YX}$ is also one-to-one over $f_{B_iY}(S_{B_i})$. Then, from equation (5.40) it can be concluded that $f_{ZC}f_{B_iZ}$ is one-to-one over S_{B_i}. Now, from (5.84) we know $f_{AZ}(S)$ is a subspace of $f_{B_iZ}(\bar{B}_i \cap S_{B_i})$ for any $1 \leq i \leq q-1$. So f_{ZC} is one-to-one over $f_{AZ}(S)$. Moreover, as a pre-condition, since the characteristic of the finite field does not belong to $\{p_1, p_2, \ldots, p_l\}$, $q \neq 0$ over the finite field. Hence for equation (5.88) to hold, S must be a zero subspace. Now,

$$dim(A) = dim(A) - dim(S) = codim_A(S) = codim_A(\bar{A} \cap (\cap_{i=1}^{q-1} L_{A_i}) \cap (\cap_{i=1}^{q-1} R_{A_i}) \cap (\cap_{i=1}^{q-1} S_{A_i}))$$

Applying Lemma 6, we have:

$$dim(A) \leq codim_A(\bar{A}) + \sum_{i=1}^{q-1} codim_A(L_{A_i}) + \sum_{i=1}^{q-1} codim_A(R_{A_i}) + \sum_{i=1}^{q-1} codim_A(S_{A_i}). \tag{5.89}$$

We now calculate some values that would help us in computing a bound over $dim(A)$.

$codim_{B_i}(S_{B_i}) = codim_{B_i}(f^{-1}_{B_iY}(f_{CY}(\bar{C})))$

Applying Lemma 7; and noting that from equation (5.24) f_{CY} is one-to-one over $\bar{C}$, we have:

$codim_{B_i}(S_{B_i}) \leq codim_Y(f_{CY}(\bar{C})) = dim(Y) - dim(f_{CY}(\bar{C})) = dim(Y) - dim(\bar{C})$

or, $codim_{B_i}(S_{B_i}) \leq dim(Y) + codim_C(\bar{C}) - dim(C)$. (5.90)

$codim_{B_i}(R_{B_i}) = codim_{B_i}(f^{-1}_{B_iZ}(f_{AZ}(\bar{A})))$

Applying Lemma 7; and noting that from equation (5.56) f_{AZ} is one-to-one over $\bar{A}$, we have:

$codim_{B_i}(R_{B_i}) \leq codim_Z(f_{AZ}(\bar{A})) = dim(Z) - dim(f_{AZ}(\bar{A})) = dim(Z) - dim(\bar{A})$

or, $codim_{B_i}(R_{B_i}) \leq dim(Z) + codim_A(\bar{A}) - dim(A)$. (5.91)

$codim_{B_i}(L_{B_i}) = codim_{B_i}(f^{-1}_{B_iY} f^{-1}_{YW}(f_{ZW} f_{AZ}(\bar{A})))$

Applying Lemma 7, and since from equation (5.56) $f_{ZW} f_{AZ}$ is one-to-one over $\bar{A}$, we have:

$codim_{B_i}(L_{B_i}) \leq codim_W(f_{ZW} f_{AZ}(\bar{A})) = dim(W) - dim(f_{ZW} f_{AZ}(\bar{A})) = dim(W) - dim(\bar{A})$

or, $codim_{B_i}(L_{B_i}) \leq dim(W) + codim_A(\bar{A}) - dim(A)$. (5.92)

$codim_A(S_{A_i}) = codim_A(f^{-1}_{AV_i}(f_{CV_i}(\bar{C}_i)))$

Applying Lemma 7; and noting from equation (5.72) that f_{CV_i} is one-to-one over $\bar{C}$, we have:

$codim_A(S_{A_i}) \leq codim_{V_i}(f_{CV_i}(\bar{C}_i)) = dim(V_i) - dim(f_{CV_i}(\bar{C}_i)) = dim(V_i) - dim(\bar{C}_i)$

or, $codim_A(S_{A_i}) \leq dim(V_i) + codim_C(\bar{C}_i) - dim(C)$. (5.93)

$codim_A(R_{A_i}) = codim_A(f^{-1}_{AV_i} f^{-1}_{V_iX}(f_{YX} f_{B_iY}(\bar{B}_i \cap R_{B_i} \cap L_{B_i})))$

Applying Lemma 7, we have:

$codim_A(R_{A_i}) \leq codim_X(f_{YX} f_{B_iY}(\bar{B}_i \cap R_{B_i} \cap L_{B_i}))$

$= dim(X) - dim(f_{YX} f_{B_iY}(\bar{B}_i \cap R_{B_i} \cap L_{B_i}))$

From equation (5.81) we know that $f_{YX} f_{B_iY}$ is one-to-one over $\bar{B}_i \cap R_{B_i} \cap L_{B_i}$. So,

$codim_A(R_{A_i}) \leq dim(X) - dim(\bar{B}_i \cap R_{B_i} \cap L_{B_i})$

$= dim(X) + codim_{B_i}(\bar{B}_i \cap R_{B_i} \cap L_{B_i}) - dim(B_i)$

Applying Lemma 6 and then substituting $codim_{B_i}(R_{B_i})$ and $codim_{B_i}(L_{B_i})$ from equations (5.91) and (5.92), we have:

$$codim_A(R_{A_i}) \leq dim(X) + codim_{B_i}(\bar{B}_i) + codim_{B_i}(R_{B_i}) + codim_{B_i}(L_{B_i}) - dim(B_i)$$

$$\text{or, } codim_A(R_{A_i}) \leq dim(X) + codim_{B_i}(\bar{B}_i) + dim(Z) + codim_A(\bar{A}) - dim(A) + dim(W) + codim_A(\bar{A}) - dim(A) - dim(B_i)$$

$$\text{or, } codim_A(R_{A_i}) \leq dim(W) + dim(X) + dim(Z) + codim_{B_i}(\bar{B}_i) + 2codim_A(\bar{A}) - 2dim(A) - dim(B_i). \quad (5.94)$$

$codim_A(L_{A_i}) = codim_A(f_{AZ}^{-1}(f_{B_iZ}(\bar{B}_i \cap S_{B_i})))$

Applying Lemma 7, we have:

$codim_A(L_{A_i}) \leq codim_Z(f_{B_iZ}(\bar{B}_i \cap S_{B_i})) = dim(Z) - dim(f_{B_iZ}(\bar{B}_i \cap S_{B_i}))$

From equation (5.79) we know that f_{B_iZ} is one-to-one over $\bar{B}_i \cap S_{B_i}$. So,

$codim_A(L_{A_i}) \leq dim(Z) - dim(\bar{B}_i \cap S_{B_i}) = dim(Z) + codim_{B_i}(\bar{B}_i \cap S_{B_i}) - dim(B_i)$

Applying Lemma 6 and then substituting $codim_{B_i}(S_{B_i})$ from equation (5.90), we have:

$codim_A(L_{A_i}) \leq dim(Z) + codim_{B_i}(\bar{B}_i) + codim_{B_i}(S_{B_i}) - dim(B_i)$

$$\text{or, } codim_A(L_{A_i}) \leq dim(Z) + codim_{B_i}(\bar{B}_i) + dim(Y) + codim_C(\bar{C}) - dim(C) - dim(B_i). \quad (5.95)$$

Substituting equation (5.95), (5.94), and (5.93) in equation (5.89), we have:

$$dim(A) \leq (q-1)(dim(W) + dim(X) + dim(Y) + 2dim(Z)) + \sum_{i=1}^{q-1} dim(V_i) - 2(q-1)dim(A) - 2(q-1)dim(C) - \sum_{i=1}^{q-1} 2dim(B_i) + (2q-1)codim_A(\bar{A}) + (q-1)codim_C(\bar{C}) + \sum_{i=1}^{q-1} 2codim_{B_i}(\bar{B}_i) + \sum_{i=1}^{q-1} codim_C(\bar{C}_i). \quad (5.96)$$

Now substituting equations (5.26), (5.46), (5.62) and (5.76) in equation (5.96), we have:

$$dim(A) \leq (q-1)(dim(W)+dim(X)+dim(Y)+2dim(Z)) + \sum_{i=1}^{q-1} dim(V_i) - 2(q-1)dim(A)$$
$$- 2(q-1)dim(C) - \sum_{i=1}^{q-1} 2dim(B_i) + (7q-6)codim_W(W') + (6q-5)codim_X(X')$$
$$+ \sum_{i=1}^{q-1}(2q)codim_{V_i}(V_i') + (3q-3)codim_Y(Y') + (4q-3)codim_Z(Z') + (2q-1)codim_A(A')$$
$$+ (q-1)codim_C(C') + \sum_{i=1}^{q-1} 2codim_B(B_i') + \sum_{i=1}^{q-1} codim_C(C_i')$$
$$+ (5q-4)(dim(A) - dim(A, B_1, \ldots, B_{q-1}, C))$$
$$+ (6q-5)(\sum_{i=1}^{q-1} dim(B_i) + dim(C)) - (q-1)dim(B_1, \ldots, B_{q-1}, C).$$

