Technische Universität München
Coding for Communications and Data Storage
Prof. Dr.-Ing. Antonia Wachter-Zeh

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

List of Figures

List of Tables

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 specic 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 $\boldsymbol{v}$ are denoted by underlined letters. Unless stated otherwise, vectors are indexed starting from 1, i.e. $\boldsymbol{v} = [v_1, \ldots, v_n]$. Vectors are usually considered to be row vectors. Matrices $\boldsymbol{V}$ 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* $\boldsymbol{G}$ has k rows, which form a *basis* of $\mathcal{C}$, i.e., $\boldsymbol{G}$'s row space is a set of k linearly independent vectors generating $\mathcal{C}$. The codeword $\underline{c} \in \mathcal{C}$ is encoded by the *information vector* (or *message*) $\boldsymbol{m}$, with $\boldsymbol{c} = \boldsymbol{m} \cdot \boldsymbol{G}$. For any $\boldsymbol{c} \in \mathcal{C}$: $\boldsymbol{c} \cdot \boldsymbol{H}^T = \boldsymbol{0}$, with $\boldsymbol{H}$ 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 $d = \underset{\boldsymbol{c} \in \mathcal{C} \setminus \{\boldsymbol{0}\}}{min} d(\boldsymbol{c}, \boldsymbol{0})$ with respect to a metric $d(\cdot, \cdot) : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{R}_{\geq 0}$ on $\mathbb{F}^n$ [1].

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

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

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

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 asymtotic behaviour of some formulas depending on the alphabet size q and the vector length t, by using the Bachmann-Landau notation, i.e. $\mathcal{O}\left(f\left(q,t\right)\right)$ for upper, $\Theta\left(f\left(q,t\right)\right)$ for tight, and $\Omega\left(f\left(q,t\right)\right)$ 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 $\mathcal{G}_q\left(n,k\right)$. 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 $\mathcal{P}_q\left(n\right)$, i.e. a union of all dimension $k = 0, \ldots n$ subspaces in $\mathbb{F}_q^n$ or $\mathcal{P}_q\left(n\right) = \bigcup_{k=0}^{n} \mathcal{G}_q\left(n,k\right)$. [EW18]

Definition 2.3 (Covering Grassmannian code)**.** An $\alpha - \left(n,k,\delta\right)_q^c$ covering Grassmannian code (code in short) $\mathcal{C}$ is a subset of $\mathcal{G}_q\left(n,k\right)$ 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 $\mathcal{G}_q\left(n,k\right)$ is the Gaussian coefficient (also known as q-binomial), which counts the number of subspaces of dimension k in a vector space $\mathbb{F}_q^n$,

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

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

Definition 2.4 (Subspace packing [EKOÖ18]). A subspace packing $t-(n,k,\lambda)_q^m$ 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*

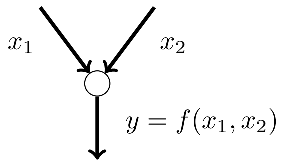
$$\mathcal{A}_q(n,k,t;\lambda) \leq \left\lfloor \frac{q^n-1}{q^k-1} \mathcal{A}_q(n-1,k-1,t-1;\lambda) \right\rfloor$$

3 Network Coding

3.1 What is Network Coding?

Our considered communication network is a directed graph[1] allowing multiple links, i.e. edges, 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 $\mathbb{F}_{q_s}$ (in scalar network coding), or a vector of length t over $\mathbb{F}_q$ (in vector network coding). Note that the assumption of unit capacity does not restrict our considered networks, since links of larger capacity can be represented by multiple parallel links of unit capacity. A request of h data units, i.e. h packets or h messages, is therefore represented by a h-dimensional row vector $\boldsymbol{x} \in \mathbb{F}_{q_s}^h$ (in scalar network coding), or $\boldsymbol{x} \in \mathbb{F}_q^{th}$ (in vector network coding). In Figure 3.1, a node of a network is repsented with its *incoming links* and *outgoing links*. A node without any incoming link is a *source* 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 networks[2].

Figure 3.1: Incoming links and outgoing links of a node



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

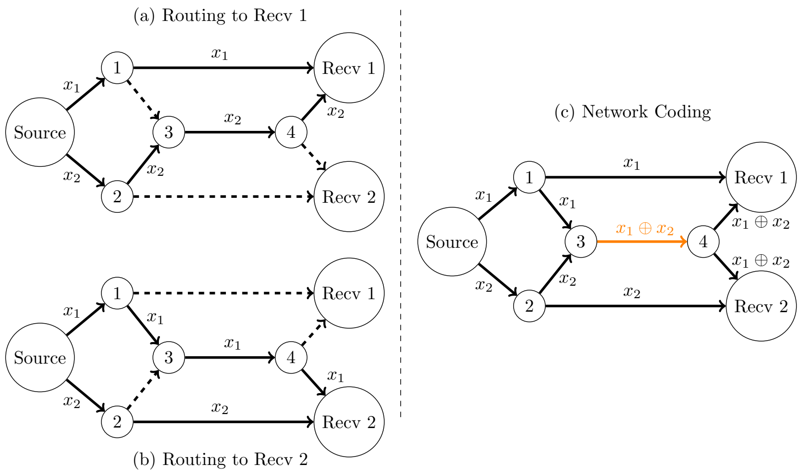
[1] Network coding over undirected networks was introduced in [LL04b].
[2] Wireless network coding was introduced in [KRH$^+$08].

of their received packets. 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, if each receiver can recover its requested packets from the received packets on its incoming links. In other words, 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 information. If these functions are linear, we obtain a *linear network coding solution*, and we do not consider *nonlinear solution* thoughout this thesis. Each function on a link consists of coding coefficients for each incoming packet. The coding coefficients form a coefficient vector of length as its number of 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*. In [KM03], Kötter and Médard provided 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.

Figure 3.2: The butterfly network



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 2 can recover x_1 and x_2 by a bitwise XOR in Figure 3.2(c). Without network coding, an additional transmission between vertex 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. 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. $101 \circledast 10 \circledast 1$. The only difference is that packets are only encoded by the source in EC [FOG08]. This problem is dealed by acknowledgement messages in the mechanism of transmission control protocol (TCP).
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 hence is 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 marices. In [MEKH03], an example of a network which does not have a scalar solution, but is solvable by vector routing was shown. 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 $\mathbb{F}_{q_{\mathrm{s}}}$ 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]. This thesis focus on determining the sovability of networks to measure the gap, and our considered networks 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 or coding coefficients such that all receiver can recover its requested information, so the function is not arbitrary or random as mentioned in [HKM+03, ACLY00]. The network structure is also known, i.e. our considered network is coherent. We later distinguish scalar and vector network coding more specifically in Section 3.3,Section 4.2.1, and Section 4.2.2.

