Number of Optimal Index Codes and Their Performance Over Fading Channels and With Restricted Information Sets.

A Project Report

submitted in partial fulfillment of the

requirements for the degree of

Master of Engineering

in

Telecommunication

submitted by

Kavitha. R

SR No.: 04-02-03-10-41-13-1-10145

Under the guidance of

Prof. B. Sundar Rajan

Department of Electrical Communication Engineering

Indian Institute of Science

Bangalore - 560 012

Jun. 2015

Acknowledgements

I wish to extend my sincere thanks to my guide, Prof. B. Sundar Rajan without whose support and guidance, this work would not have been possible. He is one of the best teachers I have known in my life. He has always been encouraging and provided a lot of freedom in the work.

I would take the opportunity to thank all the teachers of the department for their support and effort in teaching the concepts in Electrical Communication Engineering.

I offer my special thanks to Mr. Anoop Thomas for clearing all my doubts through suggestions and discussions.

And last but not the least; I would like to thank my family without whom everything would have been impossible.

Abstract

An index coding scheme in which the source (transmitter) transmits binary symbols over a wireless fading channel is considered. Index codes with the transmitter using minimum number of transmissions are known as optimal index codes. Different optimal index codes give different performances in terms of probability of error in a fading environment and this also varies from receiver to receiver. The thesis consists of three parts.

In the first part, the goal is to identify optimal index codes which minimizes the maximum probability of error among all the receivers. A criterion for optimal index codes that minimizes the maximum probability of error among all the receivers is identified. For a special class of index coding problems, an algorithm to identify optimal index codes which minimize the maximum error probability is given. Techniques and claims with simulation results are illustrated leading to conclude that a careful choice among the optimal index codes will give a considerable gain in fading channels.

In the second part of the thesis, an algebraic formulation of index codes is given from which a lower bound on the total number of index codes possible is found. A criterion to find optimal index codes with minimum-maximum error probability is found for the special case of single unicast index coding problems.

In a general index coding problem, there is a single sender with multiple messages and multiple receivers wanting a set of messages and knowing a different set of messages. The last part of the thesis considers the case where in-spite of this requirement, each receiver also has a restricted message set assigned to it, out of which it is not supposed to receive any. We find the possible rates for some special cases of index coding with restricted information by following an interference alignment approach.

Contents

Acknowledgements **i**

Abstract **ii**

1 Introduction and Background **1**

1.1 Optimal index codes with min-max error probability 2

1.2 The number of optimal index codes 2

1.3 Index coding with restricted information 3

1.4 Organisation of The Report 3

2 Optimal Index Coding with Min-Max Probability of Error over Fading Channels **5**

2.1 A Criterion for Minimum Maximum Probability of Error 7

2.2 Bandwidth optimal index code which minimizes the maximum probability of error . 8

2.3 Simulation Results 18

2.4 Results and Discussion 29

3 On the number of optimal index codes **33**

3.1 Problem Formulation 35

3.2 Method to Identify the Optimal Length for a Linear solution 40

3.3 Minimum Number of Codes Possible for an Optimal N 47

3.4 Optimal Codes with Minimum-Maximum Error Probability 52

3.5 Results and Discussion 56

4 Index Coding with Restricted Information **59**

4.1 Achievability of rate $\frac{1}{L+1}$ 60

4.2 Capacity of Special Classes of Index Coding Problem with Restricted Information . 64

4.3 Some special settings with $N_i = \phi, \forall i \in \lceil m \rfloor$ 67

4.4 Results and Discussions 73

5 Conclusion **74**

5.1 Summary of Results 74

5.2 Scope for future work 75

Bibliography **76**

Publications **78**

List of Figures

2.1 Information flow graph G of Example 2. 13

2.2 Information flow graph G of Example 3. 14

2.3 Information flow graph G and Spanning tree T of Example 4. 14

2.4 Information flow graph G and Spanning tree T of Example 4. 16

2.5 Information flow graph G and Spanning tree T of Example 6. 17

2.6 SNR Vs BEP for code $\mathfrak{C}_1$ for Rayleigh fading scenario, at all receivers of Example 7. 19

2.7 SNR Vs BEP for code $\mathfrak{C}_2$ for Rayleigh fading scenario, at all receivers of Example 7. 20

2.8 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_7 of Example 7. 20

2.9 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_1 of Example 7. 21

2.10 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_2 of Example 7. 21

2.11 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_3 of Example 7. 21

2.12 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_4 of Example 7. 21

2.13 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_5 of Example 7. 21

2.14 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_6 of Example 7. 21

2.15 SNR Vs BEP for code $\mathfrak{C}_1$ for Rician fading scenario, at all receivers of Example 7. 22

2.16 SNR Vs BEP for code $\mathfrak{C}_2$ for Rician fading scenario, at all receivers of Example 7. 23

2.17 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_7 of Example 7. 23

2.18 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_1 of Example 7. 24

2.19 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_2 of Example 7. 24

2.20 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_3 of Example 7. 24

2.21 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_4 of Example 7. 24

2.22 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_5 of Example 7. 24

2.23 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_6 of Example 7. 24

2.24 SNR Vs BEP for code $\mathfrak{C}_1$ for Rayleigh fading scenario, at all receivers of Example 8. 26

2.25 SNR Vs BEP for code $\mathfrak{C}_2$ for Rayleigh fading scenario, at all receivers of Example 8. 26

2.26 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_3 of Example 8. 27

2.27 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_1 of Example 8. 27

2.28 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_2 of Example 8. 27

2.29 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_4 of Example 8. 27

2.30 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_5 of Example 8. 27

2.31 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_6 of Example 8. 28

2.32 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_7 of Example 8. 28

2.33 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_8 of Example 8. 28

2.34 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_9 of Example 8. 28

2.35 SNR Vs BEP for code $\mathfrak{C}_1$ for Rician fading scenario, at all receivers of Example 8. 29

2.36 SNR Vs BEP for code $\mathfrak{C}_2$ for Rician fading scenario, at all receivers of Example 8. 30

2.37 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_3 of Example 8. 30

2.38 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_1 of Example 8. 31

2.39 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_2 of Example 8. 31

2.40 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_4 of Example 8. 31

2.41 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_5 of Example 8. 31

2.42 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_6 of Example 8. 31

2.43 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_7 of Example 8. 31

2.44 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_8 of Example 8. 32

2.45 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_9 of Example 8. 32

3.1 Representation of a unicast IC problem by an equivalent network code. 34

3.2 Equivalent network code corresponding to the IC problem in Example 9 39

3.3 BER versus SNR (db) curve for $\mathfrak{C}_1$ at all the receivers for Example 9. 54

3.4 BER versus SNR (db) curve for $\mathfrak{C}_2$ at all the receivers for Example 9. 55

3.5 BER versus SNR (db) curve for $\mathfrak{C}_3$ at all the receivers for Example 9. 55

3.6 Worst case BER versus SNR (db) curves for each of the three codes for Example 9. 56

3.7 BER versus SNR (db) curve for $\mathfrak{C}_{30}$ at all the receivers for Example 11 57

3.8 BER versus SNR (db) curve for $\mathfrak{C}_{29}$ at all the receivers for Example 11 57

3.9 Worst case BER versus SNR (db) curves for codes $\mathfrak{C}_{30}$ and $\mathfrak{C}_{29}$ for Example 11 58

List of Tables

2.1 Matrices describing codes $\mathfrak{C}_1$,$\mathfrak{C}_2$,$\mathfrak{C}_3$ and $\mathfrak{C}_4$ of Example 1 9

2.2 Number of transmissions used at receivers to decode its demands for codes $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$ and $\mathfrak{C}_4$. 9

2.3 Comparison of optimal length linear codes for Example 2. Each row in the table gives code and the corresponding number of transmissions the receiver uses in decoding its demanded messages. 13

2.4 Comparison of optimal length linear codes for Example 3. Each row in the table gives code and the corresponding number of transmissions the receiver uses in decoding its demanded messages. 15

2.5 Decoding procedure for Example 4. 16

2.6 Decoding procedure for Example 5. 17

2.7 Decoding procedure for Example 5. 18

3.1 Fitting matrices for Example 11 49

3.2 Optimal linear solutions for Example 11. 50

3.3 Fitting matrices for Example 12 51

3.4 All possible optimal linear solutions for Example 12. 52

Chapter 1

Introduction and Background

The problem of index coding with side information was introduced by Birk and Kol [1] in which a central server (source/transmitter) has to transmit a set of data blocks to a set of caching clients (receivers). The clients may receive only a part of the data which the central server transmits. The receivers inform the server about the data blocks which they possess through a backward channel. The server has to make use of this additional information and find a way to satisfy each client using minimum number of transmissions. This problem of finding a code which uses minimum number of transmissions is the index coding problem.