Substituting values from equations (5.11), (5.12), (5.10), (5.13), (5.14), (5.6), (5.7), (5.8), and (5.9), we get:

$$dim(A) \leq (q-1)(dim(W)+dim(X)+dim(Y)+2dim(Z)) + \sum_{i=1}^{q-1} dim(V_i) - 2(q-1)dim(A)$$
$$- 2(q-1)dim(C) - \sum_{i=1}^{q-1} 2dim(B_i) + (7q-6)dim(W|A, B_1, \ldots, B_{q-1})$$
$$+ (6q-5)dim(X|B_1, \ldots, B_{q-1}, C) + \sum_{i=1}^{q-1}(2q)dim(V_i|X, \cup_{j=1, j\neq i}^{q-1} B_j) + (3q-3)dim(Y|W, X)$$
$$+ (4q-3)dim(Z|W, C) + (2q-1)dim(A|Z, V_1, \ldots, V_{q-1}) + (q-1)dim(C|A, Y)$$
$$+ \sum_{i=1}^{q-1} 2dim(B_i|B_1, \ldots, B_{i-1}, B_{i+1}, \ldots, B_{q-1}, Y, Z) + \sum_{i=1}^{q-1} dim(C|V_i, B_i)$$
$$+ (5q-4)(dim(A) - dim(A, B_1, \ldots, B_{q-1}, C))$$
$$+ (6q-5)(\sum_{i=1}^{q-1} dim(B_i) + dim(C)) - (q-1)dim(B_1, \ldots, B_{q-1}, C).$$

5.4 Proof of the Inequality Shown in Equation (5.2)

This proof is a generalization of the proof of inequality (66) of Theorem 15 presented in [32]. Let V be a finite dimensional vector space and let $A, B_1, B_2, \ldots, B_q, V_1, V_2, \ldots, V_q, X, Y$ be subspaces of V for some positive integer q. We now list a set of functions that maps these subspaces one to another. These mappings are shown pictorially in Fig. 5.4 for some particular value of i and j.

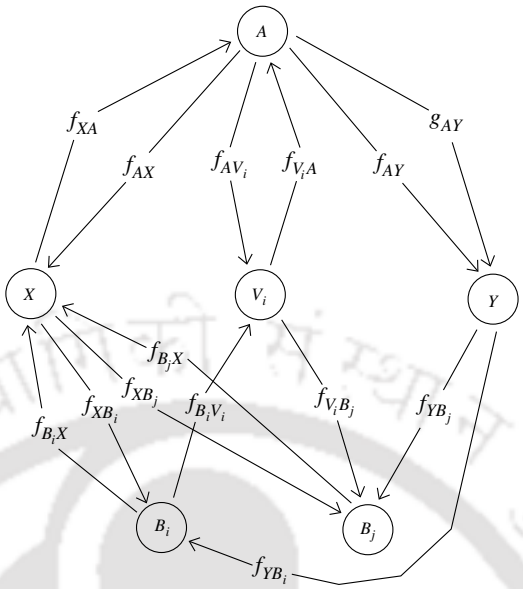

Figure 5.4: In this figure each circle with a label inside represents a vector subspace. We assume a set of mappings between these subspaces; these mappings are shown with an arrow directed from the domain to the co-domain (note that these mappings are shown for a particular value of i and j, and holds for every value if i and j where $1 \leq i, j \leq q,\ j \neq i$).

$f_{AX} : A \rightarrow X$ $\quad$ $f_{AY} : A \rightarrow Y$

$g_{AY} : A \rightarrow Y$ $\quad$ for $1 \leq i \leq q:\ f_{AV_i} : A \rightarrow V_i$

for $1 \leq i \leq q:\ f_{B_iX} : B_i \rightarrow X$ $\quad$ $f_{B_iV_i} : B_i \rightarrow V_i$

$f_{XA} : X \rightarrow A$ $\quad$ for $1 \leq i \leq q:\ f_{XB_i} : X \rightarrow B_i$

for $1 \leq i \leq q:\ f_{YB_i} : Y \rightarrow B_i$ $\quad$ for $1 \leq i \leq q:\ f_{V_iA} : V_i \rightarrow A$

for $1 \leq i, j \leq q, j \neq i:\ f_{V_iB_j} : V_i \rightarrow B_j$.

Due to Lemma 8, the following holds:

$$f_{XA} + \sum_{i=1}^{q} f_{XB_i} = I \text{ over a subspace } X' \text{ of } X \text{ where } codim_X(X') \leq dim(X|A, B_1, \ldots, B_q) \quad (5.97)$$

$$f_{V_iA} + \sum_{j=1, j\neq i}^{q} f_{V_iB_j} = I \text{ over a subspace } V_i' \text{ of } V_i \text{ where}$$
$$codim_{V_i}(V_i') \leq dim(V_i|A, B_1, \ldots, B_{i-1}, B_{i+1}, \ldots, B_q) \quad (5.98)$$

$$\sum_{i=1}^{q} f_{YB_i} = I \text{ over a subspace } Y' \text{ of } Y \text{ where } codim_Y(Y') \leq dim(Y|B_1, \ldots, B_q) \quad (5.99)$$

$$f_{AX} + f_{AY} = I \text{ over a subspace } A' \text{ of } A \text{ where } codim_A(A') \leq dim(A|X, Y) \quad (5.100)$$

$$\sum_{i=1}^{q} f_{AV_i} + g_{AY} = I \text{ over a subspace } A'' \text{ of } A \text{ where } codim_A(A'') \leq dim(A|V_1, \ldots, V_q, Y) \quad (5.101)$$

for $1 \leq i \leq q$: $f_{B_iX} + f_{B_iV_i} = I$ over a subspace B_i' of B_i where

$$codim_{B_i}(B_i') \leq dim(B_i|X, V_i). \quad (5.102)$$

Consider the following composite functions.

$$f_{XA}f_{AX} : A \to A \quad (5.103)$$

$$\text{for } 1 \leq i \leq q : f_{XB_i}f_{AX} + f_{YB_i}f_{AY} : A \to B_i. \quad (5.104)$$

Using equation (5.97), we have:

$$f_{XA}f_{AX} + \sum_{i=1}^{q} f_{XB_i}f_{AX} = f_{AX} \text{ over a subspace } f_{AX}^{-1}(X') \text{ of } A. \quad (5.105)$$

Using equation (5.99), we have:

$$\sum_{i=1}^{q} f_{YB_i}f_{AY} = f_{AY} \text{ over a subspace } f_{AY}^{-1}(Y') \text{ of } A. \quad (5.106)$$

Consider a subspace A''' where

$$A''' = f_{AX}^{-1}(X') \cap f_{AY}^{-1}(Y') \cap A'. \quad (5.107)$$

Summing the functions shown in equations (5.103) and (5.104), we have

$$f_{XA}f_{AX} + \sum_{i=1}^{q}(f_{XB_i}f_{AX} + f_{YB_i}f_{AY})$$
$$= f_{AX} + f_{AY} = I \text{ over a subspace } A''' \text{ of } A. \quad (5.108)$$

So, due to Lemma 9 there exists a subspace $\bar{A}$ of A''' over which:

$$f_{XA}f_{AX} - I = 0 \quad (5.109)$$

$$\text{for } 1 \leq i \leq q : f_{XB_i}f_{AX} + f_{YB_i}f_{AY} = 0. \quad (5.110)$$

$$\text{where } codim_{A'''}(\bar{A}) \leq dim(A) + \sum_{i=1}^{q} dim(B_i) - dim(A, B_1, \ldots, B_q). \quad (5.111)$$

Applying Lemma 6 to equation (5.107), we get:

$$codim_A(A''') \leq codim_A(f_{AX}^{-1}(X')) + codim_A(f_{AY}^{-1}(Y')) + codim_A(A'). \quad (5.112)$$

Applying Lemma 7 to equation (5.112), we get:

$$codim_A(A''') \leq codim_X(X') + codim_Y(Y') + codim_A(A'). \tag{5.113}$$

From equations (5.113) and (5.111), we have:

$$codim_A(\bar{A}) = codim_A(A''') + codim_{A'''}(\bar{A}) \leq codim_X(X') + codim_Y(Y') + codim_A(A') + dim(A) + \sum_{i=1}^{q} dim(B_i) - dim(A, B_1, \ldots, B_q). \tag{5.114}$$

Now, for each value of $1 \leq i \leq q$, consider the following composite functions.

$$f_{XA}f_{B_iX} + f_{V_iA}f_{B_iV_i} : B_i \to A \tag{5.115}$$

$$f_{XB_i}f_{B_iX} : B_i \to B_i \tag{5.116}$$

$$\text{for } 1 \leq j \leq q, j \neq i : \ f_{XB_j}f_{B_iX} + f_{V_iB_j}f_{B_iV_i} : B_i \to B_j. \tag{5.117}$$

Using equation (5.97), we have:

$$f_{XA}f_{B_iX} + \sum_{j=1}^{q} f_{XB_j}f_{B_iX} = f_{B_iX} \text{ over a subspace } f^{-1}_{B_iX}(X') \text{ of } B_i. \tag{5.118}$$

