



Master's Thesis

# Vector Network Coding

Vorgelegt von:

Ha Nguyen

München, 07 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  
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, 18.07.2019

Ort, Datum

.....  
(Ha Nguyen)



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Preliminaries</b>	<b>3</b>
<b>3</b>	<b>Generalized combination Network <math>(\epsilon, l) - \mathcal{N}_{h,r,s}</math></b>	<b>5</b>
3.1	Description . . . . .	5
3.2	Which network codes over $\mathbb{F}_q$ solve the networks from this network family?	6
3.3	Special cases of generalized combination network . . . . .	6
3.3.1	The $(l - 1)$ -Direct Links and $l$ -Parallel Links $\mathcal{N}_{h=2l,r,s=3l-1}$ . . . . .	6
3.3.2	The 1-Direct Link and $l$ -Parallel Links $\mathcal{N}_{h=2l,r,s=2l+1}$ . . . . .	6
3.3.3	The $\epsilon$ -Direct Links $\mathcal{N}_{h,r,s}$ . . . . .	6
3.3.4	The $(\epsilon = 0, l = 1) - \mathcal{N}_{h,r,s}$ Combination Network . . . . .	7
3.3.5	The 2 networks yields gap $q^{(h-3)t^2/(h-1)+\mathcal{O}(t)}$ . . . . .	7
<b>4</b>	<b>Network as a matrix channel</b>	<b>9</b>
4.1	Definition of scalar coding and vector coding . . . . .	9
4.2	Comparison between scalar and vector coding by the gap size . . . . .	11
<b>5</b>	<b>Combinatorial Results</b>	<b>13</b>
5.1	$(\epsilon = 1, l = 1) - \mathcal{N}_{h=3,r,s=4}$ Network . . . . .	13
5.2	$(\epsilon = 1, l = 1) - \mathcal{N}_{h,r,s}$ Network . . . . .	18
5.2.1	Find the lower bound of $r_{max,vector}$ . . . . .	18
5.2.2	Find the upper bound of $r_{max,scalar}$ . . . . .	20
5.2.3	Calculate the gap of size . . . . .	20
<b>6</b>	<b>Computational Results</b>	<b>21</b>
<b>7</b>	<b>Conclusion</b>	<b>23</b>
<b>8</b>	<b>Appendix</b>	<b>25</b>
	<b>Bibliography</b>	<b>I</b>



## List of Figures





# List of Tables

4.1	Notations of network coding . . . . .	11
5.1	$r_{max}$ over variations of $t$ . . . . .	16



# 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

**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*. 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  $\mathbb{F}_q^n$ :

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

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



### 3 Generalized combination Network

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

#### 3.1 Description

A generalized combination network  $(\epsilon, l) - \mathcal{N}_{h,r,s}$  consists of 3 components from top to bottom: “Source” in the first layer, “Node” in the middle layer, and “Receiver” in the third layer. 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. 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  $\alpha l$  links from  $\alpha$  nodes and  $\epsilon$  direct links from the source, i.e.  $s = \alpha l + \epsilon$ . Theorem 1 shows our interest of relations between the parameters  $h, \alpha, \epsilon$  and  $l$ .

**Theorem 3.1.** *The  $(\epsilon, l) - \mathcal{N}_{h,r,s}$  network has a trivial solution if  $l + \epsilon \geq h$ , and it has no solution if  $\alpha l + \epsilon < h$ .*

*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,  $h \leq s \Leftrightarrow h \leq \alpha l + \epsilon$   $\square$

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

The combination network in [RA06] is the  $(0, 0) - \mathcal{N}_{h,r,s}$  network. One-Direct Link Combination Network  $(1, 1) - \mathcal{N}_{h,r,s}$ .