Bar-Yossef *et al.* [2] studied a type of index coding problem in which each receiver demands only one single message and the number of receivers equals number of messages. A side information graph was used to characterize the side information possessed by the receivers. It was found that the length of the optimal linear index code is equal to the minrank of the side information graph of the index coding problem. Also few classes of index coding problems in which linear index codes are optimal were identified. However Lubetzky and Stav [13] showed that, in general, non-linear index codes are better than linear codes.

Ong and Ho [4] classify the index coding problem depending on the demands and the side information possessed by the receivers. An index coding problem is unicast if the demand sets of the receivers are disjoint. It is referred to as single unicast if it is unicast and the size of each of the demand set is one. If the side information possessed by the receivers are disjoint then the problem is referred to as uniprior index coding problem. A uniprior index coding problem in which the size of the side information is one at all receivers is referred to as single uniprior problem. All other types of index coding problems are referred to as multicast/multiprior problems. It is proved that for single uniprior index coding problems, linear index codes are sufficient to get optimality in terms of minimum number of transmissions.

The work reported in this thesis focuses on 1) Optimal index codes with min-max error probability 2) The number of optimal index codes 3) Index coding with restricted information

1.1 Optimal index codes with min-max error probability

[1]First we consider the scenario in which the binary symbols are transmitted in a fading channel and hence are subject to channel errors. We assume a fading channel between the source and the receivers along with additive white Gaussian noise (AWGN) at the receivers. Each of the transmitted symbol goes through a Rayleigh fading channel. This is the first work that considers the performance of index coding in a fading environment. The following decoding procedure is used. A receiver decodes each of the transmitted symbol first and then uses these decoded symbols to obtain the message demanded by the receiver. Simulation curves showing Bit Error Probability (BEP) as a function of SNR are provided. One can observe that the BEP performance at each receiver depends on the optimal index code used. A condition which minimizes the maximum probability of error among all the receivers is derived. For a special class of index coding problems, an algorithm to identify an optimal index code which gives the best performance in terms of minimal maximum error probability across all the receivers is given.

1.2 The number of optimal index codes

Towards identifying the best optimal length index code one needs to know the number of optimal length index codes. In this work, we present results on the number of optimal length index codes making use of the representation of an index coding problem by an equivalent network code. We give the minimum number of codes possible with the optimal length. This is done using a simpler algebraic formulation of the problem compared to the approach of Koetter and Medard [6].

[1]The content of this chapter is a joint work with Anoop Thomas and A. Chandramouli.

1.3 Index coding with restricted information

In a general index coding problem, there is a single sender with multiple messages and multiple receivers wanting a set of messages and knowing a different set of messages. We consider the case where in-spite of this, each receiver also have a restricted message set assigned to it,out of which it is not supposed to receive any. This is a case introduced by Dau *et. al.* in section IV.E of their work [18]. We have extended the theorems in [17] for the new scenario and find the possible rates for some special cases of index coding by following an interference alignment approach.

1.4 Organisation of The Report

The report is organized as follows.

- In Chapter 2, we begin with introduction of the system model and necessary notations. In Section 2.1 we present a criterion for an index code to minimize the maximum probability of error. In Section 2.2 we give an algorithm to identify an optimal index code which minimizes the maximum probability of error for single uniprior problems. In Section 2.3 we show the simulation results.

- In Chapter 3, through an algebraic characterization, we give a method to identify the optimal length of a linear solution for a single unicast index coding problem. This is done by finding a transfer matrix (whose elements depend on the index code we choose) which relates the input messages and the decoded messages. This is done in Section 3.2. We give the minimum number of codes possible with the optimal length for a single unicast index coding problem. This is done in Section 3.3. We find this by finding the minimum number of feasible solutions of a linear system of equations which represents our index coding problem. We give a method to find the best linear solution in terms of minimum-maximum error probability among all codes with the optimal length for a single unicast case in Section 3.4 and we give simulation results verifying our claim.

- In Chapter 4, we use interference alignment techniques to find feasible rates for an index coding problem. First, we define index coding with restricted information which was first introduced by Dau *et. al.* in their work[18]. We extend the theorems and results in [17] by considering this extra condition. This is done in Sections 4.1 and 4.2. In Section 4.3, we find the capacities of two index coding settings one of whose special case is addressed in [17].

Chapter 2

Optimal Index Coding with Min-Max Probability of Error over Fading Channels

In [1] index coding problems, there is a unique source S having a set of n messages $X = \{x_1, x_2, \ldots, x_n\}$ and a set of m receivers $\mathcal{R} = \{R_1, R_2, \ldots, R_m\}$. Each message $x_i \in X$ belongs to the finite field $\mathbb{F}_2$. Each $R_i \in \mathcal{R}$ is specified by the tuple $(\mathcal{W}_i, \mathcal{K}_i)$, where $\mathcal{W}_i \subseteq X$ are the messages demanded by R_i and $\mathcal{K}_i \subseteq X \setminus \mathcal{W}_i$ is the information known at the receiver. An index coding problem is completely specified by $(X, \mathcal{R})$ and the index coding problem is referred as $\mathcal{I}(X, \mathcal{R})$.

The set $\{1, 2, \ldots, n\}$ is denoted by $\lceil n \rfloor$. An index code for an index coding problem is defined as:

Definition 1. An *index code* over $\mathbb{F}_2$ for an instance of the index coding problem $\mathcal{I}(X, \mathcal{R})$, is an encoding function $\mathfrak{C} : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^N$ such that for each receiver R_i, $i \in \lceil m \rfloor$, there exists a decoding function $\mathfrak{D}_i : \mathbb{F}_2^N \times \mathbb{F}_2^{|\mathcal{K}_i|} \rightarrow \mathbb{F}_2^{\mathcal{W}_i}$ satisfying $\mathfrak{D}_i(\mathfrak{C}(X), \mathcal{K}_i) = \mathcal{W}_i, \forall\, X \in \mathbb{F}_2^n$.The parameter N is called the *length* of the index code.

An index code is said to be *linear* if the encoding function $\mathfrak{C}$ is linear over $\mathbb{F}_2$. A linear index code can be described as $\mathfrak{C}(x) = xL, \forall\, x \in \mathbb{F}_2^n$ where L is an $n \times N$ matrix over $\mathbb{F}_q$. The matrix

[1]The content of this chapter is a joint work with Anoop Thomas and A. Chandramouli. Also communicated to *IEEE Trans. on Vehicular Technology* and a shorter version to appear in *Proc. PIMRC'2015*, Hong Kong, Aug., 2015.

L is called the matrix corresponding to the linear index code $\mathfrak{C}$. The code $\mathfrak{C}$ is referred to as the linear index code based on L.

Consider an index coding problem $\mathcal{I}(X, \mathcal{R})$ with index code $\mathfrak{C}$, such that $\mathfrak{C}(X) = \{c_1, c_2, \ldots, c_N\}$. The source has to transmit the index code over a fading channel. Let $\mathcal{S}$ denote the constellation used by the source. Let $\nu : \mathbb{F}_2 \rightarrow \mathcal{S}$ denote the mapping of bits to the channel symbol used at the source. Let $\nu(\mathfrak{C}(X)) = s_X$, denote the sequence of channel symbols transmitted by the source. Assuming quasi-static fading, the received symbol sequence at receiver R_j corresponding to the transmission of s_X is given by $y_j = h_j s_X + n_j$ where h_j is the fading coefficient associated with the link from source to receiver R_j. The additive noise n_j is assumed to be a sequence of noise samples distributed as $\mathcal{CN}(0, 1)$, which denotes circularly symmetric complex Gaussian random variable with variance one. Coherent detection is assumed at the receivers. In the model considered, the receiver decodes $\mathfrak{C}(X)$ and then tries to find the demanded message $x_i \in \mathcal{W}_i$ using the decoded index code. In this report it is shown that different optimal index codes give rise to different performance in terms of probability of error.

We recall few of the relevant standard definitions in graph theory. A *graph* is a pair $G = (V, E)$ of sets where the elements of V are the vertices of graph and the elements of E are its edges. The vertex set of a graph is referred to as $V(G)$, its edge set as $E(G)$. Two vertices v_1, v_2 of G are *adjacent* if v_1v_2 is an edge of G. An *arc* is a directed edge. For an arc v_1v_2, vertex v_1 is the tail of the arc and vertex v_2 is the head of the arc. If all the vertices of G are pairwise adjacent then G is *complete*. Consider a graph $G' = (V', E')$. If $V' \subseteq V$ and $E' \subseteq E$, then G' is a *subgraph* of G written as $G' \subseteq G$. A subgraph G' is a *spanning subgraph* if $V' = V$. A *path* is a non-empty graph $P = (V, E)$ of the form $V = \{v_0, v_1, \ldots, v_k\}$, $E = \{v_0v_1, v_1v_2, \ldots, v_{k-1}v_k\}$ where the v_i are all distinct. If $P = v_0v_1 \ldots v_{k-1}$ is a path and $k \geq 3$, then a cycle is a path with an additional edge $v_{k-1}v_0$. A graph is *acyclic* if it does not contain any cycle. The number of edges of a path is its *length*. The *distance* $d_G(x, y)$ in G of two vertices x, y is the length of a shortest x-y path in G. The greatest distance between any two vertices in G is the *diameter* of G. A graph G is called *connected* if any two of its vertices are linked by a path in G. A *tree* is a connected acyclic graph. A *spanning tree* is a tree which spans the graph. For two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, $G_1 \cup G_2 := (V_1 \cup V_2, E_1 \cup E_2)$, $G_1 \cap G_2 := (V_1 \cap V_2, E_1 \cap E_2)$ and $G_1 \backslash G_2 := (V_1 \backslash V_2, E_1 \backslash E_2)$.