Using equation (5.98), we have:

$$f_{V_iA}f_{B_iV_i} + \sum_{j=1, j\neq i}^{q} f_{V_iB_j}f_{B_iV_i} = f_{B_iV_i} \text{ over a subspace } f^{-1}_{B_iV_i}(V_i') \text{ of } V_i. \tag{5.119}$$

Consider the following subspace

$$B_i'' = f^{-1}_{B_iX}(X') \cap f^{-1}_{B_iV_i}(V_i') \cap B_i'. \tag{5.120}$$

Summing the functions shown in equations (5.115)-(5.117) over B_i'', we get:

$$\begin{aligned}
&f_{XA}f_{B_iX} + f_{V_iA}f_{B_iV_i} + f_{XB_i}f_{B_iX} + \sum_{j=1, j\neq i}^{q} (f_{XB_j}f_{B_iX} + f_{V_iB_j}f_{B_iV_i}) \\
&= f_{XA}f_{B_iX} + \sum_{j=1}^{q} f_{XB_j}f_{B_iX} + f_{V_iA}f_{B_iV_i} + \sum_{j=1, j\neq i}^{q} f_{V_iB_j}f_{B_iV_i} \\
&= f_{B_iX} + f_{B_iV_i} \qquad \text{[from equations (5.118) and (5.119)]} \\
&= I.
\end{aligned}$$

So according to Lemma 9 there exists a subspace $\bar{B}_i$ over which the following identities hold:

$$f_{XA}f_{B_iX} + f_{V_iA}f_{B_iV_i} = 0 \tag{5.121}$$

$$f_{XB_i}f_{B_iX} - I = 0 \tag{5.122}$$

$$\text{for } 1 \leq j \leq q, j \neq i: \ f_{XB_j}f_{B_iX} + f_{V_iB_j}f_{B_iV_i} = 0. \tag{5.123}$$

$$\text{where } codim_{B_i''}(\bar{B}_i) \leq dim(A) + \sum_{i=1}^{q} dim(B_i) - dim(A, B_1, \ldots, B_q). \tag{5.124}$$

Applying Lemma 6 to equation (5.120), we have:

$$codim_{B_i}(B_i'') = codim_{B_i}(f^{-1}_{B_iX}(X')) + codim_{B_i}(f^{-1}_{B_iV_i}(V_i')) + codim_{B_i}(B_i'). \tag{5.125}$$

Applying Lemma 7 to equation (5.125), we have:

$$codim_{B_i}(B_i'') = codim_X(X') + codim_{V_i}(V_i') + codim_{B_i}(B_i'). \tag{5.126}$$

From equations (5.124) and (5.126), we have:

$$\begin{aligned} codim_{B_i}(\bar{B}_i) = codim_{B_i}(B_i'') + codim_{B_i''}(\bar{B}_i) \leq codim_X(X') + codim_{V_i}(V_i') + codim_{B_i}(B_i') \\ + dim(A) + \sum_{j=1}^{q} dim(B_j) - dim(A, B_1, \ldots, B_q). \end{aligned} \tag{5.127}$$

Now consider the following composite functions:

$$\sum_{i=1}^{q} f_{V_iA}f_{AV_i} : A \to A \tag{5.128}$$

$$\text{for } 1 \leq i \leq q: \ \sum_{j=1, j\neq i}^{q} f_{V_jB_i}f_{AV_j} + f_{YB_i}g_{AY} : A \to B_i. \tag{5.129}$$

Using equation (5.98), we have:

$$\text{for } 1 \leq i \leq q: \ f_{V_iA}f_{AV_i} + \sum_{j=1, j\neq i}^{q} f_{V_iB_j}f_{AV_i} = f_{AV_i} \text{ over a subspace } f^{-1}_{AV_i}(V_i') \text{ of } A. \tag{5.130}$$

Using equation (5.99), we have:

$$\sum_{i=1}^{q} f_{YB_i}g_{AY} = g_{AY} \text{ over a subspace } g^{-1}_{AY}(Y') \text{ of } A. \tag{5.131}$$

Consider the following subspace

$$A'''' = (\cap_{i=1}^{q} f^{-1}_{AV_i}(V_i')) \cap g^{-1}_{AY}(Y') \cap A''. \tag{5.132}$$

Summing the functions shown in equations (5.128) and (5.129) over A'''', we get:

$$\begin{aligned}
&\sum_{i=1}^{q} f_{V_iA} f_{AV_i} + \sum_{i=1}^{q} \Big(\sum_{j=1, j\neq i}^{q} f_{V_jB_i} f_{AV_j} + f_{YB_i} g_{AY} \Big) \\
&= \sum_{i=1}^{q} f_{V_iA} f_{AV_i} + \sum_{i=1}^{q} \sum_{j=1, j\neq i}^{q} f_{V_jB_i} f_{AV_j} + \sum_{i=1}^{q} f_{YB_i} g_{AY} \\
&= \sum_{i=1}^{q} f_{V_iA} f_{AV_i} + \sum_{j=1}^{q} \sum_{i=1, i\neq j}^{q} f_{V_jB_i} f_{AV_j} + \sum_{i=1}^{q} f_{YB_i} g_{AY} \\
&= \sum_{i=1}^{q} f_{V_iA} f_{AV_i} + \sum_{i=1}^{q} \sum_{j=1, j\neq i}^{q} f_{V_iB_j} f_{AV_i} + \sum_{i=1}^{q} f_{YB_i} g_{AY} \\
&= \sum_{i=1}^{q} f_{AV_i} + g_{AY} \qquad \text{Applying equations (5.130) and (5.131)} \\
&= I. \qquad \text{Using equation (5.101)}
\end{aligned} \tag{5.133}$$

Then, due to Lemma 9, over a subspace $\hat{A}$ of A'''', we have:

$$\sum_{i=1}^{q} f_{V_iA} f_{AV_i} - I = 0 \tag{5.134}$$

$$\text{for } 1 \leq i \leq q : \sum_{j=1, j\neq i}^{q} f_{V_jB_i} f_{AV_j} + f_{YB_i} g_{AY} = 0. \tag{5.135}$$

where,

$$codim_{A''''}(\hat{A}) \leq dim(A) + \sum_{i=1}^{q} dim(B_i) - dim(A, B_1, \ldots, B_q). \tag{5.136}$$

Applying Lemma 6 on equation (5.132), we get:

$$codim_A(A'''') = \sum_{i=1}^{q} codim_A(f_{AV_i}^{-1}(V_i')) + codim_A(g_{AY}^{-1}(Y')) + codim_A(A''). \tag{5.137}$$

Applying Lemma 7 on equation (5.137), we get:

$$codim_A(A'''') = \sum_{i=1}^{q} codim_{V_i}(V_i') + codim_Y(Y') + codim_A(A''). \tag{5.138}$$

Using equations (5.138) and (5.136), we have:

$$\begin{aligned}
codim_A(\hat{A}) = codim_A(A'''') + codim_{A''''}(\hat{A}) \leq \sum_{i=1}^{q} codim_{V_i}(V_i') + codim_Y(Y') + codim_A(A'') \\
+ dim(A) + \sum_{i=1}^{q} dim(B_i) - dim(A, B_1, \ldots, B_q).
\end{aligned} \tag{5.139}$$

Consider the following subspaces.

$$A^* = f_{AX}(\bar{A}) \tag{5.140}$$

$$A^{**} = A^* \cap B_1^* \tag{5.141}$$

$$A^{***} = f_{XA}(A^{**}) \tag{5.142}$$

$$\text{for } 1 \leq i \leq q: \ B_i^* = f_{B_iX}(\bar{B}_i) \tag{5.143}$$

$$B_1^{**} = B_1^* \cap B_2^* \cap \cdots \cap B_q^* \tag{5.144}$$

$$\text{for } 2 \leq i \leq q: \ B_i^{**} = B_1^* \cap B_i^* \tag{5.145}$$

$$\text{for } 1 \leq i \leq q: \ B_i^{***} = f_{XB_i}(B_i^{**}). \tag{5.146}$$

From equation (5.109) and (5.140) we know that f_{XA} is one-to-one over A^*. Now from (5.140) , we get $f_{XA}(A^*) = \bar{A}$, which implies $f_{XA}(A^{**}) \subseteq \bar{A}$ (as due to (5.141) $A^{**} \subseteq A^*$). This implies $A^{***} \subseteq \bar{A}$ (from (5.142)). Then, $f_{XA}f_{AX}(A^{***}) = A^{***} = f_{XA}(A^{**})$, and so we must have $A^{**} = f_{AX}(A^{***})$. With similar reasoning, from equation (5.122) and (5.143)-(5.146) we have: $B_i^{**} = f_{B_iX}(B_i^{***})$ for $1 \leq i \leq q$. [This is done in the following way. From equation (5.122) and (5.143) we know that f_{XB_i} is one-to-one over B_i^*. Then from (5.143): $f_{XB_i}(B_i^*) = \bar{B}_i$ which implies $f_{XB_i}(B_i^{**}) \subseteq \bar{B}_i$ (due to (5.144) and (5.145)). This implies $B_i^{***} \subseteq \bar{B}_i$ (from (5.146)). Then, $f_{XB_i}f_{B_iX}(B_i^{***}) = B_i^{***} = f_{XB_i}(B_i^{**})$, and so we must have $B_i^{**} = f_{B_iX}(B_i^{***})$.]