3.3 Network as a matrix channel

To formulate this description, the source has a set of disjoint messages referred to packets which are either symbols from $\mathbb{F}_{q_s}$ (scalar coding) or vectors of length t over $\mathbb{F}_q$ (vector coding). Each link in the network carries functions of the packets, and a *network code* is a set of these functions. The network code is called *linear* if all the functions are linear and nonlinear otherwise. Each receiver $R_j, j \in \{1, \dots, N\}$ requests a subset of the source's length-h messages, and this subset is called a *packet*. 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 packets. The coefficients of a linear combination are called *global coding vectors* [SET03]. The linear equation system that any receiver R_j has to solve is as following:

$$\begin{array}{c|c} Scalar & Vector \\ \underbrace{\begin{bmatrix} y_{j_1} \\ \vdots \\ y_{j_s} \end{bmatrix}}_{\mathbb{F}_{q_s}^{s}} = \underbrace{\boldsymbol{A}_j}_{\mathbb{F}_{q_s}^{s\times h}} \cdot \underbrace{\begin{bmatrix} x_1 \\ \vdots \\ x_h \end{bmatrix}}_{\mathbb{F}_{q_s}^{h}} & \underbrace{\begin{bmatrix} \boldsymbol{y}_{j_1} \\ \vdots \\ \boldsymbol{y}_{j_s} \end{bmatrix}}_{\mathbb{F}_{q}^{st}} = \underbrace{\boldsymbol{A}_j}_{\mathbb{F}_{q}^{st\times th}} \cdot \underbrace{\begin{bmatrix} \boldsymbol{x}_1 \\ \vdots \\ \boldsymbol{x}_h \end{bmatrix}}_{\mathbb{F}_{q}^{th}} \end{array} \tag{3.1}$$

The transfer matrix $\boldsymbol{A}_j$ 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:

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

In general, the network is represented as a matrix channel for both scalar and vector coding:

Definition 3.1. Network As Matrix Channel
The channel output can be written as: $\boldsymbol{Y}_j = \boldsymbol{A}_j \cdot \boldsymbol{X}$

Because we reconstruct $\boldsymbol{X}$ with knowing $\boldsymbol{A}_j$, i.e. the network structure is known, our network is coherent. A network is *sovable* 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 $x_1, \ldots, x_h$, or vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_h$. Therefore, we want to find global coding vectors such that the matrix $\boldsymbol{A}_j$ has full-rank for every $j = 1, \ldots, N$, and such that q_s or q^t is minimized. 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	$x_1, \ldots, x_h \in \mathbb{F}_{q_\mathrm{s}}$ $\boldsymbol{x} \in \mathbb{F}_{q_\mathrm{s}}^h$	$\boldsymbol{x}_1, \ldots, \boldsymbol{x}_h \in \mathbb{F}_q^t$ $\boldsymbol{x} \in \mathbb{F}_q^{th}$
Global Coding Vectors Of Receiver R_j	$\boldsymbol{a}_{j_1}, \ldots, \boldsymbol{a}_{j_s} \in \mathbb{F}_{q_\mathrm{s}}^h$	$\boldsymbol{A}_{j_1}, \ldots, \boldsymbol{A}_{j_s} \in \mathbb{F}_q^{t \times th}$
Transfer Matrix Of Receiver R_j	$\boldsymbol{A}_j \in \mathbb{F}_{q_\mathrm{s}}^{s \times h}$	$\boldsymbol{A}_j \in \mathbb{F}_q^{st \times th}$
Packets On Receiver R_j	$y_{j_1}, \ldots, y_{j_s} \in \mathbb{F}_{q_\mathrm{s}}$ $\boldsymbol{y} \in \mathbb{F}_{q_\mathrm{s}}^s$	$\boldsymbol{y}_{j_1}, \ldots, \boldsymbol{y}_{j_s} \in \mathbb{F}_q^t$ $\boldsymbol{Y}_j \in \mathbb{F}_q^{st}$
Number of nodes	r_{scalar}	r_{vector}

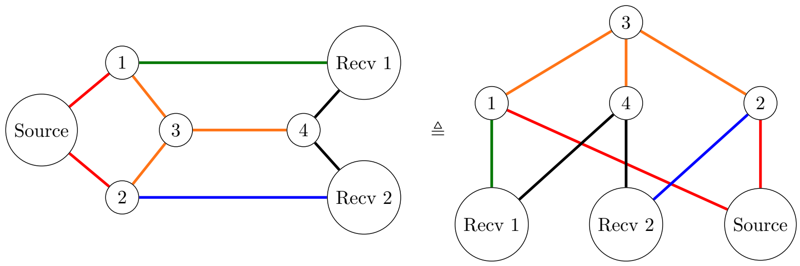
Remark 3.1. By using the vector coding, the upper bound number of solutions increases from q^{tkh} to q^{t^2kh}. Therefore, vector network coding offers more freedom in choosing the coding coefficients than does scalar linear coding for equivalent alphabet sizes, and a smaller alphabet size might be 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

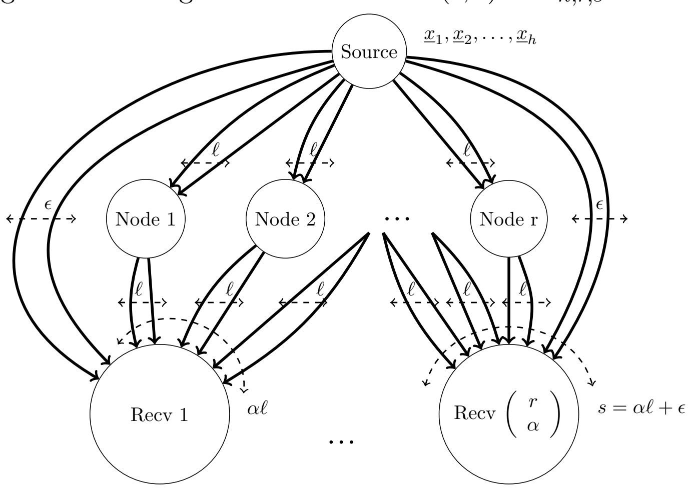
The *gap* represents the difference between the smallest field (alphabet) size for which a scalar linear solution exists and the smallest alphatbet size for which we can construct a vector solution. In this study, we define a solvable vector network coding over the field size $\mathbb{F}_q^t$, and we find the minimum amount of maximum 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: $r_{scalar} \leq f_2\left(q_{\mathrm{s}}\right)$, 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 $r_{max,scalar} = f_2\left(q_{\mathrm{s}}\right) = f_1(q,t) = r_{max,vector}$. Finally, we calculate the gap by $g = q_{\mathrm{s}} - q_v = q_{\mathrm{s}} - q^t$. 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 "Intermedate Nodes" by "Nodes" from this section. The network has a source with h messages, r nodes, and $\begin{pmatrix} r \\ \alpha \end{pmatrix}$ 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 edges. Each receiver is connected by s links in total, specifically αl 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, $h \leq s \Leftrightarrow h \leq \alpha\ell + \epsilon$ □
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. □