2.1 A Criterion for Minimum Maximum Probability of Error

In this section we identify a condition that is required to minimize the maximum probability of error for decoding a message across all the receivers. Since the transmissions are over a fading channel each transmitted symbol has a probability of error. Let the probability of error of each transmitted symbol (denoted by t_x) be p. Let us consider an index code $\mathfrak{C}$ of length N for an index coding problem $\mathcal{I}(X, \mathcal{R})$. Consider a receiver $R_i \in \mathcal{R}$, which uses c of the N transmissions to recover a message $x_i \in \mathcal{W}_i$. We try to find the probability of error in decoding the message x_i. Let the decoded message be $\widehat{x_i}$. The probability of error in decoding the message x_i is

$$\begin{aligned} Pr(\widehat{x_i} \neq x_i) &= Pr(1\ t_x \text{ in error } \cup 3\ t_x \text{ in error } \cup \ldots c\ t_x \text{ in error })\\ &= \sum_{i \text{ odd}, i \leq c} Pr(i\ t_x \text{ in error }) = \sum_{i \text{ odd}, i \leq c} \begin{pmatrix} c \\ i \end{pmatrix} p^i (1-p)^{c-i}. \end{aligned} \tag{2.1}$$

We show that the probability of error in decoding a message decreases if receiver uses less number of transmissions to decode that message.

Lemma 1. The probability of error in decoding a message at a particular receiver decreases with a decrease in the number of transmissions used to decode the message.

Proof. This lemma can be proved by showing that the upper bound in (2.1) is an increasing function on c which is the number of transmissions used to decode the message. We have

$$\sum_{i \text{ odd}, i \leq c} \begin{pmatrix} c \\ i \end{pmatrix} p^i (1-p)^{c-i} = \frac{(p + (1-p))^c - ((1-p) - p)^c}{2} = \frac{1 - (1-2p)^c}{2}.$$

Consider,

$$\frac{1-(1-2p)^{c+1}}{2} - \frac{1-(1-2p)^c}{2} = \frac{(1-2p)^c(1-(1-2p))}{2} = (1-2p)^c p.$$

As c increases the difference remains positive as long as $p < 0.5$. As probability of transmitted symbol to be in error is less than 0.5, the lemma is proved. □

We have considered only decoding of one message at a particular receiver. However a receiver may have multiple demands. Also there are many receivers to be considered. So we try to bound the maximum error probability. To achieve this we try to identify those optimal index codes which will reduce the maximum number of transmissions used by any receiver to decode any of its demanded message. Such optimal index codes perform better than other optimal index codes of the same number of transmissions. Such index codes are not only bandwidth optimal (since the minimum number of transmissions are used) but are also optimal in the sense of minimum maximum probability of error.

2.2 Bandwidth optimal index code which minimizes the maximum probability of error

In Section 2.1, we derived a condition for minimizing the maximum probability of error. The index code should be such that the maximum number of transmissions used by any receiver to decode any of its demands should be as less as possible. In this section, we identify such index codes for single uniprior index coding problems. Recall that in a single uniprior problem each receiver R_i demands a set of messages W_i and knows only one message x_i. There are several linear solutions which are optimal in terms of least bandwidth for this problem but among them we try to identify the index code which minimizes the maximum number of transmissions that is required by any receiver in decoding its desired messages. We motivate our problem with the following example.

Example 1. Consider a single uniprior index coding problem $\mathcal{I}(X, \mathcal{R})$ with $X = \{x_1, x_2, \ldots, x_9\}$ and $\mathcal{R} = \{R_1, R_2, \ldots, R_9\}$. Each receiver $R_i \in \mathcal{R}$, knows x_i and demands x_{i+2} where $+$ denotes modulo 9 addition. In addition to the above demands, receiver R_1 and R_2 also demands x_2 and x_3 respectively. The length of the optimal linear code for this problem is eight. In this example we consider four optimal linear codes and shows that the number of transmissions used in decoding the demands at receivers depends on the code.

Consider codes $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$ and $\mathfrak{C}_4$ represented by the matrices L_1, L_2, L_3 and L_4 respectively. The matrices representing the codes are given in Table 2.1. The number of transmissions required by each receiver in decoding its demand for each of the codes is given in Table 2.2. Since receivers R_1 and R_2 have two demands, two entries are given in its column each corresponding to one of its demands. The maximum number of transmissions used by each of the receivers is highlighted. From the table we can observe that the maximum number of transmissions required by a receiver

$$L_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad L_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

$$L_3 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad L_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Table 2.1 Matrices describing codes $\mathfrak{C}_1$,$\mathfrak{C}_2$,$\mathfrak{C}_3$ and $\mathfrak{C}_4$ of Example 1

Codes	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9
$\mathfrak{C}_1$	$1, 1$	$\underline{2}, \underline{2}$	$\underline{2}$	$\underline{2}$	$\underline{2}$	$\underline{2}$	$\underline{2}$	1	$\underline{2}$
$\mathfrak{C}_2$	$2, 1$	$1, \underline{4}$	$\underline{4}$	1	1	2	1	1	1
$\mathfrak{C}_3$	$1, 1$	$2, 1$	1	1	1	1	1	1	$\underline{4}$
$\mathfrak{C}_4$	$4, \underline{5}$	$1, 1$	1	1	1	1	1	1	4

Table 2.2 Number of transmissions used at receivers to decode its demands for codes $\mathfrak{C}_1, \mathfrak{C}_2, \mathfrak{C}_3$ and $\mathfrak{C}_4$.

in decoding its demands is four for codes $\mathfrak{C}_2$ and $\mathfrak{C}_3$. For code $\mathfrak{C}_4$, the maximum number of transmissions used to decode the message is five. However for code $\mathfrak{C}_1$, the maximum number is two. Among the four codes considered, code $\mathfrak{C}_1$ gives minimum maximum error probability across the receivers. In this section we give an algorithm to identify such codes which gives minimum maximum error probability across receivers.

The single uniprior problem can be represented by information flow graph G of m vertices each representing a receiver, with directed edge from vertex i to vertex j if and only if node j wants x_i. Note that in a single uniprior problem the number of receivers is equal to the number of messages. This is because each receiver knows only one message and the message known to each receiver is different. So $n > m$ implies that there are some messages which does not form part of side information of any of the receivers. Such messages have to be transmitted directly and we can reduce that to an index coding problem where $n = m$. Ong and Ho have proved that all single uniprior problems have bandwidth optimal linear solutions. The Algorithm 1 (Pruning algorithm), which takes information flow graph as input was proposed. The output of Algorithm 1 is G' which is a set of non-trivial strongly connected components each represented by $G'_{sub,i}$ and a collection of arcs. The benefit is that a coding scheme satisfying G' will satisfy the original index coding problem G as well. We propose Algorithm 2 for the single uniprior problem which finds the bandwidth optimal index code that minimizes the maximum probability of error.

Algorithm 1 The Pruning Algorithm

Initialization: $G' = (V', E') \leftarrow G = (V, A)$
1)Iteration

while there exists a vertex $i \in V'$ with

- **(i)** more than one outgoing arc, and
- **(ii)** an outgoing arc that does not belong to any cycle [denote any such arc by (i,j)]

do

remove from G', all outgoing arcs of vertex i except for the arc (i, j);

end

2) label each non-trivial strongly connected component in G' as $G'_{sub,i}$, $i \in \{1, 2, \ldots, N_{sub}\}$;

Algorithm 2

1. Perform the pruning algorithm on the information flow graph of the single uniprior problem and obtain the sets G' and $G'_{sub,i}, i \in \{1, 2, \ldots, N_{sub}\}$.
2. For each $G'_{sub,i}$ perform the following:
   - Form a complete graph on vertices of $G'_{sub,i}$.
   - Identify the spanning tree T, which has the minimum maximum distance between (i, j) for all $(i, j) \in E(G'_{sub,i})$.
   - For each edge (i, j) of T, transmit $x_i \oplus x_j$.
3. For each edge (i, j) of $G' \backslash G'_{sub}$, transmit x_i.