Let us define the following subspaces:

$$S_a = \{a \in A | g_{AY}(a) \in f_{AY}(A^{***})\} \tag{5.147}$$

$$\text{for } 1 \leq i \leq q: \ S_i = \{a \in A | f_{AV_i}(a) \in f_{B_iV_i}({B_i}^{***})\} \tag{5.148}$$

$$S = \hat{A} \cap S_a \cap S_1 \cap S_2 \cap \cdots \cap S_q. \tag{5.149}$$

Let $\hat{a} \in S$. Then $f_{AV_i}(\hat{a}) = f_{B_iV_i}(b_i)$ for some $b_i \in B_i^{***}$ where $1 \leq i \leq q$. Also $g_{AY}(\hat{a}) = f_{AY}(a)$ for some $a \in A^{***}$. So from equations (5.134) and (5.135) respectively, we have:

$$\sum_{i=1}^{q} f_{V_iA}f_{B_iV_i}(b_i) = \hat{a} \tag{5.150}$$

$$\text{and for } 1 \leq i \leq q: \sum_{j=1, j\neq i}^{q} f_{V_jB_i}f_{B_jV_j}(b_j) + f_{YB_i}f_{AY}(a) = 0. \tag{5.151}$$

Summing equation (5.121) for $1 \leq i \leq q$, we have:

$$\sum_{i=1}^{q}(f_{XA}f_{B_iX} + f_{V_iA}f_{B_iV_i})(b_i) = 0 \tag{5.152}$$

Substituting $\sum_{i=1}^{q} f_{V_iA}f_{B_iV_i}(b_i)$ from equation (5.150) in equation (5.152), we have:

$$\sum_{i=1}^{q} f_{XA}f_{B_iX}(b_i) = -\hat{a} \tag{5.153}$$

interchanging i and j in equation (5.123), and then summing for $1 \leq j \leq q, j \neq i$, we have:

$$\text{for } 1 \leq i \leq q : \sum_{j=1,j\neq i}^{q} (f_{XB_i}f_{B_jX} + f_{V_jB_i}f_{B_jV_j})(b_j) = 0 \tag{5.154}$$

Substituting $\sum_{j=1,j\neq i}^{q} f_{V_jB_i}f_{B_jV_j}(b_j)$ from equation (5.151) in equation (5.154), we have:

$$\text{for } 1 \leq i \leq q : \sum_{j=1,j\neq i}^{q} f_{XB_i}f_{B_jX}(b_j) - f_{YB_i}f_{AY}(a) = 0 \tag{5.155}$$

Substituting $f_{YB_i}f_{AY}(a)$ from equation (5.110), we have:

$$\text{for } 1 \leq i \leq q : \sum_{j=1,j\neq i}^{q} f_{XB_i}f_{B_jX}(b_j) + f_{XB_i}f_{AX}(a) = 0 \tag{5.156}$$

For $i = 1$, from equation (5.156), we get:

$$\sum_{j=2}^{q} f_{XB_1}f_{B_jX}(b_j) + f_{XB_1}f_{AX}(a) = 0$$

$$\text{or, } f_{XB_1}(\sum_{j=2}^{q} f_{B_jX}(b_j) + f_{AX}(a)) = 0$$

Since $f_{B_jX}(b_j) \in (B_1^* \cap B_j^*)$ for $2 \leq j \leq q$; and $f_{AX}(a) \in (A^* \cap B_1^*)$; and as f_{XB_1} is invertible over B_1^*, we have:

$$\sum_{j=2}^{q} f_{B_jX}(b_j) + f_{AX}(a) = 0. \tag{5.157}$$

For $2 \leq i \leq q$, from equation (5.156), we get:

$$f_{XB_i}(\sum_{j=1,j\neq i}^{q} f_{B_jX}(b_j) + f_{AX}(a)) = 0$$

$$\text{or, } f_{XB_i}(f_{B_1X}(b_1) - f_{B_iX}(b_i) + \sum_{j=2}^{q} f_{B_jX}(b_j) + f_{AX}(a)) = 0$$

$$\text{or, } f_{XB_i}(f_{B_1X}(b_1) - f_{B_iX}(b_i)) = 0 \qquad \text{[using equation (5.157)]}$$

$$\text{or, } (f_{B_1X}(b_1) - f_{B_iX}(b_i)) = 0 \qquad \text{[Since } f_{B_1X}(b_1) \in B_i^* \text{ and } f_{XB_i} \text{ is invertible over } B_i^* \text{]}$$

or, $f_{B_1X}(b_1) = f_{B_iX}(b_i)$. (5.158)

Substituting equation (5.158) in equation (5.153), we get:

$$\sum_{i=1}^{q} f_{XA} f_{B_1X}(b_1) = -\hat{a}$$
or, $q f_{XA} f_{B_1X}(b_1) = -\hat{a}$

Now, if the characteristic of the finite field divides q, we must have $q = 0$. So, $-\hat{a} = 0$.

Since this is true for any arbitrary $\hat{a} \in S$, we must have $S = \{0\}$, which implies $dim(S) = 0$.

Now, $dim(A) = dim(A) - dim(S) = codim_A(S) = codim_A(\hat{A} \cap S_a \cap S_1 \cap S_2 \cap \cdots \cap S_q)$
$\leq codim_A(\hat{A}) + codim_A(S_a) + \sum_{i=1}^{q} codim_A(S_i)$ [applying Lemma 6]. (5.159)

Hence, from (5.147) we have:

$codim_A(S_a) = codim_A(g_{AY}^{-1}(f_{AY}(A^{***}))) \leq codim_Y(f_{AY}(A^{***}))$ [from Lemma 7]

or, $codim_A(S_a) \leq dim(Y) - dim(f_{AY}(A^{***}))$ (5.160)

Since $f_{AX}(A^{***})$ is a subspace of B_1^*(due to (5.141) and that $A^{**} = f_{AX}(A^{***})$), $f_{XB_1} f_{AX}$ is invertible over A^{***}. So from equation (5.110): $f_{YB_1} f_{AY}$ is invertible over A^{***}, and hence f_{AY} is invertible over A^{***}. Then, $dim(f_{AY}(A^{***})) = dim(A^{***})$. Hence from eqn. (5.160) we have:

$codim_A(S_a) \leq dim(Y) - dim(A^{***}) = dim(Y) - dim(f_{XA}(A^{**}))$

Now, A^{**} is a subspace of $f_{AX}(\bar{A})$, and over $f_{AX}(\bar{A})$, f_{XA} is invertible because of eqn. (5.109).

So, $codim_A(S_a) \leq dim(Y) - dim(A^{**}) = dim(Y) - dim(A^* \cap B_1^*)$
$= dim(Y) + codim_X(A^* \cap B_1^*) - dim(X)$

or, $codim_A(S_a) \leq dim(Y) + codim_X(A^*) + codim_X(B_1^*) - dim(X)$ [from Lemma 6]

or, $codim_A(S_a) \leq dim(Y) + dim(X) - dim(A^*) + dim(X) - dim(B_1^*) - dim(X)$

or, $codim_A(S_a) \leq dim(Y) + dim(X) - dim(f_{AX}(\bar{A})) - dim(f_{B_1X}(\bar{B}_1))$

or, $codim_A(S_a) \leq dim(Y) + dim(X) - dim(\bar{A}) - dim(\bar{B}_1)$

or, $codim_A(S_a) \leq dim(Y) + dim(X) + codim_A(\bar{A}) + codim_{B_1}(\bar{B}_1) - dim(A) - dim(B_1)$. (5.161)

for $1 \leq i \leq q$, from (5.148) we have:

$codim_A(S_i) = codim_A(f^{-1}_{AV_i}(f_{B_iV_i}(B_i^{***}))) \leq codim_{V_i}(f_{B_iV_i}(B_i^{***}))$ [from Lemma 7]

or, $codim_A(S_i) \leq dim(V_i) - dim(f_{B_iV_i}(B_i^{***}))$

Since $f_{B_iX}(B_i^{***})$ is a subspace of B_1^*, $f_{XB_1}f_{B_iX}$ is invertible over B_i^{***}; from equation (5.123) $f_{V_iB_1}f_{B_iV_i}$ is invertible over B_i^{***}, and hence $f_{B_iV_i}$ must be invertible over B_i^{***}. So,

$$codim_A(S_i) \leq dim(V_i) - dim(B_i^{***}) = dim(V_i) - dim(f_{XB_i}(B_i^{**})) \tag{5.162}$$

Now, B_i^{**} is a subspace of $f_{B_iX}(\bar{B}_i)$, and over $f_{B_iX}(\bar{B}_i)$: f_{XB_i} is invertible from eq. (5.122). So, for $2 \leq i \leq q$ we have:

$codim_A(S_i) \leq dim(V_i) - dim(B_i^{**}) = dim(V_i) - dim(B_i^* \cap B_1^*)$

$= dim(V_i) + codim_X(B_i^* \cap B_1^*) - dim(X)$

$\leq dim(V_i) + codim_X(B_i^*) + codim_X(B_1^*) - dim(X)$ [using Lemma 6]

$= dim(V_i) + dim(X) - dim(B_i^*) + dim(X) - dim(B_1^*) - dim(X)$

$= dim(V_i) + dim(X) - dim(f_{B_iX}(\bar{B}_i)) - dim(f_{B_1X}(\bar{B}_1))$

$= dim(V_i) + dim(X) - dim(\bar{B}_i) - dim(\bar{B}_1)$ [using equation (5.122)]

$$= dim(V_i) + dim(X) + codim_{B_i}(\bar{B}_i) + codim_{B_1}(\bar{B}_1) - dim(B_i) - dim(B_1) \tag{5.163}$$

for $i = 1$ form equation (5.162) we have:

$codim_A(S_1) \leq dim(V_1) - dim(B_1^{**}) = dim(V_1) - dim(B_1^* \cap B_2^* \cap \cdots \cap B_q^*)$

$= dim(V_1) + codim_X(B_1^* \cap B_2^* \cap \cdots \cap B_q^*) - dim(X)$

$\leq dim(V_1) + \sum_{i=1}^{q} codim_X(B_i^*) - dim(X)$ [from Lemma 6]

$= dim(V_1) + (q)dim(X) - \sum_{i=1}^{q} dim(B_i^*) - dim(X)$

$= dim(V_1) + (q-1)dim(X) - \sum_{i=1}^{q} dim(f_{B_iX}(\bar{B}_i))$

$= dim(V_1) + (q-1)dim(X) - \sum_{i=1}^{q} dim(\bar{B}_i)$ [using equation (5.122)]

$$= dim(V_1) + (q-1)dim(X) + \sum_{i=1}^{q} codim_{B_i}(\bar{B}_i) - \sum_{i=1}^{q} dim(B_i). \tag{5.164}$$

So, substituting equations (5.161), (5.163), and (5.164) in equation (5.159), we have:

$$dim(A) \leq codim_A(\hat{A}) + codim_A(S_a) + \sum_{i=1}^{q} codim_A(S_i)$$

or, $dim(A) \leq codim_A(\hat{A}) + dim(Y) + dim(X) + codim_A(\bar{A}) + codim_{B_1}(\bar{B_1}) - dim(A)$

$- dim(B_1) + dim(V_1) + (q-1)dim(X) + \sum_{i=1}^{q} codim_{B_i}(\bar{B_i}) - \sum_{i=1}^{q} dim(B_i) + \sum_{i=2}^{q} dim(V_i)$

$+ (q-1)dim(X) + \sum_{i=2}^{q} codim_{B_i}(\bar{B_i}) + (q-1)codim_{B_1}(\bar{B_1}) - \sum_{i=2}^{q} dim(B_i) - (q-1)dim(B_1)$

or, $dim(A) \leq codim_A(\hat{A}) + dim(Y) + (2q-1)dim(X) + codim_A(\bar{A}) - dim(A)$

$- (q+1)dim(B_1) + \sum_{i=1}^{q} dim(V_i) + \sum_{i=2}^{q} 2codim_{B_i}(\bar{B_i}) + (q+1)codim_{B_1}(\bar{B_1}) - \sum_{i=2}^{q} 2dim(B_i)$

Substituting values from equations (5.139), (5.114), and (5.127), we get:

$$dim(A) \leq \sum_{i=1}^{q} codim_{V_i}(V_i') + codim_Y(Y') + codim_A(A'') + dim(A) + \sum_{i=1}^{q} dim(B_i)$$

$- dim(A, B_1, \ldots, B_q) + dim(Y) + (2q-1)dim(X) + codim_X(X') + codim_Y(Y') + codim_A(A')$

$+ dim(A) + \sum_{i=1}^{q} dim(B_i) - dim(A, B_1, \ldots, B_q) - dim(A) - (q+1)dim(B_1) + \sum_{i=1}^{q} dim(V_i)$

$+ \sum_{i=2}^{q} 2(codim_X(X') + codim_{V_i}(V_i') + codim_{B_i}(B_i') + dim(A) + \sum_{j=1}^{q} dim(B_j) - dim(A, B_1, .., B_q))$

$+ (q+1)(codim_X(X') + codim_{V_1}(V_1') + codim_{B_1}(B_1') + dim(A) + \sum_{j=1}^{q} dim(B_j)$

$- dim(A, B_1, \ldots, B_q)) - \sum_{i=2}^{q} 2dim(B_i)$

or, $dim(A) \leq (q+2)codim_{V_1}(V_1') + \sum_{i=2}^{q} 3codim_{V_i}(V_i') + 2codim_Y(Y') + codim_A(A'') + dim(Y)$

$+ (2q-1)dim(X) + (3q)codim_X(X') + codim_A(A') - dim(A) - (q+1)dim(B_1) + \sum_{i=1}^{q} dim(V_i)$

$+ \sum_{i=2}^{q} 2codim_{B_i}(B_i') + (q+1)codim_{B_1}(B_1') - \sum_{i=2}^{q} 2dim(B_i)$

$+ (3q+1)(dim(A) + \sum_{j=1}^{q} dim(B_j) - dim(A, B_1, \ldots, B_q))$

Substituting values from equations (5.97), (5.99), (5.98), (5.100), (5.102) and (5.101), we get:

or, $dim(A) \leq (q+2)dim(V_1|A, B_2, \ldots, B_q) + \sum_{i=2}^{q} 3dim(V_i|A, B_1, \ldots, B_{i-1}, B_{i+1}, \ldots, B_q)$

$+ 2dim(Y|B_1, \ldots, B_q) + dim(A|V_1, \ldots, V_q, Y) + dim(Y) + (2q-1)dim(X)$

$+ (3q)dim(X|A, B_1, \ldots, B_q) + dim(A|X, Y) - dim(A) - (q+1)dim(B_1) + \sum_{i=1}^{q} dim(V_i)$

$$+ \sum_{i=2}^{q} 2dim(B_i|X, V_i) + (q+1)dim(B_1|X, V_1) - \sum_{i=2}^{q} 2dim(B_i)$$
$$+ (3q+1)(dim(A) + \sum_{j=1}^{q} dim(B_j) - dim(A, B_1, \ldots, B_q))$$
$$\text{or, } 2dim(A) + (q+1)dim(B_1) + \sum_{i=2}^{q} 2dim(B_i) \leq (2q-1)dim(X) + dim(Y) + \sum_{i=1}^{q} dim(V_i)$$
$$+ dim(A|X, Y) + dim(A|V_1, \ldots, V_q, Y) + (q+1)dim(B_1|X, V_1) + \sum_{i=2}^{q} 2dim(B_i|X, V_i)$$
$$+ (3q)dim(X|A, B_1, \ldots, B_q) + 2dim(Y|B_1, \ldots, B_q) + (q+2)dim(V_1|A, B_2, \ldots, B_q)$$
$$+ \sum_{i=2}^{q} 3dim(V_i|A, B_1, \ldots, B_{i-1}, B_{i+1}, \ldots, B_q)$$
$$+ (3q+1)(dim(A) + \sum_{j=1}^{q} dim(B_j) - dim(A, B_1, \ldots, B_q)).$$

5.5 Proof of the Inequality Shown in Equation (5.3)

We here derive another characteristic-dependent linear rank inequality by defining the set S in equation (5.149) in a different way. (So the following content continues from equation (5.139).)

$$\text{For } 1 \leq i \leq q: \; S_{A_i} = \{u \in A | f_{AX}(u) \in f_{B_iX}(\bar{B}_i)\} \tag{5.165}$$

Now note that over $f_{B_iX}(\bar{B}_i)$, f_{XB_i} is one-to-one from equation (5.122); and f_{AX} is one-to-one over $\bar{A}$ from equation (5.109). Then, over a subspace $\bar{A} \cap S_{A_i}$, $f_{XB_i}f_{AX}$ is one-to-one. Hence from equation (5.110), both f_{YB_i} and f_{AY} are one-to-one over $\bar{A} \cap S_{A_i}$.