Table 4.1: Parameters of network coding

h	The number of source messages
r	The number of nodes in the middle layer
$\binom{r}{\alpha}$	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

4.2.1 Scalar network coding

A message is equivalent to a symbol over $\mathbb{F}_{q_s}$. As a network of the multicast model, all receivers request the same packet of h symbols at the same time [HT13]. A packet is a 1-dimentional 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* $(\epsilon,\ell)-\mathcal{N}_{h,r,s=\alpha l+\epsilon}$*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

The messages are vectors of length t over $\mathbb{F}_q$, i.e. a vector solution is 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 a 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 $(h-\epsilon)\,t$.

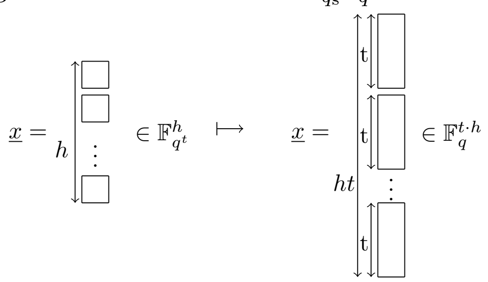
Theorem 4.4 ([EZ19]). *A vector solution for the* $(\epsilon,\ell)-\mathcal{N}_{h,r,s}$ *network exists if and only if there exists* $\mathcal{G}_q\,(ht,\ell t)$ *such that any* α *subspaces of the set span a subspace of dimension at least* $(h-\epsilon)\,t$.

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 $\mathbb{F}_{q_s=q^t}$ to the equivalent vector solution



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 $x_1, \ldots, x_{h=3} \in \mathbb{F}_{2^2}$, and for vector coding the messages are $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{h=3} \in \mathbb{F}_2^2$. From the polynomial column, let's choose arbitrarily a scalar vector $\boldsymbol{x}_{scalar} = (x_1, x_2, x_3) = (1, \alpha, \alpha+1)$. Then, we map it to $\boldsymbol{x}_{vector} = (\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3)$ 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: $a_0 \cdot \alpha^0 + a_1 \cdot \alpha^1 + \ldots + a_{t-1} \cdot \alpha^{t-1} \mapsto \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix}$.

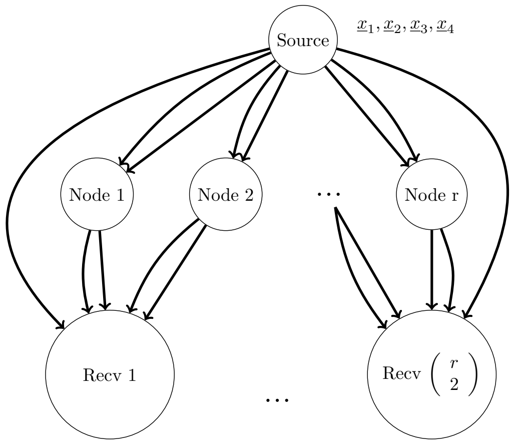
4.3 Special Cases of Generalized Combination Network

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

This family contains the largest number of direct links from the source to the receivers. For $\ell \geq 2$, this network $(\epsilon = \ell-1, \ell) - \mathcal{N}_{h=2\ell,r,s=3\ell-1}$ yields the gap $q^{(\ell-1)t^2/\ell + \mathcal{O}(t)}$ between vector solutions and optimal scalar solutions. The vector solution is based on an $\mathcal{MRD}\left[\ell t \times \ell t, t\right]_q$ code. Further, the gap tends to $q^{t^2/2+\mathcal{O}(t)}$ for large ℓ.

Lemma 4.1 ([EW18])**.** *There is a scalar linear solution of field size q_{s} for the $(\epsilon = \ell-1, \ell)-\mathcal{N}_{h=2\ell r,s=3\ell-1}$ network, where $\ell \geq 2$, if and only if $r \leq \begin{bmatrix} 2\ell \\ \ell \end{bmatrix}_{q_{\mathrm{s}}}$.*

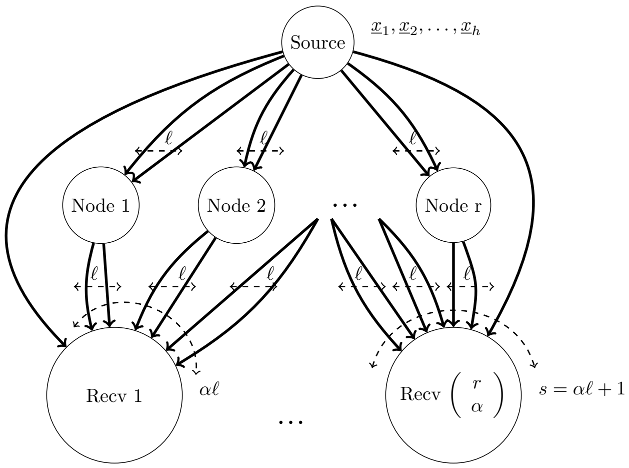
Figure 4.3: The $(1,2)-\mathcal{N}_{4,r,5}$ network as an example of the $(\ell-1,\ell)-\mathcal{N}_{2\ell,r,3\ell-1}$



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

This is the smallest direct-link family has an vector solution outperforming the optimal scalar solution, i.e. an vector solution outperforming the optimal scalar has not yet been found for the network $(0,\ell>1)-\mathcal{N}_{h,r,s}$. Similar to the previous subfamily $(\epsilon=\ell-1,\ell)-\mathcal{N}_{h=2\ell,r,s=3\ell-1}$, when $\ell \geq 2$ or $h \geq 4$, this network yields the largest gap $q^{t^2/2+\mathcal{O}(t)}$ in the alphabet size by using the same approach with an $\mathcal{MRD}\left[\ell t \times \ell t, (\ell-1)t\right]_q$ code.