The first step of Algorithm 2 is the pruning algorithm which gives G' and its connected components $G'_{sub,i}$. The number of such connected components in G' is N_{sub}. Algorithm 2 operates on each of the connected components $G'_{sub,i}$. A complete graph is formed on the vertices of $G'_{sub,i}$. Recall that in a complete graph all the vertices are pairwise adjacent. Consider a spanning tree T_i of the complete graph on vertices of $G'_{sub,i}$. Consider an edge $(i,j) \in E(G'_{sub,i})$. An edge $(i,j) \in E(G'_{sub,i})$ indicates that vertex j demands the message x_i. In the spanning tree T_i, there will be a unique path between the vertices i and j. Algorithm 2 computes the distance of that unique path. This is done for all edges $(i,j) \in E(G'_{sub,i})$ and the maximum distance is observed. This is repeated for different spanning tress and among the spanning tress the one which has the minimum maximum distance is identified by the algorithm. Let T be the spanning tree identified by the algorithm. From T we obtain the index code as follows. For each edge (i,j) of T, transmit $x_i \oplus x_j$. There will be few demands which correspond to arcs in $G' \setminus G'sub$ where G'_{sub} is the union of all connected components $G'_{sub,i}$. For each arc $(i,j) \in G' \setminus G'_{sub}, x_i$ is transmitted.

Theorem 1. For every single uniprior index coding problem, the Algorithm 2 gives the bandwidth optimal index code which minimizes the maximum probability of error. Moreover the number of transmissions used by any receiver in decoding any of its message is at most two for the index code obtained from Algorithm 2.

Proof. First we prove that Algorithm 2 gives a valid index code. Symbols transmitted in third step of algorithm are messages itself and any receiver demanding those messages gets satisfied. All receiver nodes in T are able to decode the message of every other vertex in T in the following way. Consider two vertices i and j with vertex j demanding x_i. Since T is a spanning tree there exists a unique path between any pair of its vertices. Consider that unique path $P = (i, k_1, k_2, \dots, j)$ between i and j. Receiver j can obtain $x_i \oplus x_j$ by performing XOR operation on all the transmitted symbols corresponding to the edges in the path P. Now we prove the optimality in bandwidth. The number of edges of every spanning tree is $V(G'_{sub,i}) - 1$. For each $G'_{sub,i}$ we transmit $V(G'_{sub,i}) - 1$ symbols. The total number of transmissions for our index code is equal to $\sum_{i=1}^{N_{sub}} (V(G'_{sub,i}) - 1) + |E(G' \backslash G'_{sub})|$. The index code of Algorithm 2 uses the same number of transmissions as the bandwidth optimal index code [4]. Observe that for every connected graph G_{conn} representing a single uniprior problem, the source cannot achieve optimal bandwidth if it transmits any of the message directly. Let us assume that the source transmits x_i. Note that message x_i is the side information of one of the receivers say j. So to satisfy the demands of receiver j the source has to transmit its want-set directly. Thus to satisfy all the receivers, the source needs to transmit $|V(G_{conn})|$ symbols where as the optimal number of transmissions is $|V(G_{conn}) - 1|$. Hence for any connected component $G'_{sub,i}$ source cannot transmit the messages directly. Finally, observe that the number of transmissions used by the receiver to decode the desired message is equal to the distance between the vertices in the corresponding spanning tree. So the spanning tree which minimizes the maximum distance for all the demands of the index coding problem gives the index code which minimizes the maximum probability of error. There exists spanning trees for a complete graph with diameter two, so every receiver can decode any of its desired message using at most two transmissions. □

Algorithm 2 identifies an index code which minimizes the maximum number of transmissions required by any receiver to decode its demanded message. Note that the spanning tree identified in step 2 of the algorithm need not be unique. Hence there are multiple index codes which offers the same minimum maximum number of transmissions. Among these we could find those index codes which reduces the total number of transmissions used by all the receivers. This could be achieved by modifying the step 2 of Algorithm 2. Identify the set of spanning trees which has the minimum maximum distance between (i, j) for all $(i, j) \in E(G'_{sub,i})$. Among these spanning trees we can compute the total distance between all edges $(i, j) \in E(G'_{sub,i})$ and identify the spanning tree T_i which minimizes the overall sum. For each edge $(i, j) \in T_i$ transmit $x_i + x_j$. This will give the index code which minimizes the total number of transmissions used in decoding all the messages at all the receivers.

In the remainder of this section we show few examples which illustrate the use of the algorithm. The simulation results showing the improved performance at receivers is given in Section 2.3.

Example 2. In this example we consider a single uniprior index coding problem having three receivers. The index coding problem has a message set $X = \{x_1, x_2, x_3\}$ and the set of receivers $\mathcal{R} = \{R_1, R_2, R_3\}$. Receiver R_1 demands messages x_2 and x_3. Receiver R_2 demands x_1 and receiver R_3 demands x_1 and x_2. The information flow graph G for this problem is given in Figure 2.1. For this index coding problem, length of the optimal index code is two. Total number of optimal

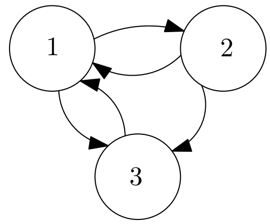


Fig. 2.1 Information flow graph G of Example 2.

Code	Encoding	R_1		R_2	R_3	
		$x_2 \in \mathcal{W}_1$	$x_3 \in \mathcal{W}_1$	$x_1 \in \mathcal{W}_2$	$x_1 \in \mathcal{W}_3$	$x_2 \in \mathcal{W}_3$
$\mathfrak{C}_1$	$x_1 + x_2, x_1 + x_3$	1	1	1	1	2
$\mathfrak{C}_2$	$x_2 + x_1, x_2 + x_3$	1	2	1	1	2
$\mathfrak{C}_3$	$x_3 + x_1, x_3 + x_2$	1	2	2	1	1

Table 2.3 Comparison of optimal length linear codes for Example 2. Each row in the table gives code and the corresponding number of transmissions the receiver uses in decoding its demanded messages.

linear index codes is three. The list of optimal index codes are as follows:

- Code $\mathfrak{C}_1$ which transmits $\{x_1 + x_2, x_1 + x_3\}$.
- Code $\mathfrak{C}_2$ which transmits $\{x_1 + x_2, x_2 + x_3\}$.
- Code $\mathfrak{C}_3$ which transmits $\{x_1 + x_3, x_2 + x_3\}$.

The number of transmissions used by each of the receivers in decoding its demanded message for the codes above is given in Table 2.3. From Table 2.3, we can infer that for all the optimal index codes, the maximum number of transmissions used by any receiver is two. So for this specific instance of index coding problem, any index code which is optimal in terms of bandwidth is optimal in terms of minimum maximum error probability.

Example 3. Consider a single uniprior index coding problem with four messages x_1, x_2, x_3, x_4 and four receivers R_1, R_2, R_3, R_4. Each receiver R_i knows x_i and wants x_{i+1} where + denotes modulo 4 addition. The information flow graph G for this problem is given in Figure. The optimal length of the index code for this index coding problem is three. We list out all possible optimal length linear index codes by an exhaustive search. Total number of optimal length linear index codes for this problem is 28. We list out all possible index codes in Table **??**. There are many index codes in which the maximum number of transmissions used by a receiver is three. However there are twelve index codes in which the maximum number of transmissions used is two. The output of Algorithm 2 belongs to the category of index codes which allows any receiver to decode its wanted message with the help of at most any two of the 3 transmissions. Observe that out of the 28 codes, 12 of

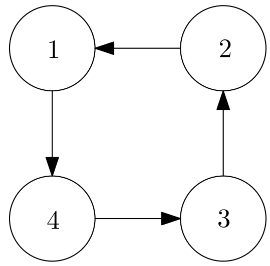
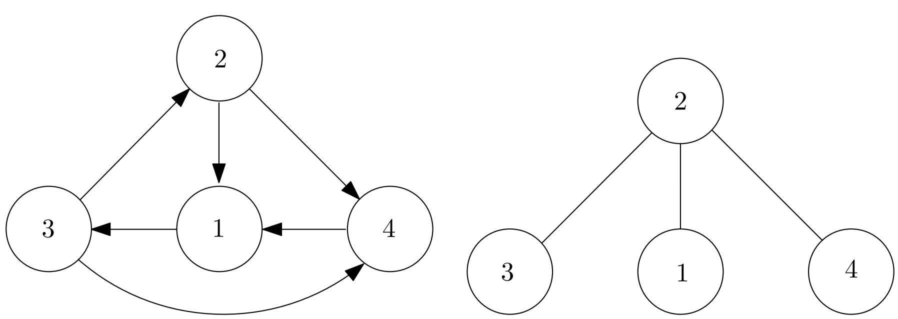


Fig. 2.2 Information flow graph G of Example 3.

them are good in terms of minimum-maximum error probability. Among the 12, there is one code which is the best in terms of minimizing the error probabilities of all the receivers as well. Our algorithm may not give that one. Algorithm 2 ensures that the code which it outputs will belong to this group of 12 codes whose worst case error probabilities are same. Note that the number of codes which perform better in terms of minimizing the maximum error probability is less than 50% of the total number of optimal length index codes. For a similar problem involving five receivers we were able to identify the total number of optimal length index codes as 840 and out of which at least 480 codes does not satisfy the minimum maximum error probability criterion. Hence we conclude that arbitrarily choosing an optimal length index code could result in using an index code which performs badly in terms of minimizing the maximum probability of error.

