



Master's Thesis

Vector Network Coding Gap Sizes for the Generalized Combination Network

Vorgelegt von:

Ha Nguyen

München, 08 2019

Betreut von:

Sven Puchinger

Master's Thesis am
Coding for Communications and Data Storage (COD)
der Technischen Universität München (TUM)
Titel : Vector Network Coding Gap Sizes for the Generalized Combination Network
Autor : Ha Nguyen

Ha Nguyen
Sintperstr. 50
81539 München
ha.nguyen@tum.de

Ich versichere hiermit wahrheitsgemäß, die Arbeit bis auf die dem Aufgabensteller bereits bekannte Hilfe selbständig angefertigt, alle benutzten Hilfsmittel vollständig und genau angegeben und alles kenntlich gemacht zu haben, was aus Arbeiten anderer unverändert oder mit Abänderung entnommen wurde.

München, 05.08.2019

.....

Ort, Datum

(Ha Nguyen)

Contents

1	Introduction	1
2	Preliminaries	3
2.1	Notation and Basic Terminology	3
2.2	Definition	4
2.3	Theorem	5
3	Network Coding	7
3.1	What is Network Coding?	7
3.2	Advantages of Network Coding	8
3.3	Network as a matrix channel	10
3.4	Network Model	11
3.4.1	Multicast Networks as Generalized Combination Networks	11
3.4.2	Comparison between scalar and vector solutions by the gap size	12
4	Generalized combination Network	15
4.1	Description	15
4.2	Network Coding for This Network	16
4.2.1	Scalar network coding	16
4.2.2	Vector network coding	17
4.3	Instances of Generalized Combination Network	18
4.3.1	The $(\ell - 1)$ -Direct Links and ℓ -Parallel Links $\mathcal{N}_{h=2\ell, r, s=3\ell-1}$ Network	19
4.3.2	The 1-Direct Link and ℓ -Parallel Links $\mathcal{N}_{h=2\ell, r, s=2\ell+1}$ Network	19
4.3.3	The ϵ -Direct Links $\mathcal{N}_{h, r, s}$	20
4.3.4	The $(\epsilon = 0, \ell = 1) - \mathcal{N}_{h, r, s}$ Combination Network	21
4.3.5	The Largest Possible Gap between q_v and q_s in Previous Studies	21
5	Combinatorial Results	23
5.1	$(\epsilon = 1, \ell = 1) - \mathcal{N}_{h=3, r, s=4}$ Network	23
5.2	$(\epsilon = 1, \ell = 1) - \mathcal{N}_{h, r, s}$ Network	29
5.2.1	Find the lower bound of $r_{max, vector}$	29

5.2.2	Find the Upper Bound of $r_{max,scalar}$	31
5.2.3	Calculate Gap	32
5.3	$(\epsilon = 1, \ell \geq 2) - \mathcal{N}_{h=2\ell, r, s=2\ell+1}$	32
6	Computational Results	35
6.1	Main Approach	35
6.2	Alternative Approaches	40
7	Conclusion	43
8	Appendix	45
	Bibliography	I

List of Figures

3.1	Incoming links and outgoing links of a node in network coding	7
3.2	The butterfly network	8
3.3	The butterfly network is represented as a combination network	12
4.1	The generalized network $(\epsilon, \ell) - \mathcal{N}_{h,r,s}$	15
4.2	The mapping of scalar solution over $\mathbb{F}_{q_s=q^t}$ to the equivalent vector solution	18
4.3	The $(1, 2) - \mathcal{N}_{4,r,5}$ network as an example of the $(\ell - 1, \ell) - \mathcal{N}_{2\ell,r,3\ell-1}$. .	19
4.4	The $(\ell - 1, \ell) - \mathcal{N}_{2\ell,r,3\ell-1}$ network	20
4.5	The $(\epsilon \geq 1, \ell = 1) - \mathcal{N}_{h,r,s}$ network	20
4.6	The $(\epsilon = 0, \ell = 1) - \mathcal{N}_{h,r,s}$ combination network	21
5.1	The $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h=3,r,s=4}$ network	23
5.2	The vector network coding of $(\epsilon = 1, l = 1) - \mathcal{N}_{h=3,r,s=4}$ represents as a matrix problem	24
6.1	The vector network coding of $(\epsilon = 1, l = 1) - \mathcal{N}_{h=3,r,s=4}$ represents as a matrix problem	40

List of Tables

3.1	Notations of network coding	11
4.1	Parameters of network coding	16
4.2	New gap found in this study	22
5.1	r over variations of t	29

1 Introduction

For the traditional way of network coding, scalar solutions are used. However, it was proved in Professor Antonia's paper that vector solutions outperform scalar solutions in specific cases. It means that we can connect more devices into our network, which is especially meaningful for the IOT devices. The overview of networks where vector solutions outperform the scalar solution is described in Chapter X (Not Yet Inserted). Then we consider a case that is unable to solve by subspace codes or rank-metric codes in Chapter 2. Our computational method shows better results than the scalar solution, 67 results and 166 results respectively in case of $t=2$ and $t=3$, where scalar solution has only 42 results and 146 results. The method is described in Chapter 3.

2 Preliminaries

2.1 Notation and Basic Terminology

Vectors and Matrices Vectors \mathbf{v} are denoted by underlined letters. Unless stated otherwise, vectors are indexed starting from 1, i.e. $\mathbf{v} = [v_1, \dots, v_n]$. Vectors are usually considered to be row vectors. Matrices \mathbf{V} are shown in bold and capital letters. Elements of **matrices** or **vectors** are surrounded by square brackets, and elements of **tuples** are surrounded by round brackets.

Vector space A vector space of dimension n over a finite field with q elements is denoted by \mathbb{F}_q^n .

Linear Block Code >>> WHY ONLY LINEAR?

Block codes are finite length codes first studied by Golay [Gol49] and Hamming [Ham50]. A *linear* $[n, k]_q$ *block code* \mathcal{C} of length n , dimension k and codimension (or redundancy) $r = n - k$, is a k -dimensional *linear subspace* of \mathbb{F}_q^n . A *generator matrix* \mathbf{G} has k rows, which form a *basis* of \mathcal{C} , i.e., \mathbf{G} 's row space is a set of k linearly independent vectors generating \mathcal{C} . The codeword $\mathbf{c} \in \mathcal{C}$ is encoded by the *information vector* (or *message*) \mathbf{m} , with $\mathbf{c} = \mathbf{m} \cdot \mathbf{G}$. For any $\mathbf{c} \in \mathcal{C}$: $\mathbf{c} \cdot \mathbf{H}^T = \mathbf{0}$, with \mathbf{H} is a *parity-check matrix* of \mathcal{C} , whose row space generates the $[n, n - k]_q$ dual code \mathcal{C}^\perp . $[n, k, d]_q$ is equivalent to $[n, k]_q$ with minimum distance d fulfills $d = \min_{\mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\}} d(\mathbf{c}, \mathbf{0})$ with respect to a metric $d(\cdot, \cdot) : \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{R}_{\geq 0}$ on \mathbb{F}_q^n ¹.

Maximum Rank Distance (MRD) code >>> EXPLANATION

Gaussian coefficient Gaussian coefficient (also known as q -binomial) counts the number of subspaces of dimension k in a vector space \mathbb{F}_q^n ,

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}$$

¹i.e., $d(\mathbf{x}, \mathbf{y}) \geq 0, d(\mathbf{x}, \mathbf{y}) = 0$ iff $\mathbf{x} = \mathbf{y}$, $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$ and $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}_q^n$.

Multigraph A graph is permitted to have multiple edges. Edges that are incident to same vertices can be in parallel.

Directed Acyclic Graph A finite directed graph with no directed cycles, i.e. it consists of a finite number vertices and edges, with each edge directed from a vertex to another, such that there is no loop from any vertex v with a sequence of directed edges back to the vertex again v .

Multicast Multicast communication supports the distribution of a data packet to a group of users [ZNK12]. It can be one-to-many or many-to-many distribution [Har08]. In this study, we consider only one-to-many multicast network.

Asymptotic Behavior For the combinatorial results, we study the asymptotic behaviour of some formulas depending on the alphabet size q and the vector length t , by using the Bachmann-Landau notation, i.e. $\mathcal{O}(f(q, t))$ for upper, $\Theta(f(q, t))$ for tight, and $\Omega(f(q, t))$ for lower bounds, where f is a function of the alphabet size and the vector length.

2.2 Definition

>>> EXPLAIN WHY I NEED EACH DEFINITION?

Definition 2.1 (Grassmannian Code). A Grassmannian code is a set of all subspaces of dimension $k \leq n$ in \mathbb{F}_q^n , and is denoted by $\mathcal{G}_q(n, k)$. Due to being the set of all subspaces that have the same dimension k , it is also called a *constant dimension code*. [EZ19]

Definition 2.2 (Projective Space). The *projective space of order n* is a set of all subspaces of \mathbb{F}_q^n , and is denoted by $\mathcal{P}_q(n)$, i.e. a union of all dimension $k = 0, \dots, n$ subspaces in \mathbb{F}_q^n or $\mathcal{P}_q(n) = \bigcup_{k=0}^n \mathcal{G}_q(n, k)$. [EW18]

Definition 2.3 (Covering Grassmannian Code). An $\alpha - (n, k, \delta)_q^c$ covering Grassmannian code (code in short) \mathcal{C} is a subset of $\mathcal{G}_q(n, k)$ such that each subset of α codewords of \mathcal{C} span a subspace whose dimension is at least $\delta + k$ in \mathbb{F}_q^n . [EZ19]

The cardinality of a Grassmannian code The cardinality of $\mathcal{G}_q(n, k)$ is the Gaussian coefficient (also known as q -binomial), which counts the number of subspaces of dimension k in a vector space \mathbb{F}_q^n ,

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

$$\text{where } q^{(n-k)k} \leq \begin{bmatrix} n \\ k \end{bmatrix}_q \leq 4q^{(n-k)k}.$$

Definition 2.4 (Multiple Grassmannian Code [EKOÖ18]). A $t - (n, k, \lambda)_q^m$ multiple Grassmannian code, i.e. a subspace packing, is a set \mathcal{S} of k -subspaces or k -dimensional subspaces (called *blocks*), such that each t -subspace of \mathbb{F}_q^n is contained in at most λ codewords of \mathcal{C} .

Definition 2.5 ([EKOÖ18]). $\mathcal{A}_q(n, k, t; \lambda)$ denotes the maximum size of a $t - (n, k, \lambda)_q^m$ code, where there are no repeated codewords.

2.3 Theorem

>>> EXPLAIN BEFORE WHY I NEED EACH THEOREM?

Theorem 2.1 ([EZ19]). *If n, k, t and λ are positive integers such that $1 \leq t < k < n$ and $1 \leq \lambda \leq \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q$, then*

$$\mathcal{A}_q(n, k, t; \lambda) \leq \left\lfloor \lambda \frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q} \right\rfloor$$

Theorem 2.2 ([EZ19]). *If n, k, t and λ are positive integers such that $1 \leq t < k < n$ and $1 \leq \lambda \leq \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q$, then*

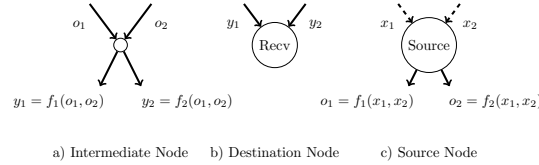
$$\mathcal{A}_q(n, k, t; \lambda) \leq \left\lfloor \frac{q^n - 1}{q^k - 1} \mathcal{A}_q(n-1, k-1, t-1; \lambda) \right\rfloor$$

3 Network Coding

3.1 What is Network Coding?

We first explain the term of network, then we further introduce Network Coding. Our considered communication network is a directed graph¹ allowing multiple links from one node to another. Each *link* in a network has *unit capacity*, i.e. it carries a packet which is either a symbol from \mathbb{F}_{q_s} , or a vector of length t over \mathbb{F}_q . Note that the assumption of unit capacity does not restrict our considered networks in Section 4.1, since links of larger capacity can be represented by multiple parallel links ℓ of a data unit. In Figure 3.1(a), a node of a network is represented with its *incoming* and *outgoing* links. A node without any incoming link is a *source* node of the network. Packets are transmitted from the source to a set of destination nodes, i.e. *receivers*, over error-free links, which is still applicable to present-day wireline networks².

Figure 3.1: Incoming links and outgoing links of a node in network coding



In simple routing, information is transmitted from the source to receivers through a chain of *intermediate nodes* by a method known as store-and-forward [YLCZ06]. In this method, the information transmission can be represented as **packet transmissions** on links and the packets received from an incoming link of an intermediate node, i.e. *incoming packets*, can only be forwarded to a next node via **an outgoing link as its outgoing packets**. *Network coding* was though first introduced in Ahlswede et al.'s seminal paper [ACLY00] as “coding at a node in a network”, where coding means an arbitrary combination of received packets on a node’s incoming links for an outgoing packet. It means that each intermediate node in the network (not only at the source) is allowed to forward a *function* of their

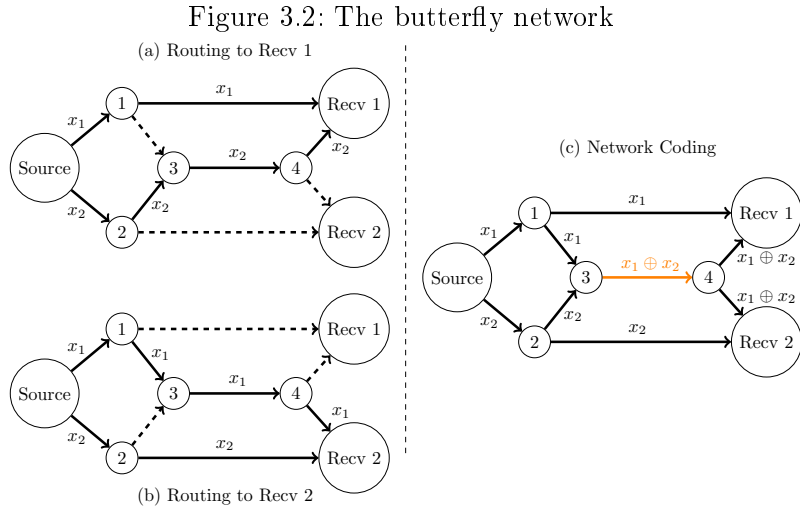
¹Network coding over undirected networks was introduced in [LL04b].