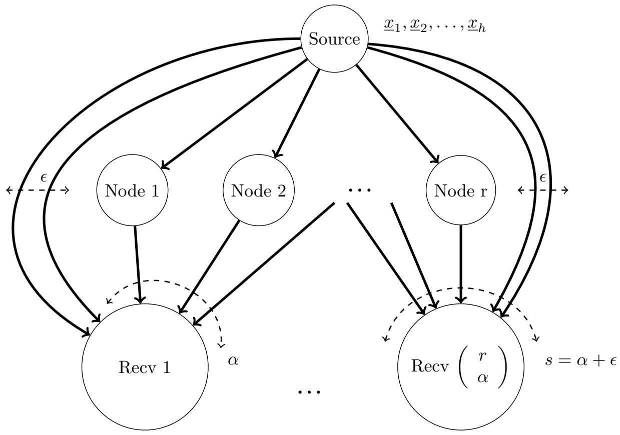
Figure 4.4: The $(\ell-1,\ell)-\mathcal{N}_{2\ell,r,3\ell-1}$ network



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

This family is denoted as $(\epsilon \geq 1, \ell = 1)-\mathcal{N}_{h,r,s}$ 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. In Section 5.1, we show our largest code set with low number of subspace codes for the network $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h=3,r,s=4}$. Furthermore, there is no gap size is known for this network in previous studies.

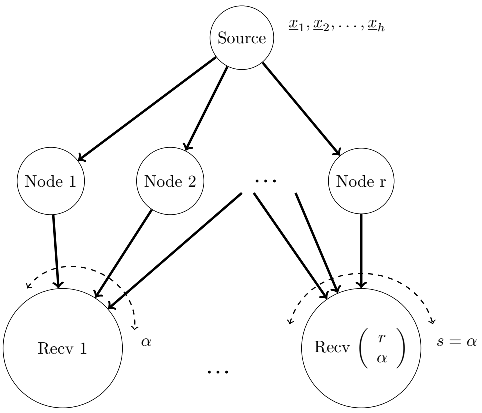
Figure 4.5: The $(\epsilon \geq 1, \ell = 1) - \mathcal{N}_{h,r,s}$ network



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], it is proved that vector solutions based on subspace codes cannot outperform optimal scalar linear solutions for $h = 2$, and they conjecture it for all h. Unfortunately, a vector solution based on an $\mathcal{MRD}\left[t \times t, t\right]_q$ code is also proved that it cannot outperform the optimal scalar linear solution.

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

$h \leq 2\ell$ **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 $(\ell-1, l) - \mathcal{N}_{2\ell,r,3\ell-1}$ network achieves the largest gap $q_\mathrm{s} = q^{(h-2)t^2/h+\mathcal{O}(t)}$.

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

$h \geq 2\ell$ **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 $(\ell-1,\ell)\text{–}\mathcal{N}_{2\ell+1,r,3\ell-1}$ network achieves the largest gap $q_\mathrm{s} = q^{(h-3)t^2/(h-1)+\mathcal{O}(t)}$.

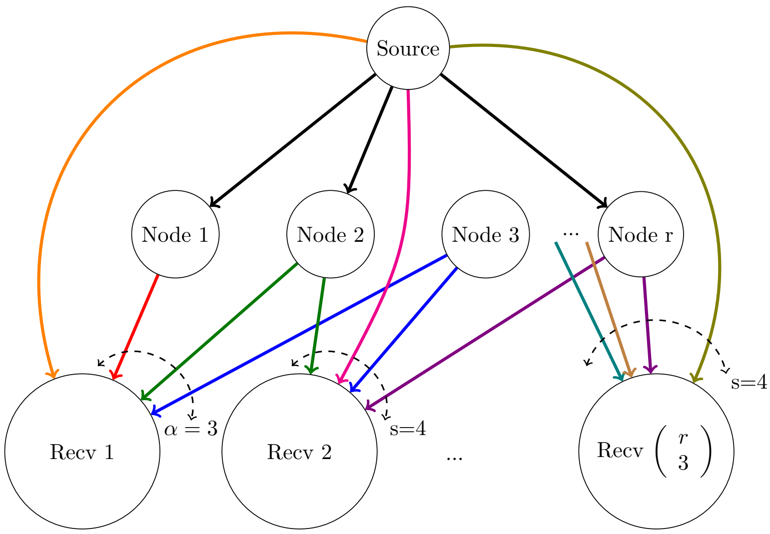
Remark 4.1. The achieved gap is $q^{(h-2)t^2/h+\mathcal{O}(t)}$ for any $q \geq 2$ and any even $h \geq 4$. If $h \geq 5$ is odd, then the achieved gap of the alphabet size is $q^{(h-3)t^2/(h-1)+\mathcal{O}(t)}$ [EW18].

5 Combinatorial Results

In previous studies [EW18], there was no general vector solution 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.

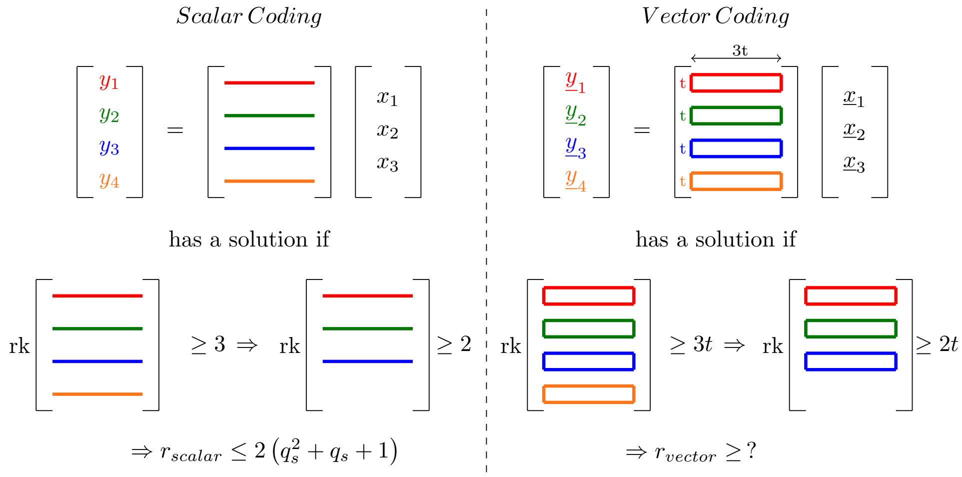
5.1 $(\epsilon = 1, \ell = 1) - \mathcal{N}_{h=3,r,s=4}$ Network