Example 4. Consider a single uniprior index coding problem with four messages x_1, x_2, x_3, x_4 and four receivers R_1, R_2, R_3 and R_4. Each receiver R_i knows x_i. The want-sets for the receivers are as follows: $\mathcal{W}_1 = \{x_2, x_4\}, \mathcal{W}_2 = \{x_3\}, \mathcal{W}_3 = \{x_1\}$ and $\mathcal{W}_4 = \{x_2, x_3\}$. The information flow graph G



(a) Information flow graph G (b) Spanning tree T

Fig. 2.3 Information flow graph G and Spanning tree T of Example 4.

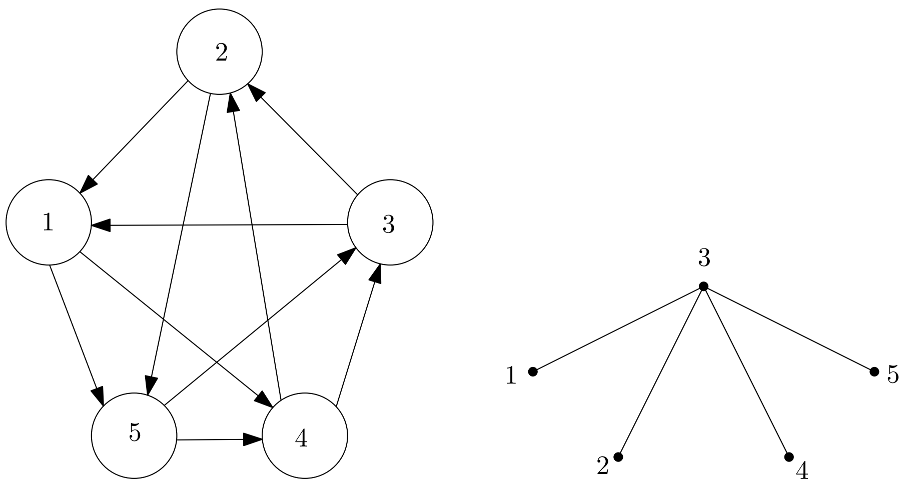
of the problem is given in Figure 2.3(a). Note that the side information flow graph is a strongly connected graph. Hence the output of the pruning algorithm is G itself. We perform Algorithm

Code	Encoding	R_1	R_2	R_3	R_4
		$\mathcal{W}_1 = \{x_2\}$	$\mathcal{W}_2 = \{x_3\}$	$\mathcal{W}_3 = \{x_4\}$	$\mathcal{W}_4 = \{x_1\}$
$\mathfrak{C}_1$	$x_1 + x_2, x_2 + x_3, x_3 + x_4$	1	1	1	3
$\mathfrak{C}_2$	$x_1 + x_2, x_2 + x_3, x_2 + x_4$	1	1	2	2
$\mathfrak{C}_3$	$x_1 + x_2, x_2 + x_3, x_1 + x_2 + x_3 + x_4$	1	1	2	2
$\mathfrak{C}_4$	$x_1 + x_2, x_2 + x_3, x_1 + x_4$	1	1	3	1
$\mathfrak{C}_5$	$x_1 + x_2, x_3 + x_4, x_1 + x_3$	1	2	1	2
$\mathfrak{C}_6$	$x_1 + x_2, x_3 + x_4, x_2 + x_4$	1	2	1	2
$\mathfrak{C}_7$	$x_1 + x_2, x_3 + x_4, x_1 + x_4$	1	3	1	1
$\mathfrak{C}_8$	$x_1 + x_2, x_1 + x_3, x_2 + x_4$	1	2	3	2
$\mathfrak{C}_9$	$x_1 + x_2, x_1 + x_3, x_1 + x_2 + x_3 + x_4$	1	2	2	3
$\mathfrak{C}_{10}$	$x_1 + x_2, x_1 + x_3, x_1 + x_4$	1	2	2	1
$\mathfrak{C}_{11}$	$x_1 + x_2, x_2 + x_4, x_1 + x_2 + x_3 + x_4$	1	3	2	2
$\mathfrak{C}_{12}$	$x_1 + x_2, x_1 + x_2 + x_3 + x_4, x_1 + x_4$	1	2	2	1
$\mathfrak{C}_{13}$	$x_2 + x_3, x_3 + x_4, x_1 + x_3$	2	1	1	2
$\mathfrak{C}_{14}$	$x_2 + x_3, x_3 + x_4, x_1 + x_2 + x_3 + x_4$	2	1	1	2
$\mathfrak{C}_{15}$	$x_2 + x_3, x_3 + x_4, x_1 + x_4$	3	1	1	1
$\mathfrak{C}_{16}$	$x_2 + x_3, x_1 + x_3, x_2 + x_4$	2	1	2	3
$\mathfrak{C}_{17}$	$x_2 + x_3, x_1 + x_3, x_1 + x_2 + x_3 + x_4$	2	1	3	2
$\mathfrak{C}_{18}$	$x_2 + x_3, x_1 + x_3, x_1 + x_4$	2	1	2	1
$\mathfrak{C}_{19}$	$x_2 + x_3, x_2 + x_4, x_1 + x_2 + x_3 + x_4$	3	1	2	2
$\mathfrak{C}_{20}$	$x_2 + x_3, x_2 + x_4, x_1 + x_4$	2	1	2	1
$\mathfrak{C}_{21}$	$x_3 + x_4, x_1 + x_3, x_2 + x_4$	3	2	1	2
$\mathfrak{C}_{22}$	$x_3 + x_4, x_1 + x_3, x_1 + x_2 + x_3 + x_4$	2	3	1	2
$\mathfrak{C}_{23}$	$x_1 + x_3, x_2 + x_4, x_1 + x_4$	2	3	2	1
$\mathfrak{C}_{24}$	$x_1 + x_3, x_1 + x_2 + x_3 + x_4, x_1 + x_4$	3	2	2	1
$\mathfrak{C}_{25}$	$x_2 + x_4, x_1 + x_2 + x_3 + x_4, x_1 + x_4$	2	2	3	1
$\mathfrak{C}_{26}$	$x_3 + x_4, x_2 + x_4, x_1 + x_2 + x_3 + x_4$	2	2	1	3
$\mathfrak{C}_{27}$	$x_3 + x_4, x_2 + x_4, x_1 + x_4$	2	2	1	1
$\mathfrak{C}_{28}$	$x_3 + x_4, x_1 + x_2 + x_3 + x_4, x_1 + x_4$	2	2	1	1

Table 2.4 Comparison of optimal length linear codes for Example 3. Each row in the table gives code and the corresponding number of transmissions the receiver uses in decoding its demanded messages.

Receivers	Demands	Decoding procedure
R_1	x_2	$x_1 \oplus c_2$
	x_4	$x_1 \oplus c_2 \oplus c_3$
R_2	x_3	$x_2 \oplus c_1$
R_3	x_1	$x_3 \oplus c_2 \oplus c_1$
R_4	x_2	$x_4 \oplus c_3$
	x_3	$x_4 \oplus c_3 \oplus c_1$

Table 2.5 Decoding procedure for Example 4.



(a) Information flow graph G_2 of Example 5

(b) Spanning tree T obtained from Algorithm 2 for Example 5.

Fig. 2.4 Information flow graph G and Spanning tree T of Example 4.

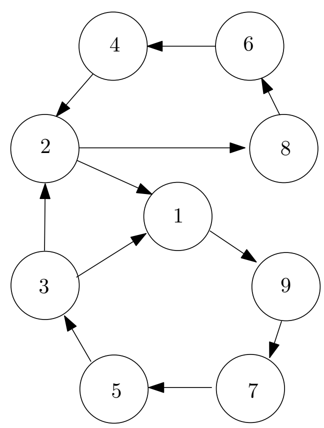
2 and the spanning tree obtained is given in Figure 2.3(b). The index code which minimizes the maximum probability of error is $\{c_1, c_2, c_3\}$ where $c_1 = x_2 \oplus x_3, c_2 = x_2 \oplus x_1$ and $c_3 = x_2 \oplus x_4$. This enables all the receivers to decode any of its demands by using at most two transmissions. At receiver R_1, x_2 can be obtained by performing $x_1 \oplus c_2$ and x_4 can be obtained by performing $x_1 \oplus c_2 \oplus c_3$. The decoding procedure used by receivers is given in Table 2.5.