Now note that from equation (5.109), we have, over $f_{AX}(\bar{A})$:

$$f_{AX}f_{XA} = I \tag{5.166}$$

Consider the composite function $f_{AX}f_{XA}f_{B_iX} + f_{AX}f_{V_iA}f_{B_iV_i}$. Due to equation (5.121), over $\bar{B}_i$, we have:

$$f_{AX}f_{XA}f_{B_iX} + f_{AX}f_{V_iA}f_{B_iV_i} = 0 \tag{5.167}$$

Consider the below subspaces:

$$\text{for } 1 \leq i \leq q: \; S_{B_i} = \{u \in B_i | f_{B_iX}(u) \in f_{AX}(\bar{A})\} \tag{5.168}$$

Then, for any $b_i \in \bar{B}_i \cap S_{B_i}$ there exists $a \in \bar{A}$ such that $f_{B_iX}(b_i) = f_{AX}(a)$. So from equation (5.167), we have:

$$f_{AX}f_{XA}f_{B_iX}(b_i) + f_{AX}f_{V_iA}f_{B_iV_i}(b_i) = 0$$
$$\text{or, } f_{AX}f_{XA}f_{AX}(a) + f_{AX}f_{V_iA}f_{B_iV_i}(b_i) = 0$$
$$\text{or, } f_{AX}(a) + f_{AX}f_{V_iA}f_{B_iV_i}(b_i) = 0 \qquad \text{[due to equation (5.109)]}$$
$$\text{or, } f_{B_iX}(b_i) + f_{AX}f_{V_iA}f_{B_iV_i}(b_i) = 0.$$

So we have:

$$f_{B_iX} + f_{AX}f_{V_iA}f_{B_iV_i} = 0 \tag{5.169}$$

Consider the composite function: $f_{XB_i}f_{B_iX} + f_{XB_i}f_{AX}f_{V_iA}f_{B_iV_i}$.

Due to equation (5.169) over $\bar{B}_i \cap S_{B_i}$, we have:

$$f_{XB_i}f_{B_iX} + f_{XB_i}f_{AX}f_{V_iA}f_{B_iV_i} = 0$$
$$\text{or, from equation (5.122): } f_{XB_i}f_{AX}f_{V_iA}f_{B_iV_i} = -I. \tag{5.170}$$

Consider the composite function: $f_{XB_j}f_{B_iX} + f_{XB_j}f_{AX}f_{V_iA}f_{B_iV_i}$ for $j \neq i$. Due to equation (5.169) over $\bar{B}_i \cap S_{B_i}$, we have:

$$f_{XB_j}f_{B_iX} + f_{XB_j}f_{AX}f_{V_iA}f_{B_iV_i} = 0$$
$$\text{using equation (5.123): } -f_{V_iB_j}f_{B_iV_i} + f_{XB_j}f_{AX}f_{V_iA}f_{B_iV_i} = 0. \tag{5.171}$$

We define the set S as following:

$$S_{\hat{A}} = \{u \in \hat{A} | g_{AY}(u) \in f_{AY}(\bar{A} \cap S_{A_1} \cap S_{A_2} \cap \cdots \cap S_{A_q})\} \tag{5.172}$$
$$R_{\hat{A}_i} = \{u \in \hat{A} | f_{AV_i}(u) \in f_{B_iV_i}(\bar{B}_i \cap S_{B_i})\} \tag{5.173}$$
$$S = \hat{A} \cap \bar{A} \cap S_{A_1} \cap S_{A_2} \cap \cdots \cap S_{A_q} \cap S_{\hat{A}} \cap R_{\hat{A}_1} \cap R_{\hat{A}_2} \cap \cdots \cap R_{\hat{A}_q}. \tag{5.174}$$

Let $\hat{a} \in S$. Then from equation (5.135), for $1 \leq i \leq q$ we have:

$$\sum_{j=1, j\neq i}^{q} f_{V_jB_i}f_{AV_j}(\hat{a}) + f_{YB_i}g_{AY}(\hat{a}) = 0$$

From (5.172) we know there exists a $a \in \bar{A} \cap (\cap_{i=1}^{q} S_{A_i})$ such that $g_{AY}(\hat{a}) = f_{AY}(a)$. So,

$$\sum_{j=1, j\neq i}^{q} f_{V_jB_i}f_{AV_j}(\hat{a}) + f_{YB_i}f_{AY}(a) = 0$$

Substituting $f_{YB_i}f_{AY}(a)$ from equation (5.110) we have:

$$\sum_{j=1,j\neq i}^{q} f_{V_jB_i}f_{AV_j}(\hat{a}) - f_{XB_i}f_{AX}(a) = 0$$

Since f_{AY} is invertible over $\bar{A} \cap \cup_{i=1}^{q} S_{A_i}$, we can write:

$$\sum_{j=1,j\neq i}^{q} f_{V_jB_i}f_{AV_j}(\hat{a}) - f_{XB_i}f_{AX}f_{AY}^{-1}f_{AY}(a) = 0$$

$$\text{or, } \sum_{j=1,j\neq i}^{q} f_{V_jB_i}f_{AV_j}(\hat{a}) - f_{XB_i}f_{AX}f_{AY}^{-1}g_{AY}(\hat{a}) = 0$$

From (5.173) we know there exists a $b_j \in \bar{B}_j \cap S_{B_j}$ such that $f_{AV_j}(\hat{a}) = f_{B_jV_j}(b_j)$. So,

$$\sum_{j=1,j\neq i}^{q} f_{V_jB_i}f_{B_jV_j}(b_j) - f_{XB_i}f_{AX}f_{AY}^{-1}g_{AY}(\hat{a}) = 0$$

Substituting $f_{V_jB_i}f_{B_jV_j}(b_j)$ from equation (5.123) we have:

$$\sum_{j=1,j\neq i}^{q} -f_{XB_i}f_{B_jX}(b_j) - f_{XB_i}f_{AX}f_{AY}^{-1}g_{AY}(\hat{a}) = 0$$

Substituting $f_{B_jX}(b_j)$ from equation (5.169) we have:

$$\sum_{j=1,j\neq i}^{q} f_{XB_i}f_{AX}f_{V_jA}f_{B_jV_j}(b_j) - f_{XB_i}f_{AX}f_{AY}^{-1}g_{AY}(\hat{a}) = 0$$

$$\text{or, } \sum_{j=1,j\neq i}^{q} f_{XB_i}f_{AX}f_{V_jA}f_{AV_j}(\hat{a}) - f_{XB_i}f_{AX}f_{AY}^{-1}g_{AY}(\hat{a}) = 0$$

$$\text{or, } f_{XB_i}f_{AX}\Big(\sum_{j=1,j\neq i}^{q} f_{V_jA}f_{AV_j} - f_{AY}^{-1}g_{AY}\Big)(\hat{a}) = 0 \tag{5.175}$$

Now from equation (5.134) we have $(f_{V_iA}f_{AV_i} + \sum_{j=1,j\neq i}^{q} f_{V_jA}f_{AV_j})(\hat{a}) = \hat{a}$. So, from (5.175):

$$f_{XB_i}f_{AX}(\hat{a} - f_{V_iA}f_{AV_i}(\hat{a}) - f_{AY}^{-1}g_{AY}(\hat{a})) = 0. \tag{5.176}$$

Let A^{1-1} be the subspace over which $f_{XB_i}f_{AX}$ is one-to-one. We have already shown that $(\bar{A} \cap S_{A_1} \cap S_{A_2} \cap \cdots \cap S_{A_q}) \subseteq A^{1-1}$. Since $\hat{a} \in \bar{A} \cap S_{A_1} \cap S_{A_2} \cap \cdots \cap S_{A_q}$, we know $\hat{a} \in A^{1-1}$. Now, $f_{V_iA}f_{AV_i}(\hat{a}) \in f_{V_iA}f_{B_iV_i}(\bar{B}_i \cap S_{B_i})$, and from equation (5.170) we know that $f_{XB_i}f_{AX}$ in one-to-one over $f_{V_iA}f_{B_iV_i}(\bar{B}_i \cap S_{B_i})$. So $f_{V_iA}f_{AV_i}(\hat{a}) \in A^{1-1}$. From (5.172) we know that $f_{AY}^{-1}g_{AY}(\hat{a}) \in f_{AY}^{-1}f_{AY}(\bar{A} \cap S_{A_1} \cap S_{A_2} \cap \cdots \cap S_{A_q}) = (\bar{A} \cap S_{A_1} \cap S_{A_2} \cap \cdots \cap S_{A_q})$. So, $(\hat{a} - f_{V_iA}f_{AV_i}(\hat{a}) - f_{AY}^{-1}g_{AY}(\hat{a})) \in A^{1-1}$. Then for equation (5.176) to hold we must have:

$$\hat{a} - f_{V_iA}f_{AV_i}(\hat{a}) - f_{AY}^{-1}g_{AY}(\hat{a}) = 0$$

$$\text{or, } f_{V_iA}f_{AV_i}(\hat{a}) = \hat{a} - f_{AY}^{-1}g_{AY}(\hat{a}). \tag{5.177}$$

As equation (5.177) holds for $1 \leq i \leq q$ we have:

$$\sum_{i=1}^{q} f_{V_iA} f_{AV_i}(\hat{a}) = q\hat{a} - q f_{AY}^{-1} g_{AY}(\hat{a})$$

Using equation (5.134): $\hat{a} = q\hat{a} - q f_{AY}^{-1} g_{AY}(\hat{a})$

If $q = 0$ over a finite field, we get: $\hat{a} = 0$.