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 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 must solve a linear equation system of 3 variables with 4 equations to recover $h = 3$ messages as below:

$$\begin{bmatrix} \boldsymbol{y}_{j_1} \\ \boldsymbol{y}_{j_2} \\ \boldsymbol{y}_{j_3} \\ \boldsymbol{y}_{j_4} \end{bmatrix} = \boldsymbol{A}_j \cdot \underline{x} = \begin{bmatrix} \boldsymbol{A}_{j_1} \\ \boldsymbol{A}_{j_2} \\ \boldsymbol{A}_{j_3} \\ \boldsymbol{A}_{j_4} \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \boldsymbol{x}_3 \end{bmatrix},$$

with $\boldsymbol{x}_i, \boldsymbol{y}_{j_v} \in \mathbb{F}_q^t$, $\boldsymbol{A}_{j_v} \in \mathbb{F}_q^{t \times 3t}$ for $v = 1, \ldots, 4$, and $\boldsymbol{A}_{j_1}, \ldots, \boldsymbol{A}_{j_3}$ must be distinct. The network is solvable, if $\boldsymbol{A}_j$ has full-rank, i.e. $\boldsymbol{A}_{j_v}$ must satisfy:

$$rk \begin{bmatrix} \boldsymbol{A}_{j_1} \\ \boldsymbol{A}_{j_2} \\ \boldsymbol{A}_{j_3} \\ \boldsymbol{A}_{j_4} \end{bmatrix} \geq 3t$$

In order to satisfy $rk\left[\boldsymbol{A}_j\right] \geq 3t$, we can easily choose suitable values for the coefficient $\boldsymbol{A}_{j_4}$ on the direct link from the source to R_j. However, the coefficients on the links from nodes to receivers are matters. Therefore, we focus on the following requirement:

$$rk \begin{bmatrix} \boldsymbol{A}_{j_1} \\ \boldsymbol{A}_{j_2} \\ \boldsymbol{A}_{j_3} \end{bmatrix} \geq 2t \qquad (5.1)$$

This means that $rk \begin{bmatrix} \boldsymbol{A}_{j_1} \\ \boldsymbol{A}_{j_2} \\ \boldsymbol{A}_{j_3} \end{bmatrix} \geq 2t$ implies $rk\left[\boldsymbol{A}_j\right] \geq 3t$, or to satisfy $rk\left[\boldsymbol{A}_j\right] \geq 3t$, we need $rk \begin{bmatrix} \boldsymbol{A}_{j_1} \\ \boldsymbol{A}_{j_2} \\ \boldsymbol{A}_{j_3} \end{bmatrix} \geq 2t$.

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

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

$\boldsymbol{A}_{j_1}, \boldsymbol{A}_{j_2}, \boldsymbol{A}_{j_3}$ 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 [Sch].

Lemma 5.1 (Symmetric Lovász local lemma (LLL) [SCV13]). *A set of events $\mathcal{E}_i$, with $i = 1, \ldots, n$, 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: $Pr\left[\bigcap_{i=1}^{n} \overline{\mathcal{E}}_i\right] > 0$.*

Lemma 5.2. *For the network $(\epsilon = 1, l = 1) - \mathcal{N}_{h=3,r,s=4}$, the probability that vector solution does not exist is equal to $\frac{1}{q^{9t^2}} \sum_{i=0}^{2t-1} \prod_{j=0}^{i-1} \frac{\left(q^{3t} - q^j\right)^2}{q^i - q^j}$.*

Proof. For our problem, let $\mathcal{E}_i$ denote the following event:

$$Pr\left[\mathcal{E}_i\right] = Pr\left[rk \begin{bmatrix} \boldsymbol{A}_{j_1} \\ \boldsymbol{A}_{j_2} \\ \boldsymbol{A}_{j_3} \end{bmatrix} < 2t\right]$$

Because the rank requirement in Equation 5.1 is opposite, we consider the complement event T:

$$rk \begin{bmatrix} \boldsymbol{A}_{j_1} \\ \boldsymbol{A}_{j_2} \\ \boldsymbol{A}_{j_3} \end{bmatrix} \geq 2t, \forall 1 \leq j_1 < j_2 < j_3 \leq r$$

By the intersection rule, we have:

$$T = \bigcap_{\mathcal{E}_i \in \mathcal{E}} \overline{\mathcal{E}}_i$$

The probability of event T indicates a measure quantifying the likelihood that we will be able to construct $rk\left[\boldsymbol{A}_j\right] \geq 3t$ with j_1,j_2, j_3 in the integer numbers between 1 and r, including both. We need to maximize r, and the rank requirement 5.1 must be satisfied, i.e. the probabilty of event T must be higher than 0:

$$\begin{aligned}
& Pr\left[rk\begin{bmatrix}\boldsymbol{A}_{j_1}\\ \boldsymbol{A}_{j_2}\\ \boldsymbol{A}_{j_3}\end{bmatrix} \geq 2t, \forall 1 \leq j_1 < j_2 < j_3 \leq r\right] && > 0\\
\Leftrightarrow \quad & Pr\left[T\right] && > 0\\
\Leftrightarrow \quad & Pr\left[\bigcap_{\mathcal{E}_i \in \mathcal{E}} \overline{\mathcal{E}}_i\right] && > 0
\end{aligned}$$

Following to LLL, each event occurst with probability at most p:

$$Pr\left[\mathcal{E}_i\right] = Pr\left[rk\begin{bmatrix}\boldsymbol{A}_{i_1}\\ \boldsymbol{A}_{i_2}\\ \boldsymbol{A}_{i_3}\end{bmatrix} < 2t\right] \leq p \tag{5.2}$$

Regarding to the left-hand side:

$$\begin{aligned}
Pr\left[rk\begin{bmatrix}\boldsymbol{A}_{i_1}\\ \boldsymbol{A}_{i_2}\\ \boldsymbol{A}_{i_3}\end{bmatrix} < 2t\right] &= \sum_{i=0}^{2t-1} Pr\left[rk\begin{bmatrix}\boldsymbol{A}_{i_1}\\ \boldsymbol{A}_{i_2}\\ \boldsymbol{A}_{i_3}\end{bmatrix} = i\right]\\
&\stackrel{1}{=} \sum_{i=0}^{2t-1} \frac{N_{t,m,n}}{q^{m\cdot n}}\\
&= \sum_{i=0}^{2t-1} \frac{\prod_{j=0}^{i-1} \frac{\left(q^m - q^j\right)\left(q^n - q^j\right)}{q^i - q^j}}{q^{m\cdot n}}\\
&\stackrel{2}{=} \sum_{i=0}^{2t-1} \frac{\prod_{j=0}^{i-1} \frac{\left(q^{3t} - q^j\right)^2}{q^i - q^j}}{q^{9t^2}} \square
\end{aligned} \tag{5.3}$$

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 $(\epsilon = 1, l = 1) - N_{h=3,r,s=4}$. This is sufficient, later on we show computational results which vector solutions outperform scalar solutions in case of $t = 2$ and $t = 3$.