Example 5. Consider a single uniprior problem with five messages x_1, x_2, x_3, x_4, x_5 and five receivers R_1, R_2, R_3, R_4, R_5. Each R_i knows x_i and wants x_{i+1} and x_{i+2} where $+$ denotes modulo 5 addition. The information flow graph G_2 is given in Figure 2.4(a). The graph is strongly connected and all the edges are parts of some cycle. We perform Algorithm 2 on G_2 and the spanning tree which minimizes the maximum distance is given in Figure 2.4(b).

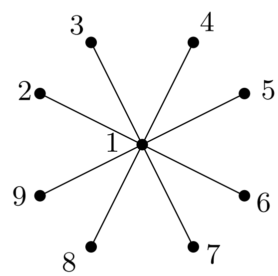
The index code which minimizes the maximum probability of error is $\{c_1, c_2, c_3, c_4\}$ where $c_1 = x_1 \oplus x_3, c_2 = x_2 \oplus x_3, c_3 = x_3 \oplus x_4$ and $c_4 = x_3 \oplus x_5$. The decoding procedure at receivers is given in Table 2.6. From the table we can observe that any receiver would take at most two

Receivers	Demands	Decoding procedure
R_1	x_2	$x_1 \oplus c_1 \oplus c_2$
	x_3	$x_1 \oplus c_1$
R_2	x_3	$x_2 \oplus c_2$
	x_4	$x_2 \oplus c_2 \oplus c_3$
R_3	x_4	$x_3 \oplus c_3$
	x_5	$x_3 \oplus c_4$
R_4	x_5	$x_4 \oplus c_3 \oplus c_4$
	x_1	$x_4 \oplus c_3 \oplus c_1$
R_5	x_1	$x_5 \oplus c_4 \oplus c_1$
	x_2	$x_5 \oplus c_4 \oplus c_2$

Table 2.6 Decoding procedure for Example 5.



(a) Information flow graph G of Example 6.



(b) Spanning tree T obtained from Algorithm 2 for Example 6.

Fig. 2.5 Information flow graph G and Spanning tree T of Example 6.

transmissions to decode any of its messages. We also observe that for any n (number of receivers), we will get a similar solution and number of transmissions required to decode any particular demanded message would be at most two.

Example 6. Consider the index coding problem of Example 1. The information flow graph G of this problem is given in Figure 2.5(a). To obtain the index code which gives minimum maximum probability of error across all receivers, we perform Algorithm 2. The spanning tree obtained from Algorithm 2 is given in Figure 2.5(b). The index code which minimizes the maximum probability of error is $\mathfrak{C}_1$ described by matrix L_1 given in Example 1. Length of the code is eight and can be represented as $\{c_1, c_2, \ldots, c_8\}$ where $c_i = x_1 \oplus x_{i+1}$. The decoding procedure at receivers for the code $\mathfrak{C}_1$ is given in Table 2.7. It is evident from the table that for code $\mathfrak{C}_1$, the maximum number of transmissions required to decode any demanded message across all receivers is two.

Receivers	Demands	Decoding procedure
R_1	x_2	$x_1 \oplus c_1$
	x_3	$x_1 \oplus c_2$
R_2	x_3	$x_2 \oplus c_1 \oplus c_2$
	x_4	$x_2 \oplus c_1 \oplus c_3$
R_3	x_5	$x_3 \oplus c_2 \oplus c_4$
R_4	x_6	$x_4 \oplus c_3 \oplus c_5$
R_5	x_7	$x_5 \oplus c_4 \oplus c_6$
R_6	x_8	$x_6 \oplus c_5 \oplus c_7$
R_7	x_9	$x_7 \oplus c_6 \oplus c_8$
R_8	x_1	$x_8 \oplus c_7$
R_9	x_2	$x_9 \oplus c_8 \oplus c_1$

Table 2.7 Decoding procedure for Example 5.

2.3 Simulation Results

In this section we give simulation results [2] which show that the choice of the optimal index codes matters. We show that optimal index codes which use lesser number of transmissions to decode the messages perform better than those using more number of transmissions. We consider the index coding problem in Example 7 below and observe an improvement in the performance by choosing index code obtained from Algorithm 2 over another arbitrary optimal index code. This shows the significance of optimal index codes which use small number of transmissions to decode the messages at the receivers.

Example 7. Consider a single uniprior index coding problem $\mathcal{I}(X, \mathcal{R})$ with $X = \{x_1, x_2, \ldots, x_7\}$ and $\mathcal{R} = \{R_1, R_2, \ldots, R_7\}$. Each receiver $R_i \in \mathcal{R}$, knows x_i and has a want-set $\mathcal{W}_i = X \setminus \{x_i\}$. We consider two index codes for the problem and show by simulation the improvement in using the index code obtained from Algorithm 2.

Let $\mathfrak{C}_1$ be the linear index code obtained from the proposed Algorithm 2. We use code $\mathfrak{C}_2$, another valid index code of optimal bandwidth for performance comparison. Codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ are described by the matrices L_1 and L_2 respectively. The matrices are given below.

$$L_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, L_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Consider receiver R_1. For code $\mathfrak{C}_1$, receiver R_1 uses only one transmission for decoding any of its

[2]The simulation in this section were done by A. Chandramouli

demands. However for code $\mathfrak{C}_2$, receiver R_1 uses more than one transmission for decoding all the demands. For example in order to decode message $x_4 \in \mathcal{W}_1$, receiver R_1 has to make use of three transmissions.

In the simulation, the source uses symmetric 4-PSK signal set which is equivalent to two binary transmissions. The mapping from bits to complex symbols is assumed to be Gray Mapping. We first consider the scenario in which the fading is Rayleigh and the fading coefficient h_j of the channel between source and receiver R_j is $\mathcal{CN}(0,1)$. The SNR Vs. BEP curves for all the receivers for code $\mathfrak{C}_1$ is plotted in Fig. 2.6. From Fig 2.6, we can observe that maximum error probability occurs at receiver R_7. Similar plot for all the receivers while using code $\mathfrak{C}_2$ is shown in Fig 2.7. From Fig. 2.7 we can observe that for code $\mathfrak{C}_2$ maximum error probability occurs at receiver R_7. We compare the performance of both the codes at receiver R_7 in Fig. 2.8. We can observe from Fig. 2.8 that the maximum probability of error across receivers is less for code $\mathfrak{C}_1$ compared to code $\mathfrak{C}_2$.

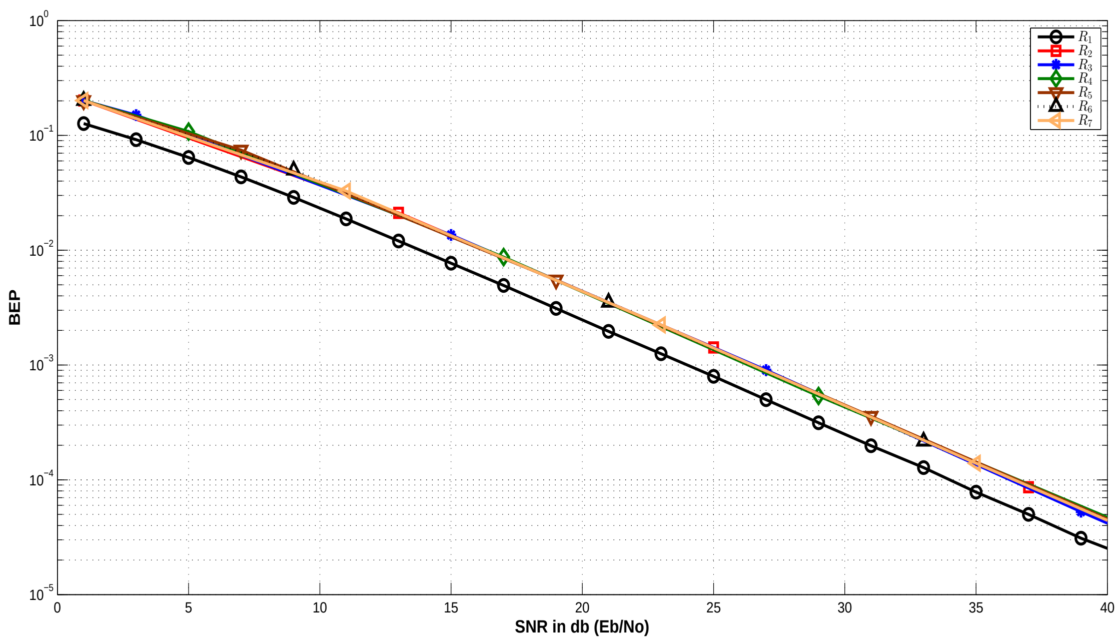


Fig. 2.6 SNR Vs BEP for code $\mathfrak{C}_1$ for Rayleigh fading scenario, at all receivers of Example 7.