²Wireless network coding was introduced in [KRH⁺08].

incoming packets, e.g. $y_1 = f_1(o_1, o_2)$ in Figure 3.1. These functions are not required to be injective functions, i.e. some outgoing packets can be duplicated from a map of same incoming packets, which motivates our study in Section 5.1. A *network code* is a set of these functions of the packets on the links of the network [EW18]. A network code is called a *solution* for the network or the network is *solvable*, if there exists an assignment of all the functions on all the links of the network such that each receiver can recover its requested packets from its incoming packets. If these functions are linear, we obtain a *linear network coding solution*, and we do not consider *nonlinear solution* throughout this thesis. Each function on a link consists of *coding coefficients* for each incoming packet. The coding coefficients form a coefficient vector whose length is equal to the number of each node's incoming links, and this coefficient vector is called the *local coding vector*, which is distinguished with *global coding vector* defined in Section 3.3. If the coding coefficients and the packets are scalars, a solution of linear network coding is called *scalar solution*. Based on these coding coefficients, Kötter and Médard provided in [KM03] an algebraic formulation for the linear network coding problem and its scalar solvability.

3.2 Advantages of Network Coding

Throughput gain and reduced complexity Network coding gives a potential gain in throughput by communicating more information with fewer packet transmissions compared to the routing method. The butterfly network in [ACLY00] as a multicast in a wireline network is a standard example for an increase of throughput.



In Figure 3.2, we denoted a receiver by “Recv”, which is used for all of figures in this

study. With the help of network coding, both Recv 1 and Recv 2 can recover x_1 and x_2 by a bitwise XOR in Figure 3.2(c). Without network coding, an additional transmission between Node 3 and 4 must be supplemented to communicate the contents of 2 packets x_1 and x_2 from the source to Recv 1 and Recv 2, i.e. we must communicate x_1 or x_2 separately on this link twice under routing in Figure 3.2(a) and (b).

Robustness and security *Packet loss* is a particular issue in wireless packet networks due to several reasons, e.g. **buffer overflow or communication failures** [HL08]. Sharing a common concept with Erasure Coding (EC) by **exploiting** a degree of redundancy to packets on any vertices in the network, the receivers are able to successfully recover the original packets from a large number of packet losses, e.g. $101 \otimes 10 \otimes 1$. The only difference is that packets are only encoded by the source in EC [FOG08]. This problem is dealt by acknowledgement messages in the mechanism of transmission control protocol (TCP) [HL08]. Network coding offers both benefits and drawbacks regarding to security. For example, node 4 is operated by an eavesdropper and it obtains only the packet $x_1 \oplus x_2$, so it cannot obtain either x_1 or x_2 and the communication is secure. Alternatively, if the eavesdropper controls node 3, it can anonymously send a fake packet masquerading as $x_1 \oplus x_2$, which is difficult to detect in network coding [HL08].

From scalar network coding to vector network coding Ebrahimi and Fragouli [EF11] have extended the algebraic approach in [KM03] to *vector network coding*. Here, all packets are vectors of length t , and the coding coefficients are $[t \times t]$ matrices. The network code is therefore a set of functions consisting of $[t \times t]$ coding matrices, and is called *vector solution* if all receivers can recover their requested information for such coding matrices. The motivation of vector network coding is that there exists networks do not have scalar solutions, but are solvable by vector routing, e.g [MEKH03]. Although it was shown that not every solvable network has a vector solution in [DFZ05, Lemma II.2], Das and Rai proved in [DR16] that there exists a network with a vector solution of dimension m but **with no vector solution over any finite field whose the dimension is less than m** . When we refer the *alphabet size* of a network coding solution, we mean the field size q_s or q_v of the finite field \mathbb{F}_{q_s} or \mathbb{F}_{q_v} respectively for such a scalar solution or a vector solution. The alphabet size is an important parameter determining the amount of computation performed at each network vertice [EW18]. The problem of finding the minimum required alphabet size of a (linear or nonlinear) scalar network code for a certain multicast network is NP-complete [LS09, LL04a, GLS18]. This thesis focuses on determining the solvability of networks to measure the gap, and our considered networks in Section 4.1 consist only error-free links, we therefore do not consider error correction here. Furthermore, we consider

the solvability of networks by proving an existence of an assignment for all functions such that all receiver can recover its requested information, so the functions or coding coefficients are clearly chosen **instead of being arbitrary or random as the ones used in [HKM⁺03, ACLY00]**. We later distinguish scalar and vector network coding more specifically in Section 3.3 and 4.2.

3.3 Network as a matrix channel

To formulate a network coding problem, the source has a set of disjoint messages referred to packets on links which are either symbols from \mathbb{F}_{q_s} (scalar coding) or vectors of length t over \mathbb{F}_q (vector coding) as mentioned in Section 3.1. Each receiver $R_j, j \in \{1, \dots, N\}$ requests a subset of same h messages from the source. Through all the functions on the links from the source to each receiver, the receiver obtains several linear combinations of the h messages to form a linear system of equations for its requested messages. The coefficients of a linear combination is called *global coding vector* [SET03]. The linear equation system that any receiver R_j has to solve is as following:

$$\begin{array}{c|c} \text{Scalar} & \text{Vector} \\ \hline \underbrace{\begin{bmatrix} y_{j_1} \\ \vdots \\ y_{j_s} \end{bmatrix}}_{\mathbb{F}_{q_s}^s} = \underbrace{\mathbf{A}_j}_{\mathbb{F}_{q_s}^{s \times h}} \cdot \underbrace{\begin{bmatrix} x_1 \\ \vdots \\ x_h \end{bmatrix}}_{\mathbb{F}_{q_s}^h} & \underbrace{\begin{bmatrix} \mathbf{y}_{j_1} \\ \vdots \\ \mathbf{y}_{j_s} \end{bmatrix}}_{\mathbb{F}_q^{st}} = \underbrace{\mathbf{A}_j}_{\mathbb{F}_q^{st \times th}} \cdot \underbrace{\begin{bmatrix} \mathbf{x}_1 \\ \vdots \\ \mathbf{x}_h \end{bmatrix}}_{\mathbb{F}_q^{th}} \end{array} \quad (3.1)$$

The transfer matrix \mathbf{A}_j contains the links' global coding vectors, which are combined by the coefficients of linear combinations on αl links from α nodes and ϵ direct-links to the corresponding receiver R_j :

$$\mathbf{A}_j = \begin{array}{c|c} \text{Scalar} & \text{Vector} \\ \hline \begin{bmatrix} \mathbf{a}_{j_1} \\ \vdots \\ \mathbf{a}_{j_{\alpha l}} \\ \vdots \\ \mathbf{a}_{j_{\alpha l + \epsilon}} \end{bmatrix} & \begin{bmatrix} \mathbf{A}_{j_1} \\ \vdots \\ \mathbf{A}_{j_{\alpha l}} \\ \vdots \\ \mathbf{A}_{j_{\alpha l + \epsilon}} \end{bmatrix} \end{array}$$

In general, the network is represented as a matrix channel for both scalar and vector coding: $\mathbf{Y}_j = \mathbf{A}_j \cdot \mathbf{X}$. In our study, the network structure is known, i.e. we reconstruct \mathbf{X} with knowing \mathbf{A}_j , so our network is coherent. A network is *solvable* or a network code is a *solution*, if each receiver can reconstruct its requested messages or solve the system

with a unique solution for scalars x_1, \dots, x_h , or vectors $\mathbf{x}_1, \dots, \mathbf{x}_h$. In network coding problems, we want to find global coding vectors such that the matrix \mathbf{A}_j has full-rank for every $j = 1, \dots, N$, and such that q_s or q^t is minimized as mentioned in Section 3.2. In Example 4.1, we provide a vector solution of field size q and dimension t , which has the same alphabet size as a scalar solution of field size q^t .

To summarize the notations of both scalar and vector coding, we represent them as in Table 3.1:

Table 3.1: Notations of network coding

	Scalar Coding	Vector coding
Source Messages/Packets	$x_1, \dots, x_h \in \mathbb{F}_{q_s}$ $\mathbf{x} \in \mathbb{F}_{q_s}^h$	$\mathbf{x}_1, \dots, \mathbf{x}_h \in \mathbb{F}_q^t$ $\mathbf{x} \in \mathbb{F}_q^{th}$
Global Coding Vectors Of Receiver R_j	$\mathbf{a}_{j_1}, \dots, \mathbf{a}_{j_s} \in \mathbb{F}_{q_s}^h$	$\mathbf{A}_{j_1}, \dots, \mathbf{A}_{j_s} \in \mathbb{F}_q^{t \times th}$
Transfer Matrix Of Receiver R_j	$\mathbf{A}_j \in \mathbb{F}_{q_s}^{s \times h}$	$\mathbf{A}_j \in \mathbb{F}_q^{st \times th}$
Packets On Receiver R_j	$y_{j_1}, \dots, y_{j_s} \in \mathbb{F}_{q_s}$ $\mathbf{y} \in \mathbb{F}_{q_s}^s$	$\mathbf{y}_{j_1}, \dots, \mathbf{y}_{j_s} \in \mathbb{F}_q^t$ $\mathbf{Y}_j \in \mathbb{F}_q^{st}$
Number of nodes	r_{scalar}	r_{vector}

Remark 3.1. By using the vector coding, the upper bound number of solutions increases from q^{tkh} to q^{t^2kh} . Therefore, vector network coding offers more freedom in choosing the coding coefficients than does scalar linear coding for equivalent alphabet sizes, and a smaller alphabet size might be achievable [EF11]. By this advantage, we can have higher number of receivers, i.e. higher number of nodes, in vector network coding.

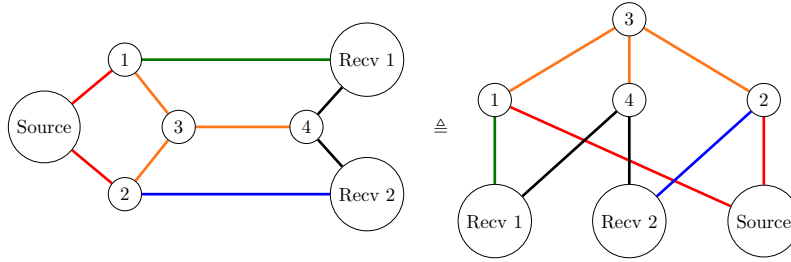
3.4 Network Model

3.4.1 Multicast Networks as Generalized Combination Networks

A class of networks which is mainly studied is the class of multicast networks. It can be one-to-many or many-to-many distribution [Har08]. In this study, we target one-to-many multicast network with the distribution of a data packet to a group of users [ZNK12]. An interesting network structure often used for multicast networks in network coding is called Combination Network (CN) and denoted by $\mathcal{N}_{h,r,s}$. Many examples in previous studies demonstrating the advantage of network coding have used structures identical or similar to that of CN. We mention a few examples to emphasize CN's importance in the study of

network coding. In Figure 3.3, the butterfly network that is often used as a first example to motivate network coding, e.g. [ACLY00, Fig. 7] and [SET03, Fig. 1], is isomorphic to $\mathcal{N}_{h,r=3,s=2}$, if we consider it as an undirected network [MLL12]. The $\mathcal{N}_{h,r=3,s=2}$ itself was also used in the first study of network coding [ACLY00]. Other CNs, i.e. $\mathcal{N}_{h,r=4,s=2}$ and $\mathcal{N}_{h,r=6,s=3}$, were also used as examples to demonstrate the advantage of network coding in [SET03, Fig. 2] and [JSC⁺05, Fig. 2] respectively. The general structure of CN was also introduced and discussed in [FS06, Sec. 4.3], [YLCZ06, Sec. 4.1], [NY, XMA07].

Figure 3.3: The butterfly network is represented as a combination network



A generalization of a CN [RA06] is called generalized combination network (GCN). GCN defined in [EW16, EW18] was used to prove that vector network coding outperforms scalar linear network coding, in multicast networks, with respect to the *alphabet size*, using rank-metric codes and Grassmannian codes. A comparison between the required alphabet size for a scalar linear solution, a vector solution, and a scalar nonlinear solution, of the same multicast network is an important problem. Etzion and Wachter-Zeh introduced a *gap* in [EW16] as the difference between the smallest alphabet size for which a scalar linear solution exists and the smallest alphabet size for which they can construct a vector solution. They have found bounds on the gap for several network families of GCN in [EW16, EW18], but no gap for the GCN networks with 3 messages has been found, i.e. $(1, 1) - \mathcal{N}_{3,r,4}$, where we denote GCN by $(\epsilon, l) - \mathcal{N}_{h,r,s}$. Therefore, a combinatorial approach is first introduced in this thesis to prove an existence of a vector solution outperforming the optimal scalar linear solution with $q^{t^2/4 + \mathcal{O}(t)}$. We then further extend the approach for a family of GCN called One-Direct Link Combination Network, i.e. $(1, 1) - \mathcal{N}_{h,r,s}$. More formal definitions of the gap and GCN can be found in Section 4.1.