Lemma 5.3. *For the network $(\epsilon = 1, l = 1) - \mathcal{N}_{h=3,r,s=4}$, the probability that vector solution does not exist is less than or equal to $\Theta\left(q^{-t^2-2t-1}\right)$.*

Proof. This lemma is a tight bound for Equation 5.2 in Lemma 5.2, i.e. we try to maximize p with an exact maximum value. We consider the nominator of Equation (5.3):

$$\prod_{j=0}^{i-1} \frac{\left(q^{3t} - q^{j}\right)^2}{q^i - q^j} = \frac{p_N^{(i)}(q)}{p_D^{(i)}(q)} = p^{(i)}(q)$$

Due to i-times product and large t:

$$\left.\begin{aligned} deg\left(p_N^{(i)}(q)\right) &= q^{i6t} \\ deg\left(p_D^{(i)}(q)\right) &= q^{i^2} \end{aligned}\right\} \Rightarrow p^{(i)}(q) \approx q^{i6t-i^2}$$

Then we have:

$$\sum_{i=0}^{2t-1}\prod_{j=0}^{i-1} \frac{\left(q^{3t} - q^{j}\right)^2}{q^i - q^j} = \sum_{i=0}^{2t-1} p^{(i)}(q) \approx \sum_{i=0}^{2t-1} q^{i6t-i^2}$$

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

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

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

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

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

$$\sum_{i=0}^{2t-1} p^{(i)}(q) \in \Theta\left(max\left\{q^{i6t-i^2} : i = 1, 2\ldots, 2t-1\right\}\right) = \Theta\left(q^{8t^2-2t-1}\right)$$

$$\Rightarrow \frac{\sum\limits_{i=0}^{2t-1} p^{(i)}(q)}{q^{9t^2}} \in \Theta\left(q^{-t^2-2t-1}\right) \square$$

Lemma 5.4. *If $d \leq \frac{3}{2}r^2$, we have $r_{max,vector} \geq \Omega\left(q^{t^2/2+\mathcal{O}(t)}\right)$.*

Proof. We proceed the other constraint of LLL in Lemma 5.1: $4dp \leq 1$. Regarding to d, we have:

$$\begin{aligned} d(r) &\leq 3 \cdot \begin{pmatrix} r-1 \\ 2 \end{pmatrix} = 3 \cdot \frac{(r-1)(r-2)}{2} = \frac{3}{2}\left(r^2 - 3r + 2\right) \\ &\leq \frac{3}{2}r^2 = d_{max}(r) \end{aligned}$$

Because $4pd_{max}(r) \leq 1$ implies that $4pd \leq 1$, we consider $d_{max}(r)$ directly:

$$4 \cdot p \cdot d_{max}(r) \leq 1 \Rightarrow 4 \cdot p \cdot \frac{3}{2}r^2 \leq 1 \Rightarrow r \leq \sqrt{\frac{1}{6p}} = r_{max,vector}$$

Similarly with above, d and r are propotional, so minimizing r is equivelent to maximizing p. The purpose is to achieve a strict lower bound proving vector solutions always outperform scalar solutions in a specific range of t, i.e., $r_{max,vector}$ asymptotes to a value higher than $r_{max,scalar}$.

By applying Lemma 5.3, we have:

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

Theorem 5.1. *For the network $(\epsilon = 1, l = 1) - \mathcal{N}_{h=3,r,s=4}$, the achieved gap is $q^{t^2/4+\mathcal{O}(t)}$.*

Proof. In advance, we have: $r_{max,scalar} \in \mathcal{O}\left(q_s^2\right)$ [EW18], specifically,

$$r_{scalar} \leq 2 \begin{bmatrix} 3 \\ 1 \end{bmatrix}_{q_s} = 2\left(q_s^2 + q_s + 1\right) \tag{5.4}$$

.

Finally, following to Section 3.4.2 and Lemma 5.4, we have the gap size:

$$\begin{aligned} & r_{max,scalar} && = r_{max,vector} \\ \Leftrightarrow \quad & q_{\text{s}}^2 && = q^{t^2/2+\mathcal{O}(t)} \\ \Leftrightarrow \quad & q_{\text{s}} && = q^{t^2/4+\mathcal{O}(t)} \\ \Rightarrow \quad & g && = q_{\text{s}} - q_v = q^{t^2/4+\mathcal{O}(t)} \square \end{aligned} \tag{5.5}$$

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

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

Following to Theorem (4.1), we are interested in the following range: $\ell+\epsilon+1 \leq h \leq \alpha\ell+\epsilon$. As previous, $\boldsymbol{A}_{j_1}, \ldots, \boldsymbol{A}_{j_{h-\epsilon}} \in \mathbb{F}_q^{t\times ht}$ and we need to satisfy the following:

$$rk \begin{bmatrix} \boldsymbol{A}_{j_1} \\ \vdots \\ \boldsymbol{A}_{j_{h-\epsilon}} \end{bmatrix} \geq ht - t \Leftrightarrow rk\left[\boldsymbol{A}_j\right] \geq (h-1)t$$

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 to $(\epsilon = 1, \ell = 1) - N_{3,r,4}$, we consider p to proceed LLL:

$$Pr\left[rk\left[\boldsymbol{A}\right] < (h-1)t\right] \leq p$$

Regarding to the left-hand side:

$$\begin{aligned} Pr\left[rk\left[\boldsymbol{A}\right] < (h-1)t\right] &= \sum_{i=0}^{(h-1)t-1} Pr\left[rk\left[\boldsymbol{A}\right] = i\right] \\ &\stackrel{1}{=} \sum_{i=0}^{(h-1)t-1} \frac{N_{i,\alpha t,ht}}{q^{(\alpha t)(ht)}} \\ &= \frac{1}{q^{(\alpha h)t^2}} \cdot \sum_{i=0}^{(h-1)t-1} \prod_{j=0}^{i-1} \frac{\left(q^{\alpha t} - q^j\right)\left(q^{ht} - q^j\right)}{q^i - q^j} \end{aligned} \tag{5.6}$$