The SNR Vs. BEP curves for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for remaining receivers are shown in Fig. 2.9 - Fig. 2.14. Fig. 2.9 shows the SNR Vs. BEP at receiver R_1. From Fig. 2.9, we can clearly see that code $\mathfrak{C}_1$ shows a better performance of around 4.5dB compared to code $\mathfrak{C}_2$. Similar increase in performance was observed at all other receivers. We can observe that in all receivers Code $\mathfrak{C}_1$

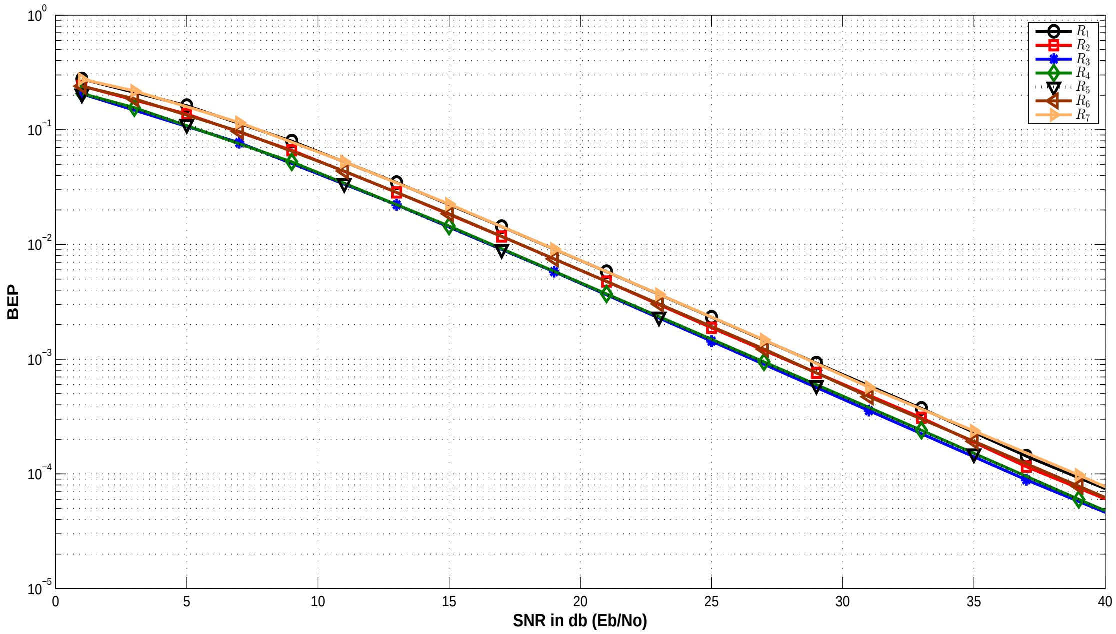


Fig. 2.7 SNR Vs BEP for code $\mathfrak{C}_2$ for Rayleigh fading scenario, at all receivers of Example 7.

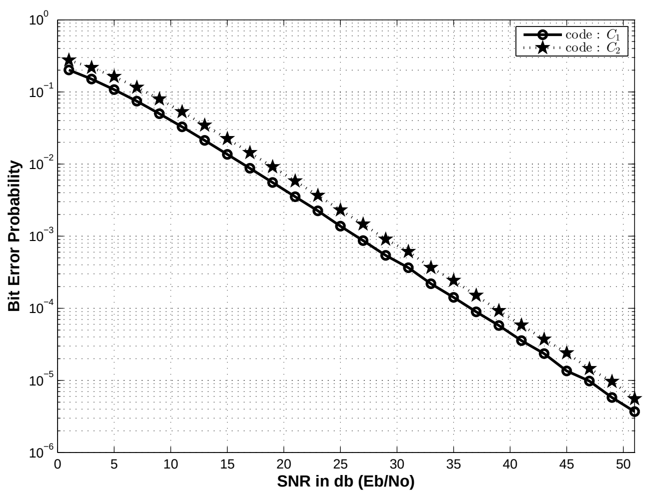


Fig. 2.8 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_7 of Example 7.

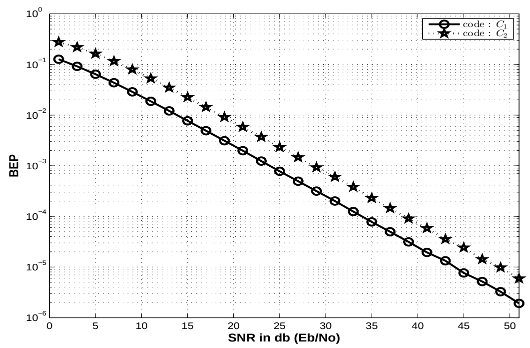


Fig. 2.9 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_1 of Example 7.

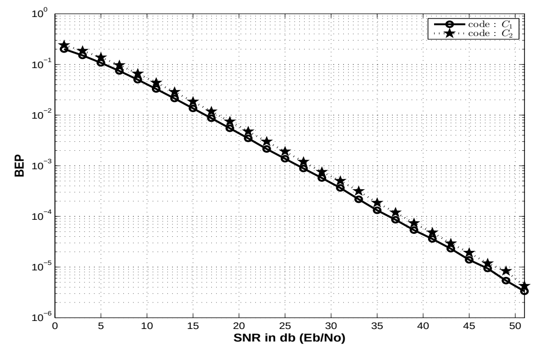


Fig. 2.10 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_2 of Example 7.

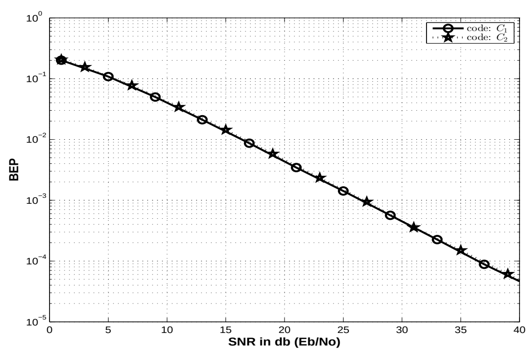


Fig. 2.11 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_3 of Example 7.

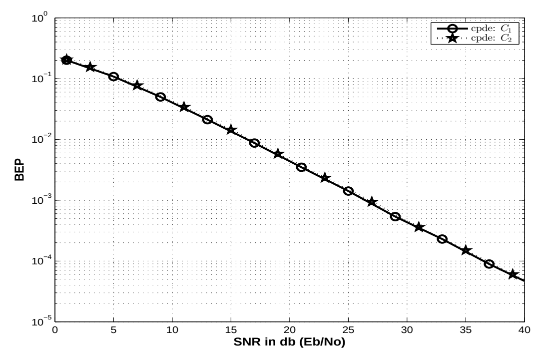


Fig. 2.12 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_4 of Example 7.

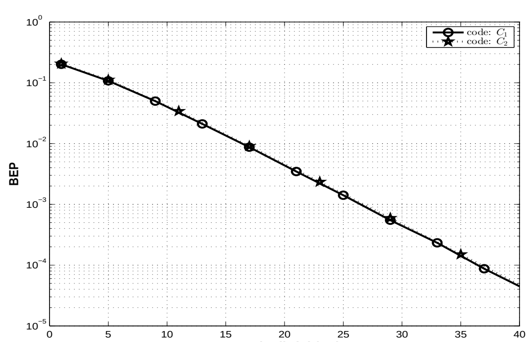


Fig. 2.13 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_5 of Example 7.

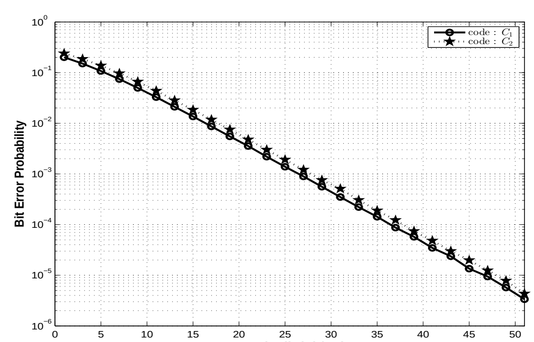


Fig. 2.14 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_6 of Example 7.