3.4.2 Comparison between scalar and vector solutions by the gap size

The *gap* represents the difference between the smallest field (alphabet) size for which a scalar linear solution exists and the smallest alphabet size for which we can construct a vector solution. In this study, we define a solvable vector network coding over the field size

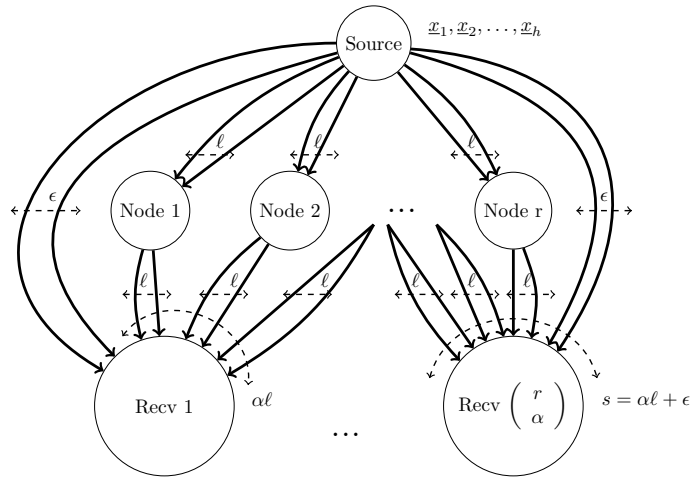
\mathbb{F}_q^t , and we find the lower bound of the maximum number of nodes such vector solution can achieve, i.e. $r_{max,vector} \geq f_1(q, t)$, with $f_1 : \mathbb{Z} \mapsto \mathbb{Z}$. Meanwhile, we has a scalar solution for the same network existing if and only if: $r_{scalar} \leq f_2(q_s)$, with $f_2 : \mathbb{Z} \mapsto \mathbb{Z}$. To find the field size q_s required for a scalar solution to reach the maximum achievable vector solution's nodes in this setting, we consider $r_{max,scalar} = f_2(q_s) = f_1(q, t) = \min[r_{max,vector}]$. Finally, we calculate the gap by $g = q_s - q_v = q_s - q^t$. Throughout this study, we show that vectors solutions significantly reduce the required alphabet size by this gap.

4 Generalized combination Network

4.1 Description

A generalized combination network $(\epsilon, \ell) - \mathcal{N}_{h,r,s}$ consists of 3 components over 3 layers from top to bottom: “Source” in the first layer, “Intermediate Nodes” in the middle layer, and “Receiver” in the third layer. Because “Source” and “Receiver” have their own names without previous confusion of a source node or a destination node, we replace “Intermediate Nodes” by “Nodes” from this section. The network has a source with h messages, r nodes, and $\binom{r}{\alpha}$ receivers, which form a single source multicast network modeled as a finite directed acyclic multigraph [LYC03]. The source connects to each node by ℓ parallel links and each node also connects to a receiver by ℓ parallel links, which are respectively called a node’s incoming and outgoing links. Each receiver is connected by s links in total, specifically $\alpha\ell$ links from α nodes and ϵ direct links from the source, i.e. $s = \alpha\ell + \epsilon$. The combination network in [RA06] is the $(0, 1) - \mathcal{N}_{h,r,s}$ network and the $(1, 1) - \mathcal{N}_{h,r,s}$ network is called One-Direct Link Combination Network. Theorem 1 shows our interest of relations between the parameters h, α, ϵ and ℓ . Following to Theorem 4.1, we are interested in networks parameters satisfying this condition: $\ell + \epsilon + 1 \leq h \leq \alpha\ell + \epsilon$.

Figure 4.1: The generalized network $(\epsilon, \ell) - \mathcal{N}_{h,r,s}$



Theorem 4.1 ([EW18]). *The $(\epsilon, \ell) - \mathcal{N}_{h,r,s}$ network has a trivial solution if $\ell + \epsilon \geq h$, and it has no solution if $\alpha\ell + \epsilon < h$.*

Proof: Following to the network coding max-flow min-cut theorem for multicast networks, the maximum number of messages from the source to each receiver is equal to the smallest min-cut between the source and any receiver. For our considered network, s links have to be deleted to disconnect the source from the receiver, which implies that the min-cut between the source and each receiver is at least s . Hence, $h \leq s \Leftrightarrow h \leq \alpha\ell + \epsilon$ \square

There exist at least $\ell + \epsilon$ disjoint links connected to each receiver. If $\ell + \epsilon \geq h$, each receiver can always reconstruct its requested messages on its links. Then we only need to do routing to select paths for the network. \square

Table 4.1: Parameters of network coding

h	The number of source messages
r	The number of nodes in the middle layer
$\begin{pmatrix} r \\ \alpha \end{pmatrix}$	The number of receivers
ℓ	The source connects to each node by ℓ parallel links, and each node also connects to one receiver by ℓ parallel links
α	A receiver is connected by any α nodes in the middle layer
ϵ	The source additionally connects to each receiver by ϵ direct parallel links
s	Each receiver is connected by s links in total, with $s = \alpha\ell + \epsilon$.

4.2 Network Coding for This Network

We start describing a difference of a source message used in scalar network coding and vector network coding. Then we find a condition for an existence of a scalar solution and a vector solution respectively. For the $(\epsilon, \ell) - \mathcal{N}_{h,r,s}$ network, the *local* and *global* coding vectors are the same, because the nodes are simplified to forward their received packets and only the source has its functions on its messages.

4.2.1 Scalar network coding

A message or a packet is equivalent to a symbol over \mathbb{F}_{q_s} . As a network of the multicast model, all receivers request the same h symbols at the same time [HT13]. A transmission

of h data units is a 1-dimensional subspace of $\mathbb{F}_{q_s}^h$. Each receiver therefore must obtain a subspace of $\mathbb{F}_{q_s}^h$, whose dimension is at least h , to be able to reconstruct the packet. Through ϵ direct links connected from the source to a receiver, the source can provide any required ϵ 1-dimensional subspaces of $\mathbb{F}_{q_s}^h$ for the corresponding receiver. Each receiver can accordingly reconstruct the packet if and only if the linear span of α ℓ -dimensional subspaces of $\mathbb{F}_{q_s}^h$ from the nodes is at least of dimension $h - \epsilon$. When this necessary condition is satisfied, the network is said to have a *solution* or to be *solvable*.

Theorem 4.2 ([RA06]). *The $(0, 1) - \mathcal{N}_{h,r,s}$ network has a solution if and only if there exists an $(r, |\mathbb{F}_{q_s}|, h, r - \alpha + 1)$ $|\mathbb{F}_{q_s}|$ -ary error correcting code.*

Theorem 4.3 ([EZ19]). *The $(\epsilon, \ell) - \mathcal{N}_{h,r,s=\alpha\ell+\epsilon}$ network is solvable over \mathbb{F}_q if and only if there exists an $\alpha - (h, \ell, h - \ell - \epsilon)_q^c$ code with r codewords.*

4.2.2 Vector network coding

In vector network coding, a message or a packet is a vector of length t over \mathbb{F}_q . A vector solution is therefore over field size q and dimension t . Such a vector solution has the same alphabet size as a scalar solution of field size q^t , and we denote $q_v = q^t$. A mapping from the scalar solution of field size q^t to an equivalent vector solution is represented in Example 4.1. Similarly with the scalar *linear* coding solution, each receiver can reconstruct its requested packet if and only if any α (ℓt) -dimensional subspaces span a subspace of dimension at least $(h - \epsilon)t$.

Theorem 4.4 ([EZ19]). *A vector solution for the $(\epsilon, \ell) - \mathcal{N}_{h,r,s}$ network exists if and only if there exists $\mathcal{G}_q(ht, \ell t)$ such that any α subspaces of the set span a subspace of dimension at least $(h - \epsilon)t$.*

Theorem 4.5 ([EZ19]). *The $(\epsilon, \ell) - \mathcal{N}_{h,r,s=\alpha\ell+\epsilon}$ network is solvable with vectors of length t over \mathbb{F}_q if and only if there exists an $\alpha - (ht, \ell t, ht - \ell t - \epsilon t)_q^c$ code with r codewords.*

Corollary 4.1. *The $\alpha - (n = ht, n - k = ht - \ell t, \lambda = ht - \ell t - \epsilon t)_q^m$ code formed from the dual subspaces of the $\alpha - (n = ht, k = \ell t, \lambda = ht - \ell t - \epsilon t)_q^c$ code yields the upper bound of $\mathcal{A}_q(n = ht, n - k = ht - \ell t, \alpha; \lambda)$ as maximum number of nodes for a vector network coding of the $(\epsilon, \ell) - \mathcal{N}_{h,r,s}$ network.*

Example 4.1. Given $h = 3, q = 2, t = 2$, we consider the extension field $\mathbb{F}_{q^t=2^2}$. This example shows how mapping messages from scalar coding to vector coding.

Figure 4.2: The mapping of scalar solution over \mathbb{F}_{q^t} to the equivalent vector solution

$$\underline{x} = \begin{matrix} \uparrow \\ \square \\ \square \\ \vdots \\ \square \\ \downarrow \end{matrix} \begin{matrix} h \\ \vdots \end{matrix} \in \mathbb{F}_{q^t}^h \mapsto \underline{x} = \begin{matrix} \uparrow \downarrow \\ \square \\ \uparrow \downarrow \\ \square \\ \vdots \\ \uparrow \downarrow \\ \square \\ \downarrow \end{matrix} \begin{matrix} t \\ \vdots \\ ht \\ t \end{matrix} \in \mathbb{F}_q^{t \cdot h}$$

We use the table of the extension field \mathbb{F}_{2^2} with the primitive polynomial $f(x) = x^2 + x + 1$:

power of α	polynomial	binary vector
-	0	00
α^0	1	01
α^1	α	10
α^2	$\alpha + 1$	11

For scalar coding, the messages are $x_1, \dots, x_{h=3} \in \mathbb{F}_{2^2}$, and for vector coding the messages are $\mathbf{x}_1, \dots, \mathbf{x}_{h=3} \in \mathbb{F}_2^2$. From the polynomial column, let's choose arbitrarily a scalar vector $\mathbf{x}_{scalar} = (x_1, x_2, x_3) = (1, \alpha, \alpha + 1)$. Then, we map it to $\mathbf{x}_{vector} = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$ by using the binary vector column as following:

$$\begin{bmatrix} x_1 = 1 \\ x_2 = \alpha \\ x_3 = \alpha + 1 \end{bmatrix} \mapsto \begin{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \end{bmatrix},$$

where we use the following rule for mapping x_i individually: $a_0 \cdot \alpha^0 + a_1 \cdot \alpha^1 + \dots + a_{t-1} \cdot$

$$\alpha^{t-1} \mapsto \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix}.$$

4.3 Instances of Generalized Combination Network

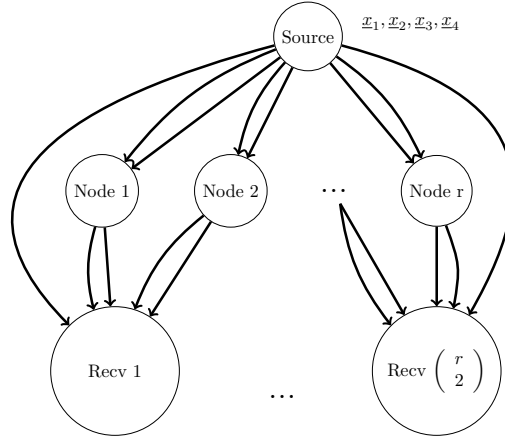
The subsection lists all instances of the $(\epsilon, \ell) - \mathcal{N}_{h,r,s}$ network used by Etzion and Wachter-Zeh in [EW18] to derive bounds on the corresponding network's gaps between scalar

and vector network coding. They cover small and large values of the pair (ϵ, ℓ) , i.e. $(\epsilon = 0, \ell = 1)$, $(\epsilon = 1, \ell)$, $(\epsilon, \ell = 1)$ and $(\epsilon = \ell - 1, \ell)$. In Section 5.2, we study another interesting case $(\epsilon = 1, \ell = 1)$.