### 3.2 Which network codes over $\mathbb{F}_q$ solve the networks from this network family?

The source can send any required  $\epsilon$  1-dimensional subspace of  $\mathbb{F}_{q_s}^h$  through  $\epsilon$  direct links to a receiver. For each receiver to reconstruct  $h$  messages, the linear span of  $\alpha l$  1-dimensional subspaces received from  $\alpha$  nodes must be at least of dimension of  $h - \epsilon$ , i.e.  $\alpha l$  1-dimensional subspaces span at least  $(h - \epsilon)$ -dimensional subspace of  $\mathbb{F}_{q_s}^h$ . Hence, a scalar linear solution for the generalized combination network exists, if and only if, there exists a Grassmannian code  $\mathcal{G}_{q_s}(h, k \geq h - \epsilon)$  with  $\binom{r}{\alpha} l$  1-dimensional subspaces of  $\mathbb{F}_{q_s}^h$ .

**Theorem 3.2.**  $(0, 1) - \mathcal{N}_{h,r,s}$  has a solution if and only if there exists an  $(r, q_s h, r - \alpha + 1)$   $q_s$ -ary error correcting code.

### 3.3 Special cases of generalized combination network

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

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

**Lemma 3.1.** There is a scalar linear solution of field size  $q_s$  for the  $(\epsilon = l - 1, l) - \mathcal{N}_{h=2l,r,s=3l-1}$  network, where  $l \geq 2$ , if and only if  $r \leq \left[ \begin{smallmatrix} 2l \\ l \end{smallmatrix} \right]_{q_s}$ .

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

This is the smallest direct-link subfamily 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  $(0, l > 1) - \mathcal{N}_{h,r,s}$ . Similar to the previous subfamily  $(\epsilon = l - 1, l) - \mathcal{N}_{h=2l,r,s=3l-1}$ , when  $l \geq 2$  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  $\mathcal{MRD}[lt \times lt, (l - 1)t]_q$  code.

#### 3.3.3 The $\epsilon$ -Direct Links $\mathcal{N}_{h,r,s}$

This subfamily is denoted as  $(\epsilon \geq 1, l = 1) - \mathcal{N}_{h,r,s}$  and is the most focus topic on this thesis, because it motivates some interesting questions on a classic coding problem and



on a new type of subspace code problem. In the chapter 3, we show our largest code set with low number of subspace codes for the network  $(\epsilon = 1, l = 1) - \mathcal{N}_{h=3, r, s=4}$ .

### 3.3.4 The $(\epsilon = 0, l = 1) - \mathcal{N}_{h, r, s}$ 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  $\mathcal{MRD}[t \times t, t]_q$  code is also proved that it cannot outperform the optimal scalar linear solution.

### 3.3.5 The 2 networks yields gap $q^{(h-3)t^2/(h-1)+\mathcal{O}(t)}$

For  $h = 2l - 1$ :  $(\epsilon = l - 2, l) - \mathcal{N}_{h=2l-1, r, s=3l-2}$

For  $h = 2l + 1$ :  $(\epsilon = l - 1, l) - \mathcal{N}_{h=2l+1, r, s=3l-1}$



## 4 Network as a matrix channel

To clarify the difference between scalar coding and vector coding, we firstly represent the network as a matrix channel, then secondly we show the advantages of vector coding in choosing coding coefficients, and we finally introduce a gap in alphabet size between scalar coding's and vector's coding solutions, which supports in showing an improvement in the alphabet size for the vector solutions.

### 4.1 Definition of scalar coding and vector coding

To formulate this description, the source has a set of disjoint messages referred to packets which are either symbols from  $\mathbb{F}_{q^t}$  (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*. The linear equation system that any receiver  $R_j$  has to solve is as following:

$$\begin{array}{c} \text{Scalar} \\ \left[ \begin{array}{c} y_{j1} \\ \vdots \\ y_{js} \end{array} \right]_{\mathbb{F}_{q^t}^s} = \underbrace{\mathbf{A}_j}_{\mathbb{F}_{q^t}^{s \times h}} \cdot \underbrace{\left[ \begin{array}{c} x_1 \\ \vdots \\ x_h \end{array} \right]}_{\mathbb{F}_{q^t}^h} \end{array} \quad \left| \quad \begin{array}{c} \text{Vector} \\ \left[ \begin{array}{c} \underline{y}_{j1} \\ \vdots \\ \underline{y}_{js} \end{array} \right]_{\mathbb{F}_q^{st}} = \underbrace{\mathbf{A}_j}_{\mathbb{F}_q^{st \times th}} \cdot \underbrace{\left[ \begin{array}{c} \underline{x}_1 \\ \vdots \\ \underline{x}_h \end{array} \right]}_{\mathbb{F}_q^{th}} \end{array} \right. \quad (4.1)$$