Firstly, we consider the product:

$$\prod_{j=0}^{i-1} \frac{\left(q^{\alpha t} - q^{j}\right)\left(q^{ht} - q^{j}\right)}{q^{i} - q^{j}} = \frac{p_N^{(i)}(q)}{p_D^{(i)}(q)} = p^{(i)}(q)$$

For $t \to \infty$:

$$\left.\begin{array}{r} deg\left(p_N^{(i)}(q)\right) = q^{i(\alpha t + ht)} \\ deg\left(p_D^{(i)}(q)\right) = q^{i^2} \end{array}\right\} \Rightarrow p^{(i)}(q) \approx q^{i(\alpha t + ht) - i^2}$$

Now, we evaluate $f(i) = i(\alpha t + ht) - i^2$ to find its maximum point:
$\dot{f}(i^*) = 0 \Leftrightarrow (\alpha t + ht) - 2i^* = 0 \Leftrightarrow i^* = \frac{\alpha t + ht}{2}$
We then check whether this point within the range $i = 0, \ldots, (h-1)t - 1$ 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 $\alpha l + \epsilon = \alpha + 1 \geq h$. This cannot happen because of $t \geq 2$, i.e. this maximum point is over then upper-range limit.

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

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

$$\sum_{i=0}^{(h-1)t-1} p^{(i)}(q) \in \Theta\left(q^{[(h-1)(\alpha+1)]t^2 + \mathcal{O}(t)}\right)$$

Thirdly, we consider the 3rd requirement of LLL to figure out a lower bound on r_{max}:
$d \leq \alpha \begin{pmatrix} r-1 \\ \alpha - 1 \end{pmatrix} = \alpha \frac{(r-1)\ldots(r-\alpha+1)}{(\alpha-1)!} \leq \frac{\alpha}{(\alpha-1)!} r^{\alpha - 1} = d_2$
We need $4dp \leq 1$, which is satisfied if $4d_2 p \leq 1$. Therefore, we consider:
$\frac{\alpha}{(\alpha-1)!} r^{\alpha-1} \leq \frac{1}{4p} \Leftrightarrow r \leq \left(\frac{(\alpha-1)!}{4\alpha} \cdot \frac{1}{p}\right)^{\frac{1}{\alpha-1}}$
Finally, we have from above:

$$\begin{aligned} p &\in \Theta\left(\frac{q^{[(h-1)(\alpha+1)]t^2 + \mathcal{O}(t)}}{q^{(\alpha h)t^2}}\right) \\ \Rightarrow r_{min,vector} &\in \Omega\left(q^{\frac{h-\alpha-1}{1-\alpha}t^2 + \mathcal{O}(t)}\right) \end{aligned}$$

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

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 $q_s = q^t$.

For $3 \leq \alpha < h$: all α links must be distinct $\Rightarrow r \leq \begin{bmatrix} \alpha \\ 1 \end{bmatrix}_{q_s} \Rightarrow r \leq$

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

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

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 $t = 3$. Both construction 1 and 2 provide better results than scalar solutions.
Construction 1: $\boldsymbol{I}_t \,\Big|\, \boldsymbol{T}$, with $\boldsymbol{T} \in \mathbb{F}_q^{t \times t(h-1)}$
Construction 2: $\boldsymbol{T} \in MatrixSpaceUrs\,(t, 3t)$
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-dimensionall 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.

Definition 6.1 (Sufficient Global Coding Vector)**.** Let $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \in \mathbb{F}_q^{n \times m}$. Then a set $\{\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}\}$ forms a subset of $g^{(3)}$ if

$$rk \begin{bmatrix} \boldsymbol{A} \\ \boldsymbol{B} \\ \boldsymbol{C} \end{bmatrix} \geq 2n$$

In other words, all $\{\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}\}$ span a subspace of $\mathbb{F}_q^{2n}$ whose dimension is at least $2n$. We denote $g3_i$ as a subset of $g3$:

$$g^{(3)} = \{\{\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}\}_i\} = \left\{g_i^{(3)}\right\}, i = 0, 1, 2, ..., \left|g^{(3)}\right| - 1$$

with $g_i^{(3)} = \{\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}\}_i$

Definition 6.2 (Relative)**.** Let $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \in \mathbb{F}_q^{n \times m}$. Then $\boldsymbol{C}$ is called a relative of a tuple $(\boldsymbol{A}, \boldsymbol{B})$ if $\{\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}\} \in g^{(3)}$ and denoted as following:

$$rel\left[(\boldsymbol{A}, \boldsymbol{B})\right] = \boldsymbol{C}$$

Definition 6.3 (Sub-relative)**.** Let $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D} \in \mathbb{F}_q^{n \times m}$. Then $\boldsymbol{D}$ is called a sub-relative of a tuple $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}) \in g^{(3)}$ if:

$$\begin{cases} \{\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{D}\} \in g3 \\ \{\boldsymbol{A}, \boldsymbol{C}, \boldsymbol{D}\} \in g3 \\ \{\boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}\} \in g3 \end{cases}$$

It is denoted as:

$$subrel\left[(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})\right] = \boldsymbol{D}$$

This definition is reused for a set of 5 or more matrices.

Definition 6.4 (MatrixSpace)**.** $MatrixSpace(n, m) = \left\{\boldsymbol{A} : \boldsymbol{A} \in \mathbb{F}_q^{n \times m}\right\}$

Definition 6.5 (MatrixSpace with unique row space)**.** $MatrixSpaceUrs(n, m)$ is a subspace of $\mathbb{F}_q^{n \times m}$, where any $\boldsymbol{A}, \boldsymbol{B} \in \mathbb{F}_q^{n \times m}$ have their row spaces such that:

$$\mathcal{R}_q\left(\boldsymbol{A}\right) \neq \mathcal{R}_q\left(\boldsymbol{B}\right)$$

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

Algorithm 1 Increasing Method

INPUT: $g^{(3)}$ of N matrices belonging to $MatrixSpace(n, m)$ or $MatrixSpaceUrs(n, m)$

1. Create a list of $rel\left[(\boldsymbol{A}, \boldsymbol{B})\right], \forall \boldsymbol{A}, \boldsymbol{B} \in MatrixSpace(n, m), \boldsymbol{A} \neq \boldsymbol{B}$

2. Choose all $\{\boldsymbol{A}, \boldsymbol{B}\}$ such that:

$$|rel\left[(\boldsymbol{A}, \boldsymbol{B})\right]| = |rel\left[(\boldsymbol{A}, \boldsymbol{B})\right]|_{max}$$

   with an upper bound for the final result set's cardinality $|Res| \leq UB, UB = |rel\left[(\boldsymbol{A}, \boldsymbol{B})\right]|_{max}$.