4.3.1 The $(\ell - 1)$ -Direct Links and ℓ -Parallel Links $\mathcal{N}_{h=2\ell, r, s=3\ell-1}$ Network

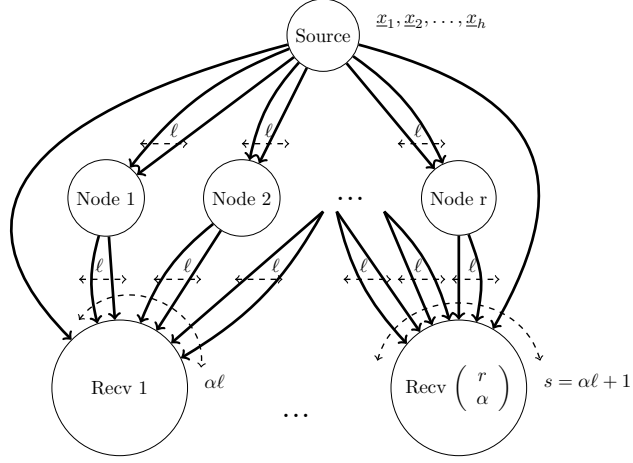
This network family is denoted by $(\ell - 1, \ell \geq 2) - \mathcal{N}_{2\ell, r, 3\ell-1}$. This family contains the largest number of direct links from the source to the receivers among all families of GCN. Its vector solution can be provided by an $\mathcal{MRD}[\ell t \times \ell t, t]_q$ code for any $r_{vector} \leq q^{\ell(\ell-1)t^2 + \ell t}$. There is a scalar solution for this network, if and only if $r_{scalar} \leq \begin{bmatrix} 2\ell \\ \ell \end{bmatrix}_{q_s} < 4_{q_s}^{\ell^2}$. Therefore, the gap tends to $q^{t^2 + \mathcal{O}(t)}$ for large ℓ .

Figure 4.3: The $(1, 2) - \mathcal{N}_{4, r, 5}$ network as an example of the $(\ell - 1, \ell) - \mathcal{N}_{2\ell, r, 3\ell-1}$



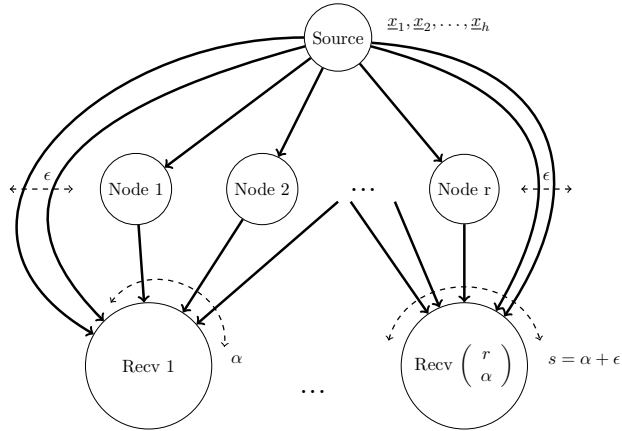
4.3.2 The 1-Direct Link and ℓ -Parallel Links $\mathcal{N}_{h=2\ell, r, s=2\ell+1}$ Network

We denote this network family by $(1, \ell \geq 2) - \mathcal{N}_{2\ell, r, 2\ell+1}$. This network family is the family with the smallest number of direct links, such that Etzion and Wachter-Zeh's vector solution outperforms the optimal scalar solution, i.e. an vector solution outperforming the optimal scalar has not yet been found for the network $(0, \ell \geq 2) - \mathcal{N}_{h, r, s}$. When $\ell \geq 2$ or $h \geq 4$, they proved that this network has a vector solution based on an $\mathcal{MRD}[\ell t \times \ell t, (\ell - 1)t]_q$ code when $r = q^{\ell t(t+1)}$, and scalar solutions only if $q_s > q^{t^2/2}$. Therefore, this network has a gap tending to $q^{t^2/2 + \mathcal{O}(t)}$ with a vector solution.

Figure 4.4: The $(\ell - 1, \ell) - \mathcal{N}_{2\ell, r, 3\ell-1}$ network


4.3.3 The ϵ -Direct Links $\mathcal{N}_{h, r, s}$

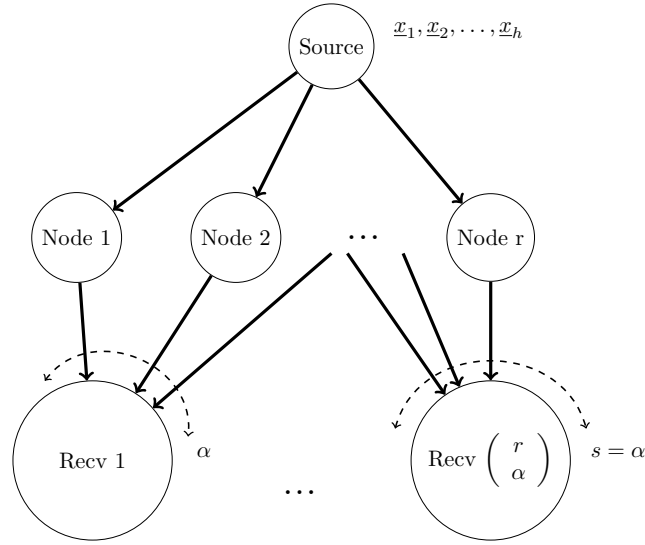
This network family is denoted by $(\epsilon \geq 1, \ell = 1) - \mathcal{N}_{h, r, s}$ and is the main focus of this thesis, because it motivates some interesting questions on a classic coding problem and on a new type of subspace code problem. Furthermore, there is no gap size is known for this network in previous studies. In Section 5.1, we show that there exists vector solutions generating the gaps $g = q^{t^2/4 + \mathcal{O}(t)}$ and $g = q^{\frac{\alpha-h+1}{(\alpha-1)(\alpha-h+2)(h-2)}t^2 + \mathcal{O}(t)}$ respectively for the $(1, 1) - \mathcal{N}_{3, r, 4}$ network and the $(1, 1) - \mathcal{N}_{h, r, s}$ network.

 Figure 4.5: The $(\epsilon \geq 1, \ell = 1) - \mathcal{N}_{h, r, s}$ network


4.3.4 The $(\epsilon = 0, \ell = 1) - \mathcal{N}_{h,r,s}$ Combination Network

Since the scalar solution for the combination network uses an *MDS* code, a vector solution based on subspace codes must go beyond the *MDS* bound, i.e. Singleton bound $d \leq n - k + 1$, to outperform the scalar one. In paper [EW18, Sec. IV-A, Sec. IX-1,2], it is proved that vector solutions based on subspace codes cannot outperform optimal scalar linear solutions for some combination networks, e.g. $\mathcal{N}_{2,r,2}$, and they conjecture it for all h .

Figure 4.6: The $(\epsilon = 0, \ell = 1) - \mathcal{N}_{h,r,s}$ combination network



4.3.5 The Largest Possible Gap between q_v and q_s in Previous Studies

Etzion and Wachter-Zeh considered 2 cases separately $h \leq 2\ell, \epsilon \neq 0$ and $h \geq 2\ell, \epsilon \neq h - 2\ell$

$h \leq 2\ell$ and $\epsilon \neq 0$

For this network, the number of direct links is at least 1, i.e. $\epsilon \geq 1$, and the number of parallel links is less than half of the number of source messages, i.e. $\ell \leq \frac{h}{2}$.

h is even The above $(\ell - 1, \ell) - \mathcal{N}_{2\ell, r, 3\ell - 1}$ network achieves the largest gap $q_s = q^{(h-2)t^2/h + \mathcal{O}(t)}$.

h is odd The $(\ell - 2, \ell) - \mathcal{N}_{2\ell - 1, r, 3\ell - 2}$ network achieves the largest gap $q_s = q^{(h-3)t^2/(h-1) + \mathcal{O}(t)}$

Table 4.2: New gap found in this study

Network	Gap Bounds for a specific vector solution [EW18]	This study proves an existence of these gaps
$(\epsilon = 0, \ell = 1) - \mathcal{N}_{h,r,s}$	N/A	N/A
$(\epsilon \geq 1, \ell = 1) - \mathcal{N}_{h,r,s}$	Unknown	$q^{\frac{\alpha-h+1}{(\alpha-1)(\alpha-h+2)(h-2)}t^2 + \mathcal{O}(t)}$ (*)
$(\epsilon = 1, \ell \geq 2) - \mathcal{N}_{h=2\ell,r,s=2\ell+1}$	$q^{t^2/2 + \mathcal{O}(t)}$	$q^{t^2/l + \mathcal{O}(t)}$
$(\epsilon = \ell - 1, \ell) - \mathcal{N}_{h=2\ell,r,s=3\ell-1}$	$q^{t^2/2 + \mathcal{O}(t)}$	N/A

(*): We only consider the $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h,r,s}$ network.

$h \geq 2\ell$ and $\epsilon \neq h - 2\ell$

h is even The same above $(\ell - 1, \ell) - \mathcal{N}_{2\ell,r,3\ell-1}$ network achieves the largest gap $q_s = q^{(h-2)t^2/h + \mathcal{O}(t)}$.

h is odd The $(\ell - 1, \ell) - \mathcal{N}_{2\ell+1,r,3\ell-1}$ network achieves the largest gap $q_s = q^{(h-3)t^2/(h-1) + \mathcal{O}(t)}$.

Remark 4.1. The achieved gap is $q^{(h-2)t^2/h + \mathcal{O}(t)}$ for any $q \geq 2$ and any even $h \geq 4$. If $h \geq 5$ is odd, then the achieved gap of the alphabet size is $q^{(h-3)t^2/(h-1) + \mathcal{O}(t)}$ [EW18].

We are summarizing the instances of GCN with their bounds on gap found in [EW18] and list our findings in this study.

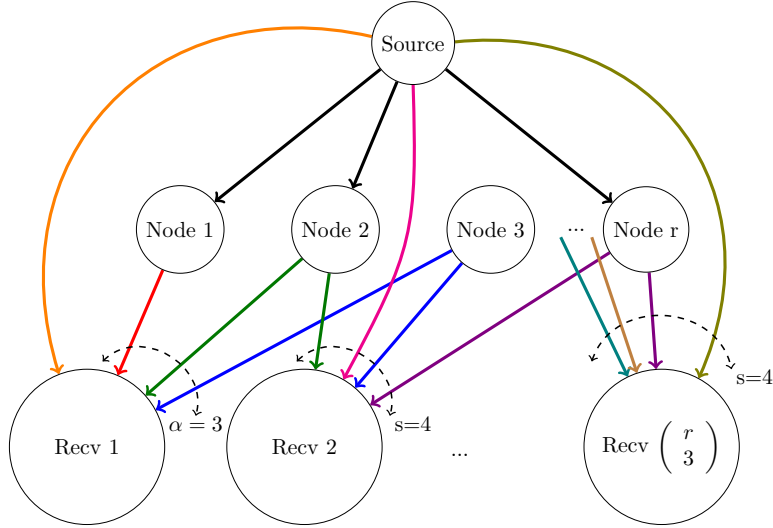
Some of them has global coding vectors as square matrices, so the decoding base easily by inversing such global coding vectors to get each receiver's requested messages. However, we do not go into details of decoding methods in this study.

5 Combinatorial Results

In previous studies [EW18], no general vector solution outperforming scalar network coding was found for multicast networks with $h = 3$ messages. Hence, we start with a probabilistic argument to prove that there exists a vector solution outperforming the optimal linear solution for the $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h=3,r,s=4}$ network. Then we generalize the proof to the $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h,r,s}$ network.

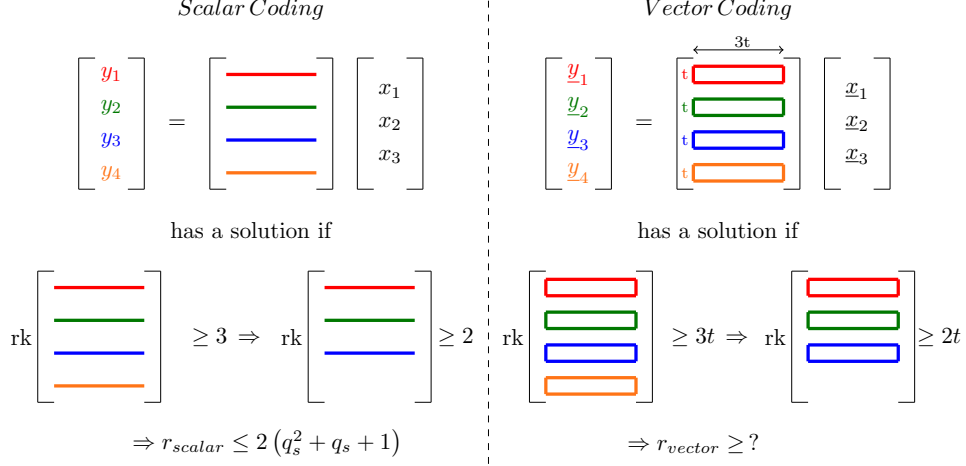
5.1 $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h=3,r,s=4}$ Network

Figure 5.1: The $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h=3,r,s=4}$ network



In this subsection, we derive a lower bound on the maximum number of receivers for the $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h=3,r,s=4}$ network. Due to $\alpha = 3$, the number of receivers is $N = \binom{r_{vector}}{3}$ by definition in Section 4.1. To derive the lower bound, we introduce a rank requirement on incoming packets to each receiver.

Figure 5.2: The vector network coding of $(\epsilon = 1, l = 1) - \mathcal{N}_{h=3, r, s=4}$ represents as a matrix problem



Following to Equation 3.1, each receiver R_j must solve a linear equation system of 3 variables with 4 equations to recover $h = 3$ messages as below:

$$\begin{bmatrix} y_j^{(r_1)} \\ y_j^{(r_2)} \\ y_j^{(r_3)} \\ y_j^{(r_4)} \end{bmatrix} = \mathbf{A}_j \cdot \underline{x} = \begin{bmatrix} \mathbf{A}_j^{(r_1)} \\ \mathbf{A}_j^{(r_2)} \\ \mathbf{A}_j^{(r_3)} \\ \mathbf{A}_j^{(r_4)} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix},$$

with $x_i, y_j^{(v)} \in \mathbb{F}_q^t$, $\mathbf{A}_j^{(r_v)} \in \mathbb{F}_q^{t \times 3t}$ for $v = 1, \dots, 4$, and $\mathbf{A}_j^{(r_1)}, \dots, \mathbf{A}_j^{(r_3)}$ must be distinct.