As this holds for any $\hat{a} \in S$, we must have $S = \{0\}$. Now we calculate some values that help us compute an upper-bound over $dim(A)$.

$$codim_A(S_{A_i}) = codim_A(f_{AX}^{-1}(f_{B_iX}(\bar{B}_i))) \leq codim_X(f_{B_iX}(\bar{B}_i)) = dim(X) - dim(f_{B_iX}(\bar{B}_i))$$

$$\text{or, } codim_A(S_{A_i}) \leq dim(X) - dim(\bar{B}_i) = dim(X) + codim_{B_i}(\bar{B}_i) - dim(B_i). \tag{5.178}$$

$$codim_{B_i}(S_{B_i}) = codim_{B_i}(f_{B_iX}^{-1}(f_{AX}(\bar{A}))) \leq codim_X(f_{AX}(\bar{A})) = dim(X) - dim(f_{AX}(\bar{A}))$$

$$codim_{B_i}(S_{B_i}) \leq dim(X) - dim(\bar{A}) = dim(X) + codim_A(\bar{A}) - dim(A). \tag{5.179}$$

$$dim(A) = dim(A) - dim(S) = codim_A(S)$$

$$\text{or, } dim(A) \leq codim_A(\hat{A}) + codim_A(\bar{A}) + \sum_{i=1}^{q} codim_A(S_{A_i}) + codim_A(g_{AY}^{-1}(f_{AY}(\bar{A} \cap (\cap_{i=1}^{q} S_{A_i}))))$$
$$+ \sum_{i=1}^{q} codim_A(f_{AV_i}^{-1}(f_{B_iV_i}(\bar{B}_i \cap S_{B_i})))$$

$$\text{or, } dim(A) \leq codim_A(\hat{A}) + codim_A(\bar{A}) + \sum_{i=1}^{q} codim_A(S_{A_i}) + codim_Y(f_{AY}(\bar{A} \cap (\cap_{i=1}^{q} S_{A_i})))$$
$$+ \sum_{i=1}^{q} codim_{V_i}(f_{B_iV_i}(\bar{B}_i \cap S_{B_i}))$$

As over $\bar{A} \cap (\cap_{i=1}^{q} S_{A_i})$, f_{AY} is one-to-one, and as from equation (5.169) over $\bar{B}_i \cap S_{B_i}$ $f_{B_iV_i}$ is one-to-one, we have:

$$\text{or, } dim(A) \leq codim_A(\hat{A}) + codim_A(\bar{A}) + \sum_{i=1}^{q} codim_A(S_{A_i}) + codim_Y(\bar{A} \cap (\cap_{i=1}^{q} S_{A_i}))$$
$$+ \sum_{i=1}^{q} codim_{V_i}(\bar{B}_i \cap S_{B_i})$$

$$\text{or, } dim(A) \leq codim_A(\hat{A}) + codim_A(\bar{A}) + \sum_{i=1}^{q} codim_A(S_{A_i}) + dim(Y) + codim_A(\bar{A} \cap (\cap_{i=1}^{q} S_{A_i}))$$
$$- dim(A) + \sum_{i=1}^{q} dim(V_i) + \sum_{i=1}^{q} codim_{B_i}(\bar{B}_i \cap S_{B_i}) - \sum_{i=1}^{q} dim(B_i)$$

$$\text{or, } dim(A) \leq codim_A(\hat{A}) + 2codim_A(\bar{A}) + \sum_{i=1}^{q} 2codim_A(S_{A_i}) + dim(Y) - dim(A) + \sum_{i=1}^{q} dim(V_i) + \sum_{i=1}^{q} codim_{B_i}(\bar{B}_i) + \sum_{i=1}^{q} codim_{B_i}(S_{B_i}) - \sum_{i=1}^{q} dim(B_i)$$

Substituting values from equations (5.179) and (5.178), we have:

$$dim(A) \leq codim_A(\hat{A}) + 2codim_A(\bar{A}) + \sum_{i=1}^{q} 2(dim(X) + codim_{B_i}(\bar{B}_i) - dim(B_i)) + dim(Y)$$

$$-dim(A) + \sum_{i=1}^{q} dim(V_i) + \sum_{i=1}^{q} codim_{B_i}(\bar{B}_i) + \sum_{i=1}^{q} (dim(X) + codim_A(\bar{A}) - dim(A)) - \sum_{i=1}^{q} dim(B_i)$$

$$\text{or, } dim(A) \leq codim_A(\hat{A}) + (q+2)codim_A(\bar{A}) + (3q)dim(X) + \sum_{i=1}^{q} 3codim_{B_i}(\bar{B}_i) - \sum_{i=1}^{q} 3dim(B_i) + dim(Y) - (q+1)dim(A) + \sum_{i=1}^{q} dim(V_i)$$

$$\text{or, } (q+2)dim(A) + \sum_{i=1}^{q} 3dim(B_i) \leq codim_A(\hat{A}) + (q+2)codim_A(\bar{A}) + (3q)dim(X) + \sum_{i=1}^{q} 3codim_{B_i}(\bar{B}_i) + dim(Y) + \sum_{i=1}^{q} dim(V_i)$$

$$\text{or, } (q+2)dim(A) + \sum_{i=1}^{q} 3dim(B_i) \leq \sum_{i=1}^{q} codim_{V_i}(V_i') + codim_Y(Y') + codim_A(A'')$$

$$+ (q+2)(codim_X(X') + codim_Y(Y') + codim_A(A')) + (3q)dim(X) + \sum_{i=1}^{q} 3(codim_X(X')$$

$$+ codim_{V_i}(V_i') + codim_{B_i}(B_i')) + dim(Y) + \sum_{i=1}^{q} dim(V_i) + (4q+3)(dim(A) + \sum_{j=1}^{q} dim(B_j) - dim(A, B_1, \ldots, B_q))$$

$$\text{or, } (q+2)dim(A) + \sum_{i=1}^{q} 3dim(B_i) \leq (3q)dim(X) + dim(Y) + \sum_{i=1}^{q} dim(V_i) + \sum_{i=1}^{q} 4codim_{V_i}(V_i')$$

$$+ (q+3)codim_Y(Y') + codim_A(A'') + (4q+2)codim_X(X') + (q+2)codim_A(A') + \sum_{i=1}^{q} 3codim_{B_i}(B_i') + (4q+3)(dim(A) + \sum_{j=1}^{q} dim(B_j) - dim(A, B_1, \ldots, B_q))$$

$$\text{or, } (q+2)dim(A) + \sum_{i=1}^{q} 3dim(B_i) \leq (3q)dim(X) + dim(Y) + \sum_{i=1}^{q} dim(V_i)$$

$$+ \sum_{i=1}^{q} 4dim(V_i|A, B_1, .., B_{i-1}, B_{i+1}, .., B_q) + (q+3)dim(Y|B_1, \ldots, B_q) + dim(A|V_1, \ldots, V_q, Y)$$

$$+ (4q+2)dim(X|A, B_1, \ldots, B_q) + (q+2)dim(A|X, Y) + \sum_{i=1}^{q} 3dim(B_i|X, V_i)$$

$$+ (4q+3)(dim(A) + \sum_{j=1}^{q} dim(B_j) - dim(A, B_1, \ldots, B_q)). \quad (5.180)$$

5.6 Discussion

There are some open problems that the derivation of these characteristic-dependent linear rank inequalities have brought forth.

(i) Given a network and a set of characteristic-dependent linear rank inequalities, it is not clear applying which inequality would result in the tightest upper-bound on the linear coding capacity over a given finite field. For example, if the inequalities produced in [34] are applied to the networks in Fig. 5.1 and Fig. 5.2 it produces upper-bounds less tighter than the inequalities in equations (5.1) and (5.2) respectively. And if the inequalities of equations (5.1) and (5.2) are applied back to the two networks used in [34] to construct the characteristic-dependent linear rank inequalities, it produces less tighter upper-bounds in comparison to the inequalities of [34]. It seems like, given a network, to find the best upper-bound, it is better to construct a suitable linear rank inequality from the scratch.

(ii) Can characteristic-dependent linear rank inequalities be algorithmically be generated from networks whose linear coding capacity varies with the characteristic of the finite field. We, in the proofs of these inequalities, have constructed the set S (the set that contains only the zero vector over certain characteristics but contains more vectors over other characteristics) in an ad-hoc way. What we do not know is whether there exists an algorithm to search for S systematically. If this problem is solved, then the whole DFZ method becomes algorithmic and characteristic-dependent linear rank inequalities can be generated systematically. It would also be interesting to know what would be the complexity of such an algorithm.

(iii) Why our inequalities did not produce tight upper-bounds even for the case when $q = 2$? Whether it would have produced a tight upper-bound if the set S had been constructed some other way; or whether tight upper-bounds are not guaranteed to be produced by the DFZ method. In [32] also, the authors report that the characteristics-dependent linear rank inequality generated by the DFZ method produces an upper-bound of 6/7 on the linear coding capacity of the non-Fano

network over finite fields of even characteristics; whereas its linear coding capacity over such a finite field is equal to 5/6.

(iv) Each and every instance of the application of the DFZ method (contained in [32], [33], [34], and in this thesis), produced and upper-bound that is of the form $\frac{k}{k+1}$, when the inequality is applied back to the network using which it has been constructed. We do not know whether this is a limitation of the DFZ method or it is just these networks that were tried have this similarity in outcome.