3. For each found pair set of $\{\boldsymbol{A}, \boldsymbol{B}\}$, we compute the union set of the pair and its Relative, i.e., $\{\boldsymbol{A}, \boldsymbol{B}\} \cup rel\left[(\boldsymbol{A}, \boldsymbol{B})\right]$. If the union set is repeated or duplicated, we take only the first pair generating such value. We denote the chosen set as $main\_team\_and\_rel$

4. Considering $main\_team\_and\_rel_i \in main\_team\_and\_rel$ with $i = 0, 1, 2, ..., |main\_team\_and\_rel| - 1$, we have

$$\begin{gathered} rel_j \in rel\left[main\_team\_and\_rel_i\right] \\ \forall main\_team\_and\_rel_i \in main\_team\_and\_rel \\ j = 0, 1, 2, ..., |main\_team\_and\_rel_i| - 1 \end{gathered}$$

   to compute $n\_main\_team_i$, which is combined by $\{\boldsymbol{A}, \boldsymbol{B}, rel_j\}$ if $|subrel\left[(\boldsymbol{A}, \boldsymbol{B}, rel_j)\right]|_{max}$ similarly to step 2.

5. Keep only $n\_main\_team_i$ with $|subrel\left[(n\_main\_team_i)\right]|_{max}$ with $i = 0, 1, 2, ..., |main\_team\_and\_rel| - 1$. Similar to step 3, we also avoid duplicated values here.

6. Repeat step 4, 5, 6 until $|subrel\left[(n\_main\_team_i)\right]|_{max} = 0$

OUTPUT: Get the final result set with all matrices such that:

$$Res = \left\{\boldsymbol{X}_i : \boldsymbol{X}_i \in \mathbb{F}_q^{n \times m}\right\}, i = 0, 1, ..., UB$$

with any 3 combinations of $(\boldsymbol{X}_j, \boldsymbol{X}_k, \boldsymbol{X}_t) \in g^{(3)}, \forall \boldsymbol{X}_j, \boldsymbol{X}_k, \boldsymbol{X}_t \in Res, \boldsymbol{X}_j \neq \boldsymbol{X}_k \neq \boldsymbol{X}_t$ and $j \neq k \neq t$.

Example 1: Let $n = 1, m = 2, q = 2$. Then we have $N = 4$ matrices (vectors):

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

Step 1: Due to, any 3 of them form a matrix with $rk \geq 2n$, we have the relative as following:

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

Step 2: We get $UB = 2$ and all $\{\boldsymbol{A},\boldsymbol{B}\},\{\boldsymbol{A},\boldsymbol{C}\},\{\boldsymbol{A},\boldsymbol{D}\},\{\boldsymbol{B},\boldsymbol{C}\},\{\boldsymbol{B},\boldsymbol{D}\},\{\boldsymbol{C},\boldsymbol{D}\}$, because $\underset{\substack{\forall \boldsymbol{X},\boldsymbol{Y} \in MatrixSpace(1,2)\\ \boldsymbol{X} \neq \boldsymbol{Y}}}{max} \left(rel\left[(\boldsymbol{X},\boldsymbol{Y})\right]\right) = 2$

Step 3: Due to $\{\boldsymbol{X},\boldsymbol{Y}\} \cup rel\left[(\boldsymbol{X},\boldsymbol{Y})\right] = \{\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D}\}$ with $(\boldsymbol{X},\boldsymbol{Y})$ are all tuples found in Step 2. We keep only $main\_team\_and\_rel = \{(\boldsymbol{A},\boldsymbol{B}) : rel\left[(\boldsymbol{A},\boldsymbol{B})\right]\}$

Step 4: Regarding to $rel\left[(\boldsymbol{A},\boldsymbol{B})\right]$, we have $rel_0 = \boldsymbol{C}, rel_1 = \boldsymbol{D}$. Then, $|subrel\left[(\boldsymbol{A},\boldsymbol{B},rel_0)\right]| = |subrel\left[(\boldsymbol{A},\boldsymbol{B},rel_1)\right]| = 1$, so we got $n\_main\_team_0 = \{\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}\}$ as the only output of this step.

Step 5: Because step 4 gets only $\{\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}\}$, we do not need to proceed anything here.

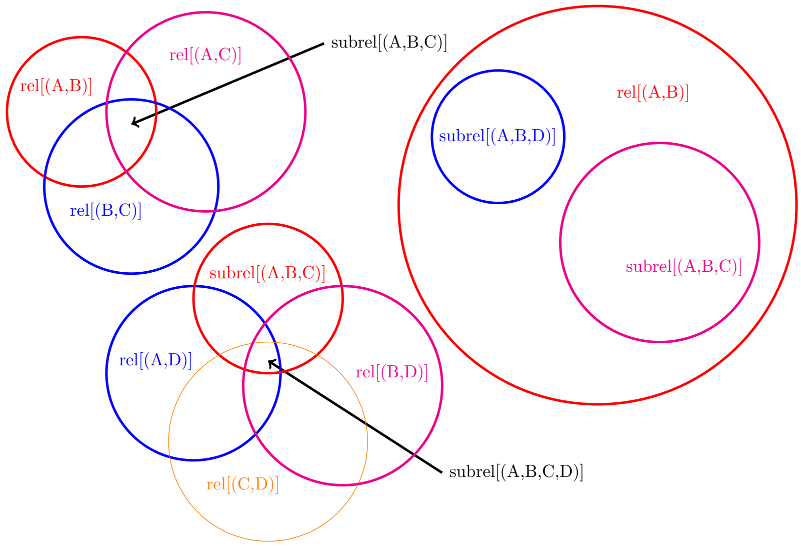
Step 6: We repeat step 4 and 5 once more and we get $Res = \{\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D}\}$, i.e., all the matrices can be used.

Example 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. $|rel\left[(\boldsymbol{A},\boldsymbol{B})\right]| \geq |subrel\left[(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C})\right]|$ or $|rel\left[(\boldsymbol{A},\boldsymbol{B})\right]| \geq |subrel\left[(\boldsymbol{A},\boldsymbol{B},\boldsymbol{D})\right]|$. It explains why UB is the maximum numbers of matrices that we can find in Res.

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



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.

[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 Zúrich, 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.

[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.