The network is solvable, if \mathbf{A}_j has full-rank, i.e. \mathbf{A}_{j_v} must satisfy:

$$\text{rk} \begin{bmatrix} \mathbf{A}_j^{(r_1)} \\ \mathbf{A}_j^{(r_2)} \\ \mathbf{A}_j^{(r_3)} \\ \mathbf{A}_j^{(r_4)} \end{bmatrix} \geq 3t$$

Because coding coefficients for $\mathbf{A}_j^{(r_4)}$ can be independently chosen for any receiver R_j , there always exists $\mathbf{A}_j^{(r_4)}$ such that,

$$\text{rk} \begin{bmatrix} \mathbf{A}_j^{(r_1)} \\ \mathbf{A}_j^{(r_2)} \\ \mathbf{A}_j^{(r_3)} \end{bmatrix} \geq 2t \tag{5.1}$$

if and only if $\text{rk}[\mathbf{A}_j] \geq 3t$.

By this constraint, the problem is thus described as below:

$$\min_{rk[\mathbf{A}_j] \geq 3t} r_{vector}$$

$\mathbf{A}_j^{(r_1)}, \mathbf{A}_j^{(r_2)}, \mathbf{A}_j^{(r_3)}$ are matrices formed on any 3 of r links from nodes to receivers, i.e. these 3 matrices are randomly chosen from a set of r matrices. We formalize the problem by an approach with Lovász local lemma, which was initially proposed by Schwartz in [Sch].

Lemma 5.1 (Symmetric Lovász local lemma (LLL) [SCV13]). *A set of events \mathcal{E}_i , with $i = 1, \dots, n$, such that each event occurs with probability at most p . If each event is independent of all others except for at most d of them and $4dp \leq 1$, then: $\Pr \left[\bigcap_{i=1}^n \bar{\mathcal{E}}_i \right] > 0$.*

Lemma 5.2. $p \leq \Theta \left(q^{-t^2-2t-1} \right), \forall t \geq 2$.

Proof. In Lemma 5.1, each event \mathcal{E}_i is a *bad event*, whose occurrence is undesirable. Following to Equation 5.1, such a event occurs when $rk[\mathbf{A}_j] < 3t$, and its probability is bounded by p (with $0 \leq p \leq 1$) as following,

$$\Pr[\mathcal{E}_i] = \Pr \left[rk \begin{bmatrix} \mathbf{A}_j^{(r_1)} \\ \mathbf{A}_j^{(r_2)} \\ \mathbf{A}_j^{(r_3)} \end{bmatrix} < 2t \right] \leq p. \quad (5.2)$$

Regarding to the left-hand side,

$$\begin{aligned} \Pr \left[rk \begin{bmatrix} \mathbf{A}_j^{(r_1)} \\ \mathbf{A}_j^{(r_2)} \\ \mathbf{A}_j^{(r_3)} \end{bmatrix} < 2t \right] &= \sum_{i=0}^{2t-1} \Pr \left[rk \begin{bmatrix} \mathbf{A}_j^{(r_1)} \\ \mathbf{A}_j^{(r_2)} \\ \mathbf{A}_j^{(r_3)} \end{bmatrix} = i \right] \\ &\stackrel{1}{=} \sum_{i=0}^{2t-1} \frac{N_{i,m,n}}{q^{m \cdot n}} \\ &= \sum_{i=0}^{2t-1} \frac{\prod_{j=0}^{i-1} \frac{(q^m - q^j)(q^n - q^j)}{q^i - q^j}}{q^{m \cdot n}} \\ &\stackrel{2}{=} \sum_{i=0}^{2t-1} \frac{\prod_{j=0}^{i-1} \frac{(q^{3t} - q^j)^2}{q^i - q^j}}{q^{9t^2}}. \end{aligned} \quad (5.3)$$

(1): The formula for the number of $[m \times n]$ matrices of rank i over \mathbb{F}_q was proved in [Ove07].

(2): $\mathbf{A}_j^{(r_1)}, \mathbf{A}_j^{(r_2)}, \mathbf{A}_j^{(r_3)}$ vertically together form a $[3t \times 3t]$ matrix.

We consider the numerator of Equation (5.3): $\prod_{j=0}^{i-1} \frac{(q^{3t}-q^j)^2}{q^i-q^j} = \frac{p_N^{(i)}(q)}{p_D^{(i)}(q)} = p^{(i)}(q)$.

Due to i -times product and large t : $\left. \begin{array}{l} \deg(p_N^{(i)}(q)) = q^{i6t} \\ \deg(p_D^{(i)}(q)) = q^{i^2} \end{array} \right\} \Rightarrow p^{(i)}(q) \approx q^{i6t-i^2}$.

Therefore, we have: $\sum_{i=0}^{2t-1} \prod_{j=0}^{i-1} \frac{(q^{3t}-q^j)^2}{q^i-q^j} = \sum_{i=0}^{2t-1} p^{(i)}(q) \approx \sum_{i=0}^{2t-1} q^{i6t-i^2}$.

To maximize the sum, we set derivation of it to 0 and find the corresponding root:

$$\begin{aligned} (i6t - i^2)' &= 0 \\ \Leftrightarrow 6t - 2i &= 0 \\ \Leftrightarrow i &= 3t \end{aligned}$$

However, the upper limit of the sum is $(2t-1)$, which is less than $3t$ for all $t \geq 2$.

$$\Rightarrow \max \left\{ q^{i6t-i^2} : i = 0, 2, \dots, 2t-1 \right\} = q^{i6t-i^2} \Big|_{i=2t-1} = q^{8t^2-2t-1}$$

Hence, by using the exact bound Θ , we have:

$$\begin{aligned} \max_i \left[\sum_{i=0}^{2t-1} p^{(i)}(q) \right] &\in \Theta \left(\max \left\{ q^{i6t-i^2} : i = 1, 2, \dots, 2t-1 \right\} \right) = \Theta \left(q^{8t^2-2t-1} \right) \\ &\Rightarrow \max_i \left[\frac{\sum_{i=0}^{2t-1} p^{(i)}(q)}{q^{9t^2}} \right] \in \Theta \left(q^{-t^2-2t-1} \right) \\ &\Rightarrow p \leq \Theta \left(q^{-t^2-2t-1} \right) \end{aligned}$$

□

Lemma 5.3. $d \leq \frac{3}{2}r^2$.

Proof. Because d is a function of r in our problem, we denote d in Lemma 5.1 specifically by $d(r)$. The Local lemma 5.1 allows dependence among at most $d(r)$ events, i.e. each event considered under the Local lemma must not be independent to each other.

Furthermore, $\mathbf{A}_j^{(r_1)}, \mathbf{A}_j^{(r_2)}, \mathbf{A}_j^{(r_3)}$ are matrices formed on any 3 of r links from nodes to receivers. Assume that 1 of r links is firstly chosen to form the matrix $\mathbf{A}_j^{(r_1)}$, then there are $\binom{r-1}{2}$ possibilities left to choose $\mathbf{A}_j^{(r_2)}$ and $\mathbf{A}_j^{(r_3)}$ from $r-1$ links. However, such a link can also be chosen firstly to form $\mathbf{A}_j^{(r_2)}$ or $\mathbf{A}_j^{(r_3)}$ instead. Therefore, we have an upper bound for $d(r)$ as following,

$$d(r) \leq 3 \cdot \binom{r-1}{2} = 3 \cdot \frac{(r-1)(r-2)}{2} = \frac{3}{2}(r^2 - 3r + 2)$$

$$\Rightarrow d(r) \leq \frac{3}{2}r^2$$

□

Example:

$r \in \{1, 2, 3, 4\}$. Our sample space to draw any 3 matrices with orders has in total $\binom{4}{3} = 4$ samples.

Assume the link 1 is firstly chosen to form the matrix $\mathbf{A}_j^{(r_1)}$, we have $\binom{3}{2} = 3$ possibilities:

$\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix}$. The existence of 1 in $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$ gives us some information on $rk \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix}$ or $rk \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix}$, which means these events $rk \begin{bmatrix} \mathbf{A}_j^{(r_1)} \\ \mathbf{A}_j^{(r_2)} \\ \mathbf{A}_j^{(r_3)} \end{bmatrix} < 2t$ are dependent.

We also have 3 possibilities, when we choose the link 1 to form the matrix $\mathbf{A}_j^{(r_2)}$: $\begin{bmatrix} 2 \\ 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 4 \end{bmatrix}$

and $\begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix}$.

There are again 3 possibilities, when we choose the link 1 to form the matrix $\mathbf{A}_j^{(r_3)}$:

$\begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 3 \\ 4 \\ 1 \end{bmatrix}$.

Let's denote the event $rk \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} < 2t$ by \mathcal{E}_1 . It is clearly to see that $Pr \left[rk \begin{bmatrix} 2 \\ 1 \\ 3 \end{bmatrix} < 2t \mid \mathcal{E}_1 \right] =$

1. The bound in Lemma 5.3 is a bit loose, because we do not neglect unsuitable matrices,

e.g. $\begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix}$. In the other words, there exists at most 9 events are dependent.

>>> IS THIS EXAMPLE CONVINCING ENOUGH? WHY IS IT NOT $d(r) \leq 3 \cdot r \cdot$

$$\binom{r-1}{2} = ?$$

Theorem 5.1. *If $r \leq \Omega(q^{t^2/2+\mathcal{O}(t)})$, then there exists a vector solution for the $(\epsilon = 1, l = 1) - \mathcal{N}_{h=3, r, s=4}$ network.*

Proof. The Local lemma 5.1 shows that there is a positive probability that none of bad events occurs: $Pr \left[\bigcap_{i=1}^n \bar{\mathcal{E}}_i \right] > 0$.

By the intersection rule, none of bad events is equivalent to an event T that its set of outcomes are all desirable, i.e. these outcomes satisfy the Equation 5.1:

$$T = \bigcap_{i=1}^n \bar{\mathcal{E}}_i = rk \begin{bmatrix} \mathbf{A}_j^{(r_1)} \\ \mathbf{A}_j^{(r_2)} \\ \mathbf{A}_j^{(r_3)} \end{bmatrix} \geq 2t, \forall 1 \leq r_1 < r_2 < r_3 \leq r.$$

The probability of event T indicates a measure quantifying the likelihood that we are able to construct $rk[\mathbf{A}_j] \geq 3t$ given r links. It means that a vector solution exists if and only if the Local lemma 5.1 is satisfied such that: $4 \cdot p \cdot d(r) \leq 1, \forall r \leq r_{max, vector}$. Therefore, we must find a lower bound of $r_{max, vector}$. Furthermore, we have $d \leq \frac{3}{2}r^2$ following to Lemma 5.3, which gives: $4 \cdot p \cdot \frac{3}{2}r^2 \leq 1 \Rightarrow r \leq \sqrt{\frac{1}{6p}} = r_{max, vector}$. Thus, finding $\min[r_{max, vector}]$ is equivalent to maximize p .

By Lemma 5.2, we have $p \leq \Theta(q^{-t^2-2t-1})$,

$$\Rightarrow \min[r_{max, vector}] \in \Omega\left(\sqrt{\frac{1}{6p}}\right) = \Omega\left(\sqrt{\frac{1}{6q^{-t^2-2t-1}}}\right) = \Omega\left(q^{t^2/2+\mathcal{O}(t)}\right).$$

Hence, the Local lemma in 5.1 is satisfied, when $r \leq \Omega(q^{t^2/2+\mathcal{O}(t)})$. None of bad events occurs, so there exists a vector solution for such r . \square

Corollary 5.1. *The $(\epsilon = 1, l = 1) - \mathcal{N}_{h=3, r, s=4}$ network has a vector solution with a gap $q^{t^2/4+\mathcal{O}(t)}$.*

In [EW18, Sec. VIII-C], we have that $r_{max,scalar} \in \mathcal{O}(q_s^2)$, where they proved that

$$r_{scalar} \leq 2 \left[\begin{array}{c} 3 \\ 1 \end{array} \right]_{q_s} = 2(q_s^2 + q_s + 1). \quad (5.4)$$

Following to Section 3.4.2 and Theorem 5.1, we have the gap size

$$\begin{aligned} r_{max,scalar} &= \min[r_{max,vector}] \\ \Leftrightarrow q_s^2 &= q^{t^2/2 + \mathcal{O}(t)} \\ \Leftrightarrow q_s &= q^{t^2/4 + \mathcal{O}(t)} \\ \Rightarrow g &= q_s - q_v = q^{t^2/4 + \mathcal{O}(t)} \end{aligned} \quad (5.5)$$

By varying t in Equation (5.3), we have the following table:

Table 5.1: r over variations of t

t	Scalar Solution	Vector Solution
1	$r_{scalar} \leq 14$	$r_{vector} \geq 3$
2	$r_{scalar} \leq 42$	$r_{vector} \geq 7$ (67*, 89**)
3	$r_{scalar} \leq 146$	$r_{vector} \geq 62$ (166*)
4	$r_{scalar} \leq 546$	$r_{vector} \geq 1317$
5	$r_{scalar} \leq 2114$	$r_{vector} \geq 58472$
6	$r_{scalar} \leq 8322$	$r_{vector} > 10^6$

*, **: computational results in construction 1 and construction 2 respectively

In the table (5.1), the vector solution outperforms the scalar solution when $t \geq 4$ for the network $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h=3,r,s=4}$. This is sufficient, we show in Section 6 computational results which vector solutions outperform scalar solutions in case of $t = 2$ and $t = 3$.