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

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

In general, the network is represented as a matrix channel:

**Definition 4.1.** Network As Matrix Channel

The channel output can be written as:  $\mathbf{Y}_j = \mathbf{A}_j \cdot \mathbf{X}$

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  $\underline{x}_1, \dots, \underline{x}_h$ . Therefore, 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  $q^t$  is minimized. The solutions of scalar and vector coding are always equivalent due to our use of scalar symbols from  $\mathbb{F}_{q^t}$ , which is explained better in Example 4.1. Because we reconstruct  $\mathbf{X}$  with knowing  $\mathbf{A}_j$ , i.e. the network structure is known,

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

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

power of $\alpha$	polynomial	binary vector
-	0	00
$\alpha^0$	1	01
$\alpha^1$	$\alpha$	10
$\alpha^2$	$\alpha + 1$	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  $\underline{x}_1, \dots, \underline{x}_{h=3} \in \mathbb{F}_2^2$ . From the polynomial column, let's choose arbitrarily a scalar vector  $\underline{x}_{scalar} = (x_1, x_2, x_3) = (1, \alpha, \alpha + 1)$ . Then, we map it to  $\underline{x}_{vector} = (\underline{x}_1, \underline{x}_2, \underline{x}_3)$  by using the binary vector column as following:

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

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

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

To summarize the notations of both scalar and vector coding, we represent them in the Table 4.1:

Table 4.1: Notations of network coding

	Scalar Coding	Vector coding
Source Messages/Packets	$x_1, \dots, x_h \in \mathbb{F}_{q^t}$ $\underline{x} \in \mathbb{F}_{q^t}^h$	$\underline{x}_1, \dots, \underline{x}_h \in \mathbb{F}_q^t$ $\underline{x} \in \mathbb{F}_q^{th}$
Global Coding Vectors Of Receiver $R_j$	$\underline{a}_{j_1}, \dots, \underline{a}_{j_{\alpha l}} \in \mathbb{F}_{q^t}^h$ $\underline{b}_{j_1}, \dots, \underline{b}_{j_{\epsilon}} \in \mathbb{F}_{q^t}^h$	$\mathbf{A}_{i_1}, \dots, \mathbf{A}_{i_{\alpha l}} \in \mathbb{F}_q^{t \times th}$ $\mathbf{B}_{j_1}, \dots, \mathbf{B}_{j_{\epsilon}} \in \mathbb{F}_q^{t \times th}$
Transfer Matrix Of Receiver $R_j$	$\mathbf{A}_j \in \mathbb{F}_{q^t}^{s \times h}$	$\mathbf{A}_j \in \mathbb{F}_q^{st \times th}$
Packets On Receiver $R_j$	$y_{j_1}, \dots, y_{j_s} \in \mathbb{F}_{q^t}$ $\underline{y} \in \mathbb{F}_{q^t}^s$	$\underline{y}_{j_1}, \dots, \underline{y}_{j_s} \in \mathbb{F}_q^t$ $\underline{y} \in \mathbb{F}_q^{st}$

*Claim 4.1.* 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 [?].

## 4.2 Comparison between scalar and vector coding by the gap size

In this study, we use vector messages in the extension field  $\mathbb{F}_q^t$ , which results in equivalent solutions for scalar linear and vector network coding with respect to alphabet size. We introduce a *gap* between the optimal scalar linear solution and our vector solution. The

---

**Algorithm 1** Calculate the gap

---

1. Find the lower bound of  $r_{max,vector}$ , which indicates a solvable vector network coding of field size  $q$  and dimension  $t$  ( $q_v = q^t$ ).
  2. Find the upper bound of  $r_{max,scalar}$ , which indicates a optimal scalar linear network coding in  $\mathbb{F}_{q_s}$ .
  3. Because the vector solution in  $\mathbb{F}_q^t$  is equivalent to the optimal scalar solution, we assign  $r_{max,scalar} = r_{max,vector}$  to find  $q_s$ .
  4. An achieved gap is calculated by  $g = q_s - q_v$
- 

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. To calculate this gap, we conduct the following steps:

Throughout this study, we show that vectors solutions significantly reduce the required alphabet size by this gap.