(v) How many characteristic-dependent linear rank inequalities are there when the number of variables are fixed? When the number of variables are 6 or less, there exists no characteristic-dependent linear rank inequality. It is not known whether the number of characteristic-dependent linear rank inequalities having a given finite number of variables is also finite.

6

Conclusion

It was already shown in [3] that a network may have a rate 1 linear solution, but it may not have a $(1,1)$ fractional linear solution. In Chapter 3, we showed that (i) a network may have a rate k/n linear solution, but have no (wk, wn) fractional linear solution unless w is a multiple of a certain integer, and (ii) a network may have a rate k/n linear solution, but have no (wk, wn) fractional linear solution unless w is greater than or equal to a certain integer. These results also show that that for any arbitrary large number m, there exits a network which has no (mk, mn) fractional linear solution but has a (wk, wn) fractional linear solution for some $w > m$, hence to achieve a rate k/n, the message dimension may has to be arbitrary large.

As a result, it is natural to ask that, for a network which is already known to have a vector linear solution, if the message dimension is fixed to some value (something which may be applicable to a practical network), can it be guaranteed that a certain rate would always be linearly achievable? Or, whether for any three positive integers k, n, and d, there exists a network which has a d-dimensional vector linear solution (same as a (d,d)-fractional linear solution), but for some positive integer w, if l is the least positive integer such that the network has (w,l)-fractional linear solution, then the ratio w/l is less than or equal to k/n. Or, looking from another direction: if a suboptimal rate is desired, what is the minimum value of the message dimension for which the desired rate would be achievable?

Our work also shows that a d_1-dimensional vector linear solution ($d_1 \geq 2$) is not superior to a d_2-dimensional vector linear solution ($d_2 \geq 2$) irrespective of whether d_2 is greater than d_1 or d_1 is greater than d_2. This is because a network may have a d_1-dimensional vector linear solution but have no d_2-dimensional vector linear solution, and vice versa.

The results of Chapter 3 can be combined with the result of [19] 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. Also, there exists a network which has a vector linear solution if and only if the message dimension is greater than or equal to m and the characteristic of the finite field belongs to P.

In Chapter 4, we showed that the set of characteristics over which a vector linear solution exists depends upon the message dimension; as the message dimension is increased, the set of characteristics over which a vector linear solution exists may get larger as well as may get smaller. We also showed that a network may have an m_1-dimensional vector linear solution and an m_2-dimensional vector linear solution, but have no $(m_1 + m_2)$-dimensional vector linear solution.

It has been shown in [12] that linear coding capacity over finite fields is greater than or equal to linear coding capacity over rings which are not fields. We showed that scalar linear network coding over rings may be superior to scalar linear network coding over finite fields in terms of achieving a solution over a lesser sized alphabet. Moreover, we leave an open problem that whether rings are also superior, again in terms of alphabet size, when the objective is to achieve a vector linear solution. That is, whether there exists a network which, for some positive integer d, has a d-dimensional vector linear solution over a finite field if only if the size of the finite field is at least n, but has d-dimensional vector linear solution over a ring whose size is strictly less than n.

It is known that a network may have a d-dimensional vector linear solution over $\mathbb{F}_q$, but have no scalar linear solution over any finite field whose size is less than or equal to q^d. We showed that for any prime number p, there exists a non-multicast network which has a scalar linear solution if and only if the size of the finite field is a power of the p, but has a 2-dimensional vector linear solution over all finite fields. This shows new extremes of the reduction in finite field size requirement that can be achieved by using vector linear network coding.

In Chapter 5, we showed three new sets of characteristic dependent linear rank inequalities. For a network whose linear coding capacity is different over different finite fields, neither linear rank inequalities that hold over all finite fields nor information inequalities (or their combination) can produce different upper-bounds over different characteristics. For such networks, characteristic dependent linear rank inequalities can be used to find upper-bounds on the linear coding capacity over a given characteristic of the finite field.

The works of Chapter 5 puts more light on the known *DFZ method* used in the literature to produce characteristic-dependent linear rank inequalities that hold in general, but obtained from example networks. A problem that remains open is: can these inequalities be systematically generated, and how hard that process would be. Such an algorithm could also be used to test whether a given network's linear coding capacity varies with the characteristic of the finite field.

Another question that remains open is that whether linear rank inequalities can also capture the fact that a network may have a vector linear solution but have no scalar linear solution. Also, now as we have shown in Chapter 4 that the set of characteristics over which a network has an m-dimensional vector linear solution depends upon m, can linear rank inequalities capture this fact as well.

भारतीय प्रौद्योगिकी संस्थान गुवाहाटी
Indian Institute of Technology Guwahati

Bibliography

[1] 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.

[2] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE Transactions on Information Theory*, vol. 11, no. 5, pp. 782–795, 2003.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] T. Ho, M. Mdard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[8] 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.

[9] Q. T. Sun, X. Yang, K. Long, X. Yin, and Z. Li, "On vector linear solvability of multicast networks," *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 5096–5107, 2016.

[10] T. Etzion and A. Wachter-Zeh, "Vector network coding based on subspace codes outperforms scalar linear network coding," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 2460–2473, 2018.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] S. Riis and R. Ahlswede, *Problems in Network Coding and Error Correcting Codes*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 861–897.

[16] 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.

[17] 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.

[18] 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. 2303–2316, 2008.

[19] 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.

[20] R. Dougherty, C. Freiling, and K. Zeger, "Linearity and solvability in multicast networks," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2243–2256, 2004.

[21] J. Connelly and K. Zeger, "A class of non-linearly solvable networks," *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 201–229, 2017.

[22] 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.

[23] R. Dougherty, C. Freiling, and K. Zeger, "Non-shannon information inequalities in four random variables," *Arxiv*, 2011. [Online]. Available: https://arxiv.org/abs/1104.3602

[24] T. Chan and A. Grant, "Non-linear information inequalities," *Entropy*, vol. 10, no. 4, pp. 765–775, 2008.

[25] F. Matus, "Infinitely many information inequalities," in *IEEE International Symposium on Information Theory (ISIT)*, 2007.

[26] D. Hammer, A. E. Romashchenko, A. Shen, and N. K. Vereshchagin, "Inequalities for shannon entropy and kolmogorov complexity," *Journal of Computer and System Sciences*, vol. 60, pp. 442–464, 2000.

[27] Z. Zhang and R. W. Yeung, "On characterization of entropy function via information inequalities," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1440–1452, 1998.

[28] 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.

[29] R. Dougherty, C. Freiling, and K. Zeger, "Linear rank inequalities on five or more variables," *Arxiv*, 2009. [Online]. Available: https://arxiv.org/abs/0910.0284v3

[30] R. Dougherty, "Computations of linear rank inequalities on six variables," in *IEEE International Symposium on Information Theory (ISIT)*, 2014.

[31] A. Blasiak, R. Kleinberg, and E. Lubetzky, "Lexicographic products and the power of non-linear network coding," *Arxiv*, 2011. [Online]. Available: https://arxiv.org/abs/1108.2489

[32] R. Dougherty, C. F. Freiling, and K. Zeger, "Achievable rate regions for network coding," *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2488–2509, 2015.

[33] R. Dougherty, E. Freiling, and K. Zeger, "Characteristic-dependent linear rank inequalities with applications to network coding," *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2510–2530, 2015.

[34] E. F. Freiling, "Characteristic dependent linear rank inequalities and applications to network coding," Ph.D. dissertation, University of California, San Diego, 2014. [Online]. Available: https://escholarship.org/uc/item/396999zr.pdf

[35] 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.

[36] S. E. Rouayheb, A. Sprintson, and C. Georghiades, "On the index coding problem and its relation to network coding and matroid theory," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3187–3195, 2010.

[37] J. G. Oxley, *Matroid theory*. Oxford University Press, 1992.

[38] A. Kim and M. Médard, "Scalar-linear solvability of matroidal networks associated with representable matroids," in *6th International Symposium on Turbo Codes and Iterative Information Processing (ISTC)*, 2010.

[39] J. Herzog and T. Hibi, "Discrete polymatroids," *Journal of Algebraic Combinatorics, 16*, vol. 16, no. 3, pp. 239–268, 2002.

[40] M. Vlădoiu, "Discrete polymatroids," *Analele Stiintifice ale Universitatii Ovidius Constanta*, vol. 14, no. 2, pp. 97–120, 2006.

[41] A. R. Lehman and E. Lehman, "Complexity classification of network information flow problems," in *41st Annu. Allerton Conf. Communication Control and Computing, Monticello, IL, USA*, 2003.

[42] S. Riis, "Linear versus nonlinear boolean functions in network flow," in *38th Annual Conference on information Sciences and Systems (CISS), Princeton, New Jersey, USA*, 2004.

[43] S. E. Rouayheb, A. Sprintson, and C. Georghiades, "On the relation between the index coding and the network coding problems," in *IEEE International Symposium on Information Theory (ISIT)*, 2008.

[44] 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.

[45] A. W. Ingleton, "Representation of matroids," in *Combinatorial mathematics and its applications*, D. J. A. Welsh, Ed., 1971, pp. 149–167.