5.2 $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h,r,s}$ Network

5.2.1 Find the lower bound of $r_{max,vector}$

As previous, $\mathbf{A}_j^{(r_1)}, \dots, \mathbf{A}_j^{(r_{h-\epsilon})} \in \mathbb{F}_q^{t \times ht}$ and we need to satisfy the following:

$$rk \left[\begin{array}{c} \mathbf{A}_j^{(r_1)} \\ \vdots \\ \mathbf{A}_j^{(r_{h-\epsilon})} \end{array} \right] \geq ht - t \Leftrightarrow rk[\mathbf{A}_j] \geq (h-1)t$$

We can formulate it by the following coding problem in Grassmannian:

Find the largest set of subspaces from $\mathcal{G}_q(ht, t)$ such that any α subspaces of the set span a subspace of dimension at least $(h-1)t$.

Similar with $(\epsilon = 1, \ell = 1) - N_{3,r,4}$, we consider p to proceed the Local lemma 5.1:

$$Pr[rk[\mathbf{A}_j] < (h-1)t] \leq p \quad (5.6)$$

Lemma 5.4. $p \leq \Theta\left(q^{(h-\alpha)t^2 + \mathcal{O}(t)}\right), \forall t \geq 2$.

Proof. Regarding to the left-hand side in Equation 5.6:

$$\begin{aligned} Pr[rk[\mathbf{A}_j] < (h-1)t] &= \sum_{i=0}^{(h-1)t-1} Pr[rk[\mathbf{A}] = i] \\ &\stackrel{1}{=} \sum_{i=0}^{(h-1)t-1} \frac{N_{i,\alpha t, ht}}{q^{(\alpha t)(ht)}} \\ &= \frac{1}{q^{(\alpha h)t^2}} \cdot \sum_{i=0}^{(h-1)t-1} \prod_{j=0}^{i-1} \frac{(q^{\alpha t} - q^j)(q^{ht} - q^j)}{q^i - q^j}. \end{aligned} \quad (5.7)$$

(1): The formula for the number of $[m \times n]$ matrices of rank i over \mathbb{F}_q was proved in [Ove07].

We consider firstly the product $\prod_{j=0}^{i-1} \frac{(q^{\alpha t} - q^j)(q^{ht} - q^j)}{q^i - q^j} = \frac{p_N^{(i)}(q)}{p_D^{(i)}(q)} = p^{(i)}(q)$.

For $t \rightarrow \infty$: $\left. \begin{aligned} \deg(p_N^{(i)}(q)) &= q^{i(\alpha t + ht)} \\ \deg(p_D^{(i)}(q)) &= q^{i^2} \end{aligned} \right\} \Rightarrow p^{(i)}(q) \approx q^{i(\alpha t + ht) - i^2}.$

Now, we evaluate $f(i) = i(\alpha t + ht) - i^2$ to find its maximum point by its derivation :

$$\dot{f}(i^*) = 0 \Leftrightarrow (\alpha t + ht) - 2i^* = 0 \Leftrightarrow i^* = \frac{\alpha t + ht}{2}$$

We then check whether this point within the range $i = 0, \dots, (h-1)t - 1$ as following:

$$0 \leq \frac{\alpha t + ht}{2} \leq (h-1)t - 1.$$

With regards to the lower bound: $0 \leq \frac{\alpha t + ht}{2} \Leftrightarrow t \geq \frac{2}{\alpha + h}$, which is always true due to the given $t \geq 2$ and $\alpha, h \geq 3$.

Regarding to the upper bound: $\frac{\alpha t + ht}{2} \leq (h-1)t - 1 \Leftrightarrow t \leq \frac{-2}{\alpha + 2 - h}$ with $\alpha + 2 > h$ due to the given $\alpha t + \epsilon = \alpha + 1 \geq h$. This cannot happen because of $t \geq 2$, i.e. this maximum point is over then upper-range limit.

$$\begin{aligned} \Rightarrow \max \left\{ q^{i(\alpha t + ht) - i^2} : i = 1, \dots, (h-1)t - 1 \right\} &= q^{i(\alpha t + ht) - i^2} \Big|_{i=(h-1)t-1} \\ &= q^{[(h-1)(\alpha+1)]t^2 - (\alpha-h+2)t-1}. \end{aligned}$$

Secondly, we apply the maximum value with the sum, we have:

$$\begin{aligned} \max \left[\sum_{i=0}^{(h-1)t-1} p^{(i)}(q) \right] &\in \Theta \left(q^{[(h-1)(\alpha+1)]t^2 + \mathcal{O}(t)} \right) \\ \Rightarrow \max \left[\frac{\sum_{i=0}^{(h-1)t-1} p^{(i)}(q)}{q^{(\alpha h)t^2}} \right] &\in \left(\frac{q^{[(h-1)(\alpha+1)]t^2 + \mathcal{O}(t)}}{q^{(\alpha h)t^2}} \right) \\ \Rightarrow p &\leq \Theta \left(q^{(h-\alpha)t^2 + \mathcal{O}(t)} \right) \end{aligned}$$

□

Lemma 5.5. $d \leq \frac{\alpha}{(\alpha-1)!} r^{\alpha-1}$.

Proof. Similar with ($\epsilon = 1, \ell = 1$) - $N_{3,r,4}$, we have:

$$d \leq \alpha \binom{r-1}{\alpha-1} = \alpha \frac{(r-1) \dots (r-\alpha+1)}{(\alpha-1)!} \leq \frac{\alpha}{(\alpha-1)!} r^{\alpha-1}$$

□

Theorem 5.2. If $r \leq \Omega \left(q^{\frac{h-\alpha-1}{1-\alpha}t^2 + \mathcal{O}(t)} \right)$, then there exists a vector solution for the ($\epsilon = 1, \ell = 1$) - $N_{h,r,s}$ network.

Proof. As previous, satisfying LLL 5.1 is equivalent to an existence of a vector solution.

We need $4dp \leq 1$, and following to Lemma 5.5: $d \leq \frac{\alpha}{(\alpha-1)!} r^{\alpha-1} \Rightarrow r \leq \left(\frac{(\alpha-1)!}{4\alpha} \cdot \frac{1}{p} \right)^{\frac{1}{\alpha-1}} = r_{\max, \text{vector}}$. We thus again find a lower bound of $r_{\max, \text{vector}}$.

By Lemma 5.5, we have $p \leq \Theta \left(q^{(h-\alpha)t^2 + \mathcal{O}(t)} \right)$, $\forall t \geq 2$,

$$\Rightarrow \min [r_{\max, \text{vector}}] \in \Omega \left(q^{\frac{h-\alpha-1}{1-\alpha}t^2 + \mathcal{O}(t)} \right).$$

Hence, the Local lemma 5.1 is satisfied, when $r \leq \Omega \left(q^{\frac{h-\alpha-1}{1-\alpha}t^2 + \mathcal{O}(t)} \right)$, and a vector solution exists for such r . □

5.2.2 Find the Upper Bound of $r_{\max, \text{scalar}}$

Find $(\alpha + 1)$ received vectors that span a subspace of dimension h . This implies that the α links from the middle layer carry α vectors which span a subspace of $\mathbb{F}_{q_s}^h$ whose dimension is at least $(h - 1)$, with $q_s = q^t$.

Following to Theorem (4.1), we are interested in the following range: $\ell + \epsilon + 1 \leq h \leq \alpha\ell + \epsilon$.

For $3 \leq \alpha < h$: all α links must be distinct $\Rightarrow r \leq \left[\begin{matrix} \alpha \\ 1 \end{matrix} \right]_{q_s} \Rightarrow r \leq \mathcal{O} (q_s^{\alpha-1})$

For $\alpha \geq h \geq 3$: to achieve $(h-1)$ -subspaces of $\mathbb{F}_{q_s}^h$, no α links will contain a vector which is contained in the same $(h-2)$ -subspace.

Hence,

$$r_{max,scalar} \leq (\alpha-1) \begin{bmatrix} \alpha \\ h-2 \end{bmatrix}_{q_s} \Rightarrow r_{max,scalar} \in \mathcal{O}\left(q_s^{(\alpha-h+2)(h-2)t^2}\right)$$

5.2.3 Calculate Gap

$$\begin{aligned} r_{max,scalar} &= \min[r_{max,vector}] \\ \Leftrightarrow q_s^{(\alpha-h+2)(h-2)t^2} &= q^{\frac{h-\alpha-1}{1-\alpha}t^2 + \mathcal{O}(t)} \\ \Leftrightarrow q_s &= q^{\frac{\alpha-h+1}{(\alpha-1)(\alpha-h+2)(h-2)}t^2 + \mathcal{O}(t)} \\ \Rightarrow g &= q_s - q_v = q^{\frac{\alpha-h+1}{(\alpha-1)(\alpha-h+2)(h-2)}t^2 + \mathcal{O}(t)} \square \end{aligned}$$

5.3 $(\epsilon = 1, \ell \geq 2) - \mathcal{N}_{h=2\ell, r, s=2\ell+1}$

Lemma 5.6. $p \leq \Theta\left(q^{-t^2-2t-1}\right), \forall t \geq 2$.

Proof. A bad event in this vector network coding problem has the following probability:

$$\begin{aligned} Pr \left[rk \begin{bmatrix} \mathbf{A}_j^{(r_1)} \\ \vdots \\ \mathbf{A}_j^{(r_{h-\epsilon})} \end{bmatrix} < (2\ell-1)t \right] &= \sum_{i=0}^{(2\ell-1)t-1} Pr \left[rk \begin{bmatrix} \mathbf{A}_j^{(r_1)} \\ \vdots \\ \mathbf{A}_j^{(r_{h-\epsilon})} \end{bmatrix} = i \right] \\ &\stackrel{1}{=} \sum_{i=0}^{(2\ell-1)t-1} \frac{N_{i,m,n}}{q^{m \cdot n}} \\ &\stackrel{2}{=} \frac{1}{q^{4\ell^2 t^2}} \sum_{i=0}^{(2\ell-1)t-1} \prod_{j=0}^{i-1} \frac{(q^{2\ell t} - q^j)^2}{q^i - q^j} \end{aligned}$$

(1): The formula for the number of $[m \times n]$ matrices of rank i over \mathbb{F}_q was proved in [Ove07].

(2): $s = \alpha\ell + \epsilon$ by definition in Section 4.1 $\Rightarrow \alpha = 2$, so we consider $[2\ell \times 2\ell]$ matrices.

We consider XYZ: $\prod_{j=0}^{i-1} \frac{(q^{2\ell t} - q^j)^2}{q^i - q^j} = \frac{p_N^{(i)}(q)}{p_D^{(i)}(q)} = p^{(i)}(q)$.

Due to i -times product and large t : $\left. \begin{aligned} \deg(p_N^{(i)}(q)) &= q^{i4\ell t} \\ \deg(p_D^{(i)}(q)) &= q^{i^2} \end{aligned} \right\} \Rightarrow p^{(i)}(q) \approx q^{i4\ell t - i^2}.$

Therefore, we have:
$$\sum_{i=0}^{(2\ell-1)t-1} \prod_{j=0}^{i-1} \frac{(q^{2\ell t} - q^j)^2}{q^i - q^j} = \sum_{i=0}^{(2\ell-1)t-1} p^{(i)}(q) \approx \sum_{i=0}^{(2\ell-1)t-1} q^{i4\ell t - i^2}.$$

To maximize the sum, we set derivation of it to 0 and find the corresponding root:

$$\begin{aligned} (i4\ell t - i^2)' &= 0 \\ \Leftrightarrow 4\ell t - 2i &= 0 \\ \Leftrightarrow i &= 2\ell t \end{aligned}$$

However, the upper limit of the sum is $(2\ell - 1)t - 1$, which is less than $2\ell t$ for all $t \geq 2$.

$$\Rightarrow \max \left\{ q^{i4\ell t - i^2} : i = 0, 2, \dots, (2\ell - 1)t - 1 \right\} = q^{i4\ell t - i^2} \Big|_{i=(2\ell-1)t-1} = q^{4\ell^2 t^2 - t^2 - 2t - 1}$$

Hence, by using the exact bound Θ , we have:

$$\begin{aligned} \max_i \left[\sum_{i=0}^{(2\ell-1)t-1} p^{(i)}(q) \right] &\in \Theta \left(q^{4\ell^2 t^2 - t^2 - 2t - 1} \right) \\ \Rightarrow \max_i \left[\frac{1}{q^{4\ell^2 t^2}} \sum_{i=0}^{(2\ell-1)t-1} p^{(i)}(q) \right] &\in \Theta \left(q^{-t^2 - 2t - 1} \right) \\ \Rightarrow p &\leq \Theta \left(q^{-t^2 - 2t - 1} \right) \end{aligned}$$

□

Lemma 5.7. $d \leq 2r$.