## 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  $(\epsilon = 1, l = 1) - \mathcal{N}_{h=3, r, s=4}$  network. Then we generalize the proof to the  $(\epsilon = 1, l = 1) - \mathcal{N}_{h, r, s}$  network.

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

What is the achieved gap?

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

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

with  $\underline{x}_i, \underline{y}_{j_v} \in \mathbb{F}_q^t$ ,  $\mathbf{A}_{j_v} \in \mathbb{F}_q^{t \times 3t}$  for  $v = 1, \dots, 4$ , and  $\mathbf{A}_{j_1}, \dots, \mathbf{A}_{j_3}$  must be distinct.

The network is solvable, if  $\mathbf{A}_j$  has full-rank for every  $j = 1, \dots, N$ , i.e.  $\mathbf{A}_{j_v}$  must satisfy:

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

In order to satisfy  $rk[\mathbf{A}_j] \geq 3t$ , we can easily choose suitable values for the coefficient  $\mathbf{A}_j^{(4)}$  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:

$$rk \begin{bmatrix} \mathbf{A}_{j_1} \\ \mathbf{A}_{j_2} \\ \mathbf{A}_{j_3} \end{bmatrix} \geq 2t \tag{5.1}$$

Therefore,  $rk \begin{bmatrix} \mathbf{A}_{j_1} \\ \mathbf{A}_{j_2} \\ \mathbf{A}_{j_3} \end{bmatrix} \geq 2t$  implies  $rk[\mathbf{A}_j] \geq 3t$ , or to satisfy  $rk[\mathbf{A}_j] \geq 3t$ , we need

$rk \begin{bmatrix} \mathbf{A}_{j_1} \\ \mathbf{A}_{j_2} \\ \mathbf{A}_{j_3} \end{bmatrix} \geq 2t$ . In Section XYZ, we have  $N = \binom{r}{\alpha}$  and  $\alpha = 3$  as a fixed values.

Therefore, maximizing the number of receivers is equivalent to maximize  $r$  under the constraint  $rk[\mathbf{A}_j] \geq 3t$ .  $\mathbf{A}_{j_1}, \mathbf{A}_{j_2}, \mathbf{A}_{j_3}$  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].

**Theorem 5.1** (Symmetric Lovász local lemma (LLL)). *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:*

$$Pr \left[ \bigcap_{i=1}^n \bar{\mathcal{E}}_i \right] > 0$$

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

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

Because the requirement on rank is opposite, we consider the complement event  $T$ :

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

By the intersection rule, we have:

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

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



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

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

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

Regarding to the left-hand side:

$$\begin{aligned}
 \Pr \left[ rk \begin{bmatrix} \mathbf{A}_{i_1} \\ \mathbf{A}_{i_2} \\ \mathbf{A}_{i_3} \end{bmatrix} < 2t \right] &= \sum_{i=0}^{2t-1} \Pr \left[ rk \begin{bmatrix} \mathbf{A}_{i_1} \\ \mathbf{A}_{i_2} \\ \mathbf{A}_{i_3} \end{bmatrix} = i \right] \\
 &\stackrel{1}{=} \sum_{i=0}^{2t-1} \frac{N_{t,m,n}}{q^{m \cdot n}} \\
 &= \sum_{i=0}^{2t-1} \frac{\prod_{j=0}^{i-1} \frac{(q^m - q^j)(q^n - q^j)}{q^i - q^j}}{q^{m \cdot n}} \\
 &\stackrel{2}{=} \sum_{i=0}^{2t-1} \frac{\prod_{j=0}^{i-1} \frac{(q^{3t} - q^j)^2}{q^i - q^j}}{q^{9t^2}} \square
 \end{aligned} \tag{5.2}$$

By varying  $t$  in Equation (5.2), we have the following table:

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

At this point, we continue to proceed the other constraint of LLL:  $4dp \leq 1$ . Regarding to  $d$ , we have:

Table 5.1:  $r_{max}$  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

$$\begin{aligned}
 d(r) &\leq 3 \cdot \binom{r-1}{2} = 3 \cdot \frac{(r-1)(r-2)}{2} = \frac{3}{2} (r^2 - 3r + 2) = d_1(r) \\
 &\leq \frac{3}{2} r^2 = d_2(r)
 \end{aligned}$$

Hence, we have below implications:

$$\begin{aligned}
 4 \cdot p \cdot d_2(r) &\leq 1 \\
 \stackrel{1}{\Rightarrow} 4 \cdot p \cdot d_1(r) &\leq 1 \\
 \stackrel{2}{\Rightarrow} 4 \cdot p \cdot d(r) &\leq 1
 \end{aligned}$$

1:  $d_1(r) \leq d_2(r)$

2:  $d(r) \leq d_1(r)$

In consideration of  $d_2(r)$ :

$$4 \cdot p \cdot d_2(r) \leq 1 \Rightarrow 4 \cdot p \cdot \frac{3}{2} r^2 \leq 1 \Rightarrow r \leq \sqrt{\frac{1}{6p}} = r_{max}$$

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.,  $r_{max}$  asymptotes to a value higher than  $r_{scalar}$ . Now, we begin to maximize  $p$ . We consider the nominator of Equation (5.2):

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

Due to  $i$ -times product and large  $t$ :

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

Then we have:

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

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

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

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

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

Hence, by using the exact bound  $\Theta$ , we have:

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

$$\Rightarrow \frac{1 + \sum_{i=1}^{2t-1} p^{(i)}(q)}{q^{9t^2}} \approx \frac{\sum_{i=1}^{2t-1} p^{(i)}(q)}{q^{9t^2}} \in \Theta \left( q^{-t^2-2t-1} \right)$$

Finally, we have:

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

Further we have:  $r_{max,scalar} \in \mathcal{O}(q_s^2)$  [EW18]

Following to (1), we have the gap size:

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

## 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 (3.1), we are interested in the following range:  $l + \epsilon + 1 \leq h \leq \alpha l + \epsilon$ .

As previous,  $\mathbf{A}_{j_1}, \dots, \mathbf{A}_{j_\alpha} \in \mathbb{F}_q^{t \times ht}$  and we need to satisfy the following:

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

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  $\alpha$  subspaces of the set span a subspace of dimension at least  $(h-1)t$ .

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

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

Regarding to the left-hand side:

$$\begin{aligned}
 Pr[rk[\mathbf{A}] < (h-1)t] &= \sum_{i=0}^{(h-1)t-1} Pr[rk[\mathbf{A}] = i] \\
 &\stackrel{1}{=} \sum_{i=0}^{(h-1)t-1} \frac{N_{i,\alpha t, ht}}{q^{(\alpha t)(ht)}} \\
 &= \frac{1}{q^{(\alpha h)t^2}} \cdot \sum_{i=0}^{(h-1)t-1} \prod_{j=0}^{i-1} \frac{(q^{\alpha t} - q^j)(q^{ht} - q^j)}{q^i - q^j} \quad (5.3)
 \end{aligned}$$

Firstly, we consider 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:

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

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  $\alpha l + \epsilon = \alpha + 1 \geq h$ . This cannot happen because of  $t \geq 2$ , i.e. this maximum point is over then upper-range limit.

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

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

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

Thirdly, we consider the 3rd requirement of LLL to figure out a lower bound on  $r_{max}$ :

$$d \leq \alpha \binom{r-1}{\alpha-1} = \alpha \frac{(r-1) \dots (r-\alpha+1)}{(\alpha-1)!} \leq \frac{\alpha}{(\alpha-1)!} r^{\alpha-1} = d_2$$

We need  $4dp \leq 1$ , which is satisfied if  $4d_2p \leq 1$ . 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:

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

### 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  $\alpha$  links from the middle layer carry  $\alpha$  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  $\alpha$  links must be distinct  $\Rightarrow r \leq \begin{bmatrix} \alpha \\ 1 \end{bmatrix}_{q_s}$

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

Hence,

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

### 5.2.3 Calculate the gap of size

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

## 6 Computational Results





## 7 Conclusion



## 8 Appendix



# Bibliography

- [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.
- [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.