Proof. Being similar with the previous subsections, we have:

$$d \leq \alpha \binom{r-1}{\alpha-1} = 2 \frac{(r-1) \dots (r-1)}{1!} \leq 2r$$

□

Theorem 5.3. If $r \leq \Omega \left(q^{t^2 + \mathcal{O}(t)} \right)$, then there exists a vector solution for the $(\epsilon = 1, \ell \geq 2)$ – $\mathcal{N}_{h=2\ell, r, s=2\ell+1}$ network.

Proof. As previous, we need $4 \cdot p \cdot d(r) \leq 1, \forall r \leq r_{\max, \text{vector}}$ so that a vector solution exists. Following to Lemma 5.7, we have $d \leq 2r \Rightarrow 4 \cdot p \cdot 2r \leq 1 \Rightarrow r \leq \frac{1}{8p}$. We still

need to maximize p to get lower on $r_{max,vector}$, and we have $p \leq \Theta\left(q^{-t^2-2t-1}\right), \forall t \geq 2$ in Lemma 5.6. Thus, $\min[r_{max,vector}] \in \Omega\left(\frac{1}{8p}\right) = \Omega\left(q^{t^2+2t+1}\right)$.

Hence, the Local lemma in 5.1 is satisfied, when $r \leq \Omega\left(q^{t^2/2+\mathcal{O}(t)}\right)$. None of bad events occurs, so there exists a vector solution for such r . \square

Lemma 5.8. *A scalar solution for the $(\epsilon = 1, \ell \geq 2) - \mathcal{N}_{h=2\ell, r, s=2\ell+1}$ network exists, if and only if there exists a Grassmannian code $\mathcal{G}_q(h = 2\ell, \ell)$ such that any $\alpha = 2$ subspaces of the set span a subspace of dimension at least $2\ell - 1$.*

Proof. Let's denote any 2 subspaces of $\mathcal{G}_q(h = 2\ell, \ell)$ as \mathcal{U} and \mathcal{V} . If \mathcal{U} and \mathcal{V} span a subspace of dimension at least $2\ell - 1$, then we have $\dim(\mathcal{U} + \mathcal{V}) = 2\ell - 1$, with $\mathcal{U} + \mathcal{V}$. Therefore, $\dim(\mathcal{U} \cap \mathcal{V}) = \dim(\mathcal{U}) + \dim(\mathcal{V}) - \dim(\mathcal{U} + \mathcal{V}) = 1$, which leads to the subspace distance $d_s(\mathcal{U}, \mathcal{V}) = 2\dim(\mathcal{U} + \mathcal{V}) - \dim(\mathcal{U}) - \dim(\mathcal{V}) = 2\ell - 2$. No 2 ℓ -dimensional subspaces of $\mathbb{F}_{q_s}^{2\ell}$ will contain a vector which is contained in the same $(2\ell - 2)$ -subspace, but $(2\ell - 1)$ of such subspaces can have such vectors,

$$\Rightarrow r_{scalar} \leq (2\ell - 1) \left[\begin{array}{c} 2\ell \\ 2\ell - 2 \end{array} \right]_{q_s} \Rightarrow r_{scalar} \leq \mathcal{O}\left(q_s^\ell\right)$$

\square

Corollary 5.2. *The $(\epsilon = 1, \ell \geq 2) - \mathcal{N}_{h=2\ell, r, s=2\ell+1}$ network has a vector solution with a gap $q^{t^2/4+\mathcal{O}(t)}$.*

Following to Section 3.4.2 and Theorem 5.3, we have the gap size

$$\begin{aligned} r_{max,scalar} &= \min[r_{max,vector}] \\ \Leftrightarrow q_s^\ell &= q^{t^2/2+\mathcal{O}(t)} \\ \Leftrightarrow q_s &= q^{t^2/2\ell+\mathcal{O}(t)} \\ \Rightarrow g &= q_s - q_v = q^{t^2/2\ell+\mathcal{O}(t)} \end{aligned} \tag{5.8}$$

This shows us that there exists a better vector solution by comparison with the gap in [EW18, Fig. 4].

6 Computational Results

In Table 5.1, our vector solutions are computed by Algorithm 1 for the $(\epsilon = 1, \ell = 1) - N_{3,r,4}$ network regarding to $t = 2$ and $t = 3$, with $q_v = q^t$ as previous sections. Both construction 1 and 2 provide better results than scalar solutions.

Construction 1: $\mathbf{I}_t \mid \mathbf{T}$, with $\mathbf{T} \in \mathbb{F}_q^{t \times t(h-1)}$

Construction 2: $\mathbf{T} \in \text{MatrixSpaceUrs}(t, 3t)$

6.1 Main Approach

Regarding to $t = 2$, for a scalar network coding solution we need a $3 - (3, 1, 1)_4^c$ code ($q_v = 2^2 = 4$) by Theorem 4.3. The largest such code consists of the 21 one-dimensional subspaces of \mathbb{F}_4^3 , each one is contained twice in the code. Therefore, the number of nodes can be at most 42 for a scalar linear coding solution, while for vector network coding 89 nodes can be used, i.e. $\mathcal{A}_{q=2}(n = 6, k = 4, t = 3; \lambda = 2) \geq 89$ following to Corollary 4.1. This is a new lower bound for $\mathcal{A}_2(6, 4, 3; 2)$ compared to a code with 51 codewords presented in [EW18]. The smallest alphabet size for a scalar solution with 89 nodes exists is $q_s = 8$. By Equation 5.4, there are 73 one-dimensional subspaces of \mathbb{F}_8^3 , and each one can be used twice in the code; therefore, we have in total 146 possible codesword, but only 89 codewords are required. In this case, the gap size $g = q_s - q_v = 2^3 - 2^2 = 8 - 4 = 2^2$, i.e. we achieve a gap size $q^{t^2/2}$, which is better the asymptotic behavior in 5.5.

Before introducing the algorithm used to generate such 89 codewords, we have to state some definitions for a better explanation. We denote a matrix space of dimension $[n \times m]$ by $M(n, m) = \left\{ \mathbf{A} : \mathbf{A} \in \mathbb{F}_{q=2}^{n \times m} \right\}$.

Definition 6.1 (Matrix Space with Unique Row Space). $U(n, m)$ is a subset of $M(n, m)$, where any $\mathbf{A}, \mathbf{B} \in U(n, m)$ have their row spaces such that:

$$\mathcal{R}_q(\mathbf{A}) \neq \mathcal{R}_q(\mathbf{B}),$$

where $\mathcal{R}_q(.)$ denotes the row space of a matrix.

Definition 6.2 (Sufficient Global Coding Vector). Let $\mathbf{A}, \mathbf{B}, \mathbf{C} \in U(t, 3t)$ and $N \lll$

$\binom{2^{3t^2}}{3}$, then a set $\mathcal{H}_{n=3t, m=3t} = \{\mathbf{H}_1, \dots, \mathbf{H}_N\}$ contains distinct *sufficient global coding vectors* \mathbf{H}_j such that:

$$rk[\mathbf{H}_j] = rk \begin{bmatrix} \mathbf{A} \\ \mathbf{B} \\ \mathbf{C} \end{bmatrix} \geq 2n, \forall j \in \{1, \dots, N\}.$$

For ease of notations, we denote $\begin{bmatrix} \mathbf{A} \\ \mathbf{B} \\ \mathbf{C} \end{bmatrix}$ by $\{\mathbf{A}, \mathbf{B}, \mathbf{C}\}$ for the rest of this thesis.

Definition 6.3 (Relative). Let $\mathbf{A}, \mathbf{B}, \mathbf{C} \in U(t, 3t)$. Then \mathbf{C} is called a *relative* of a tuple (\mathbf{A}, \mathbf{B}) if $\{\mathbf{A}, \mathbf{B}, \mathbf{C}\} \in \mathcal{H}_{n=3t, m=3t}$ and denoted as following:

$$rel[(\mathbf{A}, \mathbf{B})] = \mathbf{C}.$$

Lemma 6.1. *There are maximum $3 \cdot \binom{2^{3t^2}}{3}$ relatives for a set $\mathcal{H}_{n=3t, m=3t} = \{\mathbf{H}_1, \dots, \mathbf{H}_N\}$.*

Proof. Each sufficient global coding vector \mathbf{H}_j contains a $\{\mathbf{A}, \mathbf{B}, \mathbf{C}\}$. Thus, each of these 3 matrices can form 3 different relatives:

$$\begin{aligned} rel[(\mathbf{A}, \mathbf{B})] &= \mathbf{C} \\ rel[(\mathbf{A}, \mathbf{C})] &= \mathbf{B} . \\ rel[(\mathbf{B}, \mathbf{C})] &= \mathbf{A} \end{aligned}$$

Furthermore, the maximum size of $\mathcal{H}_{n=3t, m=3t}$ is q^{3t^2} . Therefore, $\mathcal{H}_{t=3}$ can have only maximum $3q^{3t^2}$ relatives. \square

Definition 6.4 (Sub-relative). Let $\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D} \in U(t, 3t)$. Then \mathbf{D} is called a *sub-relative* of a tuple $(\mathbf{A}, \mathbf{B}, \mathbf{C}) \in \mathcal{H}_{n=3t, m=3t}$ if:

$$\begin{cases} \{\mathbf{A}, \mathbf{B}, \mathbf{D}\} \in \mathcal{H}_{t=3} \\ \{\mathbf{A}, \mathbf{C}, \mathbf{D}\} \in \mathcal{H}_{t=3} \\ \{\mathbf{B}, \mathbf{C}, \mathbf{D}\} \in \mathcal{H}_{t=3} \end{cases} .$$

A sub-relative is denoted by:

$$subrel[(\mathbf{A}, \mathbf{B}, \mathbf{C})] = \mathbf{D}$$

This definition about Sub-relative is similarly again used for a set of 5 or more matrices.

Algorithm 1 Increasing Method

Input: $\mathcal{H}_{n=3t,m=3t}$ with its size $|\mathcal{H}_{n=3t,m=3t}| = N \lll \binom{2^{3t^2}}{3}$.

Output: A $3 - (3t, t, t)_{q=2}^c$ code or its orthogonal complement, a $3 - (3t, 2t, t)_{q=2}^m$ with its code size is maximum under $\mathcal{H}_{n=3t,m=3t}$.

- 1: **for all** $(\mathbf{A}, \mathbf{B}, \mathbf{C}) \in \mathcal{H}_{n=3t,m=3t}$ **do**
- 2: $R \leftarrow$ Generate all relatives; (*)
- 3: **end for**
- 4: $P_{max} \leftarrow \{\}$ // an empty set
- 5: **for all** $(\mathbf{X}, \mathbf{Y}) \in R$ **do**
- 6: **if** $|rel[(\mathbf{X}, \mathbf{Y})]|$ is maximum **then**
- 7: $P_{max} \leftarrow P_{max} \oplus (\mathbf{X}, \mathbf{Y})$ (**)
- 8: **end if**
- 9: **end for**
- 10: $P_{potential} \leftarrow \{\}$ // an empty set
- 11: **for all** $(\mathbf{E}, \mathbf{Q}) \in P_{max}$ **do**
- 12: **if** $|(\mathbf{E}, \mathbf{Q}) \cup rel[(\mathbf{E}, \mathbf{Q})]| \notin P_{potential}$ **then**
- 13: $P_{potential} \leftarrow P_{potential} \oplus (\mathbf{E}, \mathbf{Q})$
- 14: **end if**
- 15: **end for**
- 16: $P \leftarrow \{\}$ // an empty set
- 17: **for all** $(\mathbf{K}, \mathbf{L}) \in P_{potential}$ **do**
- 18: **for all** $\mathbf{Z} \in rel[(\mathbf{X}, \mathbf{Y})]$ **do**
- 19: **if** $subrel[(\mathbf{K}, \mathbf{L}, \mathbf{Z})]$ is maximum **then**
- 20: $P \leftarrow P_{potential} \oplus (\mathbf{K}, \mathbf{L}, \mathbf{Z})$ (***)
- 21: **end if**
- 22: **end for**
- 23: **end for**
- 24: **while** $\exists subrel$ in P is not empty (****) **do**
- 25: Line 10 to Line 23, but elements of P_{max} is replaced by P and the size of subrel or tuples are thus increased over each while loop.
- 26: **end while**

(*): If any 2-tuple exists already in R , its new relative is appended to its existing relatives to form a set of relatives.

(**): P_{max} is set to an empty set anytime we find a new maximum, before the concate-

nation \oplus .

(**): P is set to an empty set anytime we find a new maximum, before the concatenation \oplus . P removes duplicated values itself under the while-loop of Line 11 to Line 15.

(****): This means the maximum size of subrel in P is not 0.

Now, we prove that Algorithm 1 always give us our expected output. Then we compute its complexity based on number of necessary computation.

Proof. Our problem can be described like finding all matrices such that any 3 of them can accompany together. The companion is possible, when the 3 matrices satisfy the rank requirement in 5.1. The input $\mathcal{H}_{n=3t, m=3t}$ of Algorithm 1 lists all such 3 matrices by tuples of 3 matrices (called 3-tuples). Line 1 to Line 3 gives us all pairs or 2-tuples from these 3-tuples as well as their relatives. Then the algorithm starts searching for its output initially based on 2 matrices having the largest number of relatives, i.e. it appears mostly in $\mathcal{H}_{n=3t, m=3t}$ in comparison with any other pairs of matrices. This number of relatives plus 2 by themselves is actually the upper bound for a code size, when a $3 - (3t, t, t)_{q=2}^c$ code is considered [EZ19, Sec. V-D]. Furthermore, from Line 10 to Line 26, the algorithm extends the initial 2-tuples based on all of these relatives. That's why the algorithm's output gives us all of our expected matrices. \square

Our algorithm is based on $C_{relatives} \lll 3 \binom{2^{3t^2}}{3} \Rightarrow C_{relatives} \lll \mathcal{O}\left(\frac{t^6}{6}\right)$. In case $t = 2$, $U(t, 3t)$ helps us reduce $|M(t, 3t)| = 4096$ matrices to $|U(t, 3t)| = 715$ matrices, $C_{relatives} \approx 3 \binom{\frac{715}{4096} 2^{3t^2}}{3} \approx \mathcal{O}\left(\frac{2}{3000} t^6\right)$. Therefore, we are able to achieve the output of Algorithm 1 for $\mathcal{H}_{n=6, m=6}$ in a short amount of time.

We are going to list some toy examples for the algorithm as well as illustrate it in Figure 6.1.

Example 6.1. Let $n = 1, m = 2, q = 2$, which violates the input $\mathcal{H}_{n=3t, m=3t}$ but still being a good example for the rest steps in Algorithm 1. Then we have $N = 4$ matrices (vectors):

$$\begin{aligned} \mathbf{A} &= [0, 0] \\ \mathbf{B} &= [0, 1] \\ \mathbf{C} &= [1, 0] \\ \mathbf{D} &= [1, 1] \end{aligned}$$

Step 1 (Line 1 to Line 3): Due to, any 3 of them form a sufficient global coding vector,

i.e. a matrix with $rk \geq 2n$, we have the relative as following:

$$\begin{aligned} rel[(A, B)] &= [C, D] \\ rel[(A, C)] &= [B, D] \\ rel[(A, D)] &= [B, C] \\ rel[(B, C)] &= [A, D] \\ rel[(B, D)] &= [A, C] \\ rel[(C, D)] &= [A, B] \end{aligned}$$

Step 2 (Line 4 to Line 9): We get the maximum size of these steps is 2 and P_{max} results in all $\{A, B\}, \{A, C\}, \{A, D\}, \{B, C\}, \{B, D\}, \{C, D\}$, because $\max_{\forall X, Y \in M(1, 2)} (rel[(X, Y)]) = 2$.

Step 3 (Line 10 to Line 14): Due to $\{E, Q\} \cup rel[(E, Q)] = \{A, B, C, D\}$ with (E, Q) are tuples from P_{max} found in Step 2. We keep only $P_{potential} = \{(A, B) : rel[(A, B)]\}$

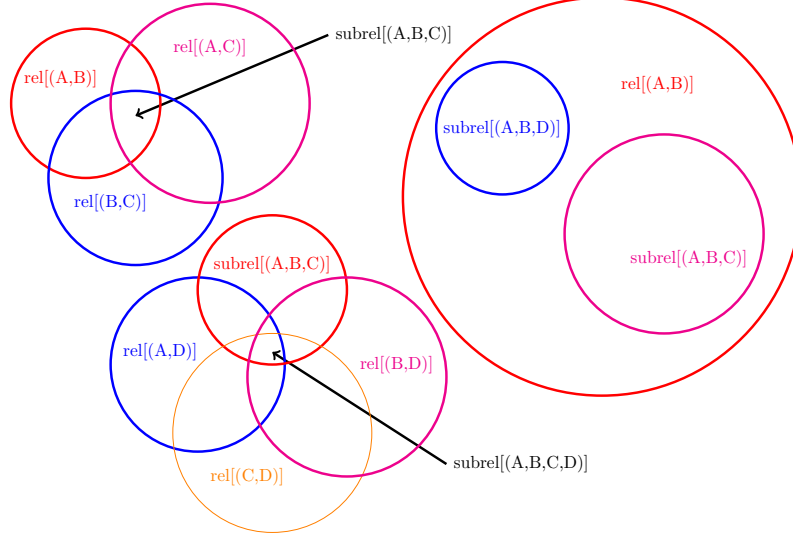
Step 4 (Line 16 to 23): Regarding to $rel[(K, L)] = rel[(A, B)]$, we have $Z \in \{C, D\}$. Then, $|subrel[(A, B, C)]| = |subrel[(A, B, D)]| = 1$, so we get $P = \{(A, B, C), ((A, B, D))\}$.

Step 5: The maximum size of subrel in P is larger than 0, so we proceed the while loop. Step 3 will be looped firstly, and we get $P_{potential} = \{(A, B, C) : rel[(A, B, C)]\}$.

Step 6: As step 4, we get a result $\{A, B, C, D\}$.

Example 6.2. For further understading, we use Figure 6.1 for illustration. In the right, we observe that the size of relative becomes smaller when its tuple identity is larger, i.e. $|rel[(A, B)]| \geq |subrel[(A, B, C)]|$ or $|rel[(A, B)]| \geq |subrel[(A, B, D)]|$. It explains why the maximum numbers of matrices that we can find for a vector solution of this network is the output of Algorithm 1. Regarding to the left, the visual explanation of *subrel* is shown.

Figure 6.1: The vector network coding of $(\epsilon = 1, l = 1) - \mathcal{N}_{h=3,r,s=4}$ represents as a matrix problem



6.2 Alternative Approaches

Firstly, instead of using *matrix space with unique row space*, we use the whole matrix space $M(n, m)$. In case $t = 2$, we cover all $2^{3t^2} = 4096$ matrices instead of only 715 matrices in Section 6.1, which will help the Algorithm 1 cover the optimal vector solution.

Definition 6.5 (Good Global Coding Vector). Let $\mathbf{A}, \mathbf{B}, \mathbf{C} \in U(t, 3t)$ and $N \leq \binom{2^{3t^2}}{3}$, then a set $\mathcal{T}_{n=3t,m=3t} = \{\mathbf{T}_1, \dots, \mathbf{T}_N\}$ contains distinct *sufficient global coding vectors* \mathbf{T}_j such that:

$$rk[\mathbf{T}_j] = rk \begin{bmatrix} \mathbf{A} \\ \mathbf{B} \\ \mathbf{C} \end{bmatrix} \geq 2n, \forall j \in \{1, \dots, N\}.$$

In Algorithm 1, we substitute the input by $\mathcal{T}_{n=3t,m=3t}$ instead of $\mathcal{H}_{n=3t,m=3t}$. This will give us an output with upper bound of $\mathcal{A}_2(3t, 2t, 3; 2t) = 126$ [EZ19, Sec. V-B].

Secondly, we tried another approach called “Randomly Increasing Method”. We got about 72 codewords instead of 89 codewords as Algorithm 1, due to a limited number of tries.

Finally, we tried removing bad matrices from a set of all 4096 matrices, until any 3 of the matrices left in the set satisfy the Equation 5.1. A matrix with the less number of existence in $\mathcal{T}_{n=3t,m=3t}$ or $\mathcal{H}_{n=3t,m=3t}$ is evaluated as a bad matrix, and it is removed for

each step. If many bad matrices exist, we only remove the first one. In case $t = 2$, we unfortunately got about 69 codewords instead of 89 codewords as Algorithm 1.

7 Conclusion

8 Appendix

Bibliography

- [ACLY00] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, “Network information flow,” *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, jul 2000.
- [DFZ05] R. Dougherty, C. Freiling, and K. Zeger, “Insufficiency of linear coding in network information flow,” *IEEE Transactions on Information Theory*, vol. 51, no. 8, pp. 2745–2759, aug 2005.
- [DR16] N. Das and B. K. Rai, “On the message dimensions of vector linearly solvable networks,” *IEEE Communications Letters*, vol. 20, no. 9, pp. 1701–1704, 2016.
- [EF11] J. Ebrahimi and C. Fragouli, “Algebraic algorithms for vector network coding,” *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 996–1007, Feb 2011.
- [EKOÖ18] T. Etzion, S. Kurz, K. Otal, and F. Özbudak, “Subspace packings,” *CoRR*, vol. abs/1811.04611, 2018. [Online]. Available: <http://arxiv.org/abs/1811.04611>
- [EW16] T. Etzion and A. Wachter-Zeh, “Vector network coding based on subspace codes outperforms scalar linear network coding,” *CoRR*, vol. abs/1604.03292, 2016. [Online]. Available: <http://arxiv.org/abs/1604.03292>
- [EW18] 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, April 2018.
- [EZ19] T. Etzion and H. Zhang, “Grassmannian codes with new distance measures for network coding,” *IEEE Transactions on Information Theory*, vol. 65, no. 7, pp. 4131–4142, July 2019.
- [FOG08] A. Fujimura, S. Y. Oh, and M. Gerla, “Network coding vs. erasure coding: Reliable multicast in ad hoc networks,” in *MILCOM 2008 - 2008 IEEE Military Communications Conference*. IEEE, nov 2008.

- [FS06] C. Fragouli and E. Soljanin, “Network coding fundamentals,” *Foundations and Trends® in Networking*, vol. 2, no. 1, pp. 1–133, 2006.
- [GLS18] M. Gone, M. Langberg, and A. Sprintson, “Latency and alphabet size in the context of multicast network coding,” in *2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, oct 2018.
- [Gol49] M. J. Golay, “Notes on digital coding,” *Proc. IEEE*, vol. 37, p. 657, 1949.
- [Ham50] R. W. Hamming, “Error detecting and error correcting codes,” *The Bell system technical journal*, vol. 29, no. 2, pp. 147–160, 1950.
- [Har08] L. Harte, *Introduction to Data Multicasting, IP Multicast Streaming for Audio and Video Media Distribution*. Althos, 2008.
- [HKM⁺03] T. Ho, R. Koetter, M. Medard, D. Karger, and M. Effros, “The benefits of coding over routing in a randomized setting,” in *IEEE International Symposium on Information Theory, 2003. Proceedings*. IEEE, 2003.
- [HL08] T. Ho and D. Lun, *Network Coding*. Cambridge University Press, 2008.
- [HT13] A.-L. Horlemann-Trautmann, “Constructions, decoding and automorphisms of subspace codes,” Ph.D. dissertation, Universität Zürich, 01 2013.
- [JSC⁺05] S. Jaggi, P. Sanders, P. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, “Polynomial time algorithms for multicast network code construction,” *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 1973–1982, jun 2005.
- [KM03] R. Koetter and M. Medard, “An algebraic approach to network coding,” *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782–795, oct 2003.
- [KRH⁺08] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, “XORs in the air: Practical wireless network coding,” *IEEE/ACM Transactions on Networking*, vol. 16, no. 3, pp. 497–510, jun 2008.
- [LL04a] A. R. Lehman and E. Lehman, “Complexity classification of network information flow problems,” in *Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, ser. SODA ’04. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 2004, pp. 142–150. [Online]. Available: <http://dl.acm.org/citation.cfm?id=982792.982814>

-
- [LL04b] Z. Li and B. Li, “Network coding in undirected networks.” CISS, 2004.
 - [LS09] M. Langberg and A. Sprintson, “Recent results on the algorithmic complexity of network coding,” in *Proc. of the 5th Workshop on Network Coding, Theory, and Applications*, 2009.
 - [LYC03] S.-Y. Li, R. Yeung, and N. Cai, “Linear network coding,” *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, feb 2003.
 - [MEKH03] M. Médard, M. Effros, D. Karger, and T. Ho, “On coding for non-multicast networks,” in *Proceedings of the Annual Allerton Conference on Communication Control and Computing*, vol. 41, no. 1. The University; 1998, 2003, pp. 21–29.
 - [MLL12] S. Maheshwar, Z. Li, and B. Li, “Bounding the coding advantage of combination network coding in undirected networks,” *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 570–584, feb 2012.
 - [NY] C. K. Ngai and R. Yeung, “Network coding gain of combination networks,” in *Manufacturing Engineer*. IEEE.
 - [Ove07] R. Overbeck, “Public key cryptography based on coding theory,” Ph.D. dissertation, Technische Universität, Darmstadt, June 2007. [Online]. Available: <http://tuprints.ulb.tu-darmstadt.de/823/>
 - [RA06] S. Riis and R. Ahlswede, “Problems in network coding and error correcting codes appended by a draft version of s. riis “utilising public information in network coding,”” in *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2006, pp. 861–897.
 - [Sch] M. Schwartz, “Personal Correspondence, 2018,” none.
 - [SCV13] M. Schwarz, T. S. Cubitt, and F. Verstraete, “An Information-Theoretic Proof of the Constructive Commutative Quantum Lovász Local Lemma,” *arXiv e-prints*, p. arXiv:1311.6474, Nov 2013.
 - [SET03] P. Sanders, S. Egner, and L. Tolhuizen, “Polynomial time algorithms for network information flow,” in *Proceedings of the fifteenth annual ACM symposium on Parallel algorithms and architectures - SPAA '03*. ACM Press, 2003.
 - [XMA07] M. Xiao, M. Medard, and T. Aulin, “A binary coding approach for combination networks and general erasure networks,” in *2007 IEEE International Symposium on Information Theory*. IEEE, jun 2007.

- [YLCZ06] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, *Network Coding Theory*. Now Publishers Inc, 2006.
- [ZNK12] X. Zhang, G. Neglia, and J. Kurose, “Network coding in disruption tolerant networks,” in *Network Coding*. Elsevier, 2012, pp. 267–308.