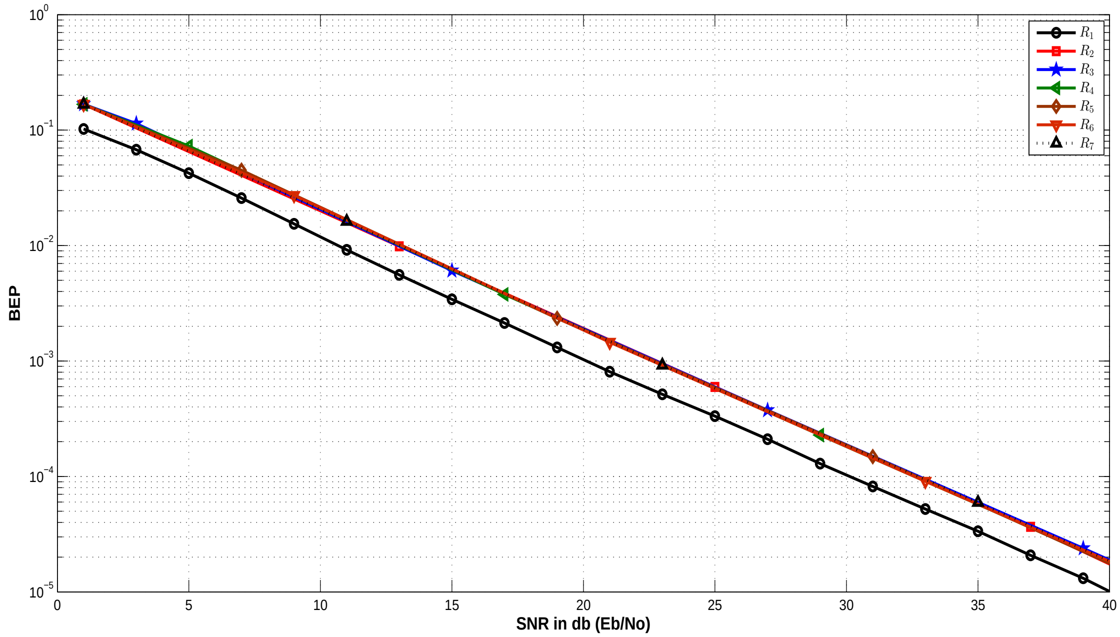


Fig. 2.15 SNR Vs BEP for code $\mathfrak{C}_1$ for Rician fading scenario, at all receivers of Example 7.

performs at least as good as code $\mathfrak{C}_2$. So in terms of reducing the probability of error, Code $\mathfrak{C}_1$ performs better than Code $\mathfrak{C}_2$.

We also consider the scenario in which the channel between source and receiver R_j is a Rician fading channel. The fading coefficient h_j is Rician with a Rician factor 2. The source uses 4-PSK signal set along with Gray mapping. The SNR Vs. BEP curves for all receivers while using code $\mathfrak{C}_1$ and code $\mathfrak{C}_2$ is given in Fig. 2.15 and Fig. 2.16 respectively. We observe that maximum error probability occurs at receiver R_7 for both the codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$. The SNR Vs. BEP curves for both the codes at receiver R_7 is shown in Fig. 2.17. From Fig. 2.17 we observe that maximum error probability for code $\mathfrak{C}_1$ is lesser than for code $\mathfrak{C}_2$. The SNR Vs. BEP plots for both the codes at other receivers are given in Fig. 2.18 - Fig. 2.23. It is evident from the plots that code $\mathfrak{C}_1$ performs better than code $\mathfrak{C}_2$. Though at some receivers it matches the performance, improvement is evident at receivers R_1 and R_7. From the simulation results we can conclude that in both Rayleigh and Rician fading models, code $\mathfrak{C}_1$ performs better than code $\mathfrak{C}_2$ in terms of reducing the probability of error.

Example 8. In this example we consider the index coding problem in Example 1. We compare the

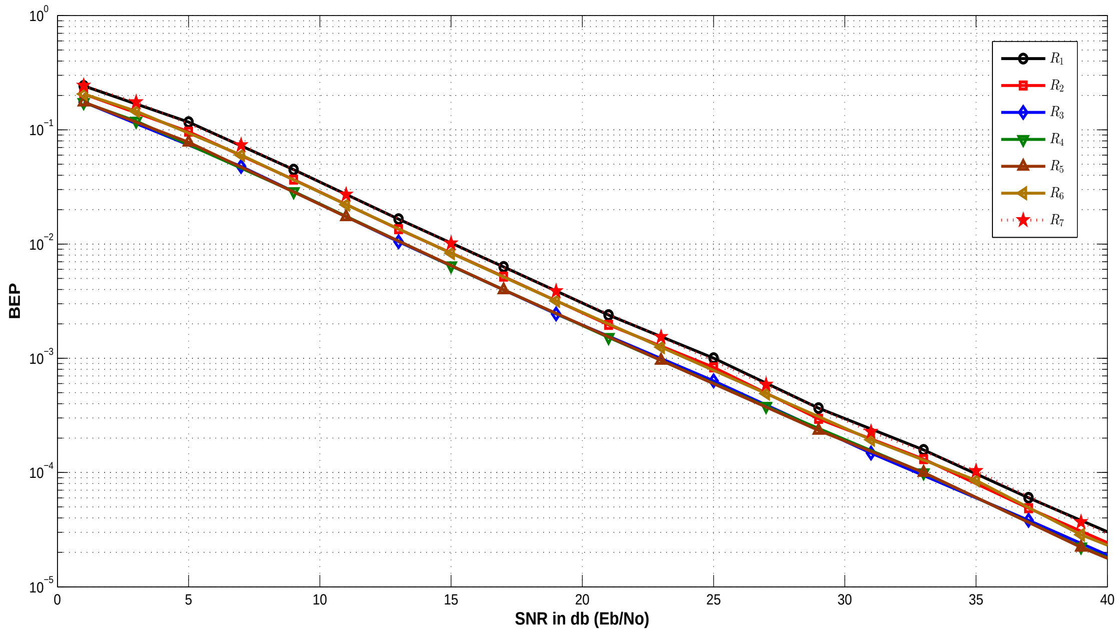


Fig. 2.16 SNR Vs BEP for code $\mathfrak{C}_2$ for Rician fading scenario, at all receivers of Example 7.

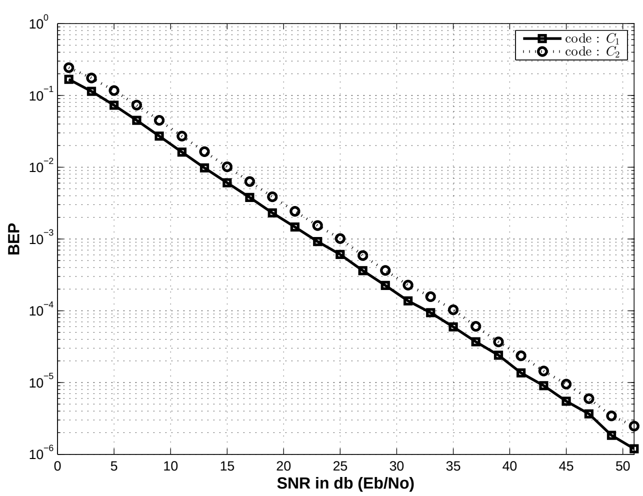


Fig. 2.17 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_7 of Example 7.

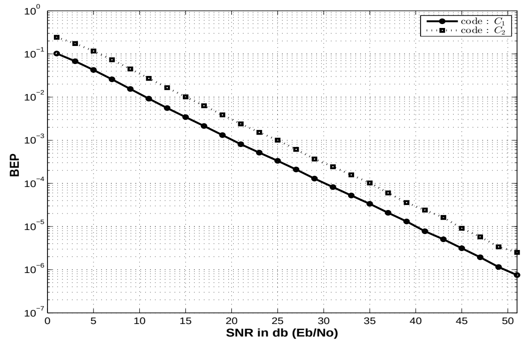


Fig. 2.18 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_1 of Example 7.

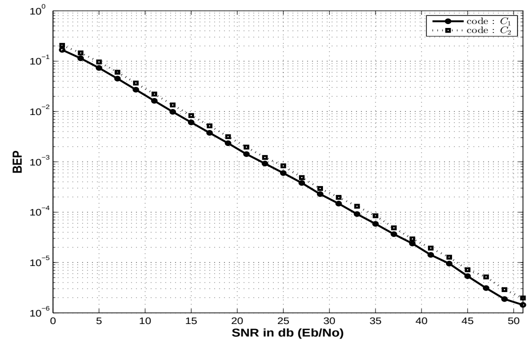


Fig. 2.19 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_2 of Example 7.

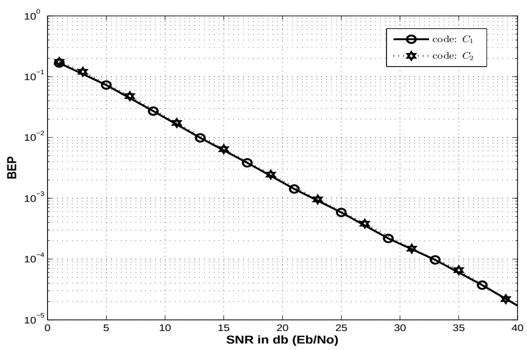


Fig. 2.20 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_3 of Example 7.

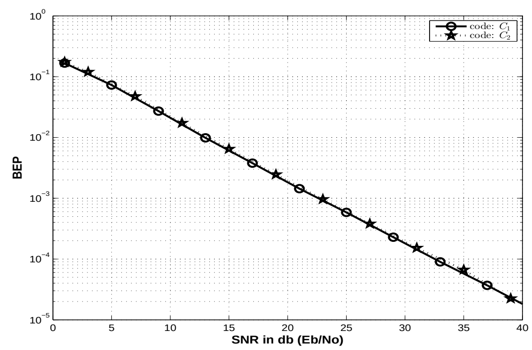


Fig. 2.21 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_4 of Example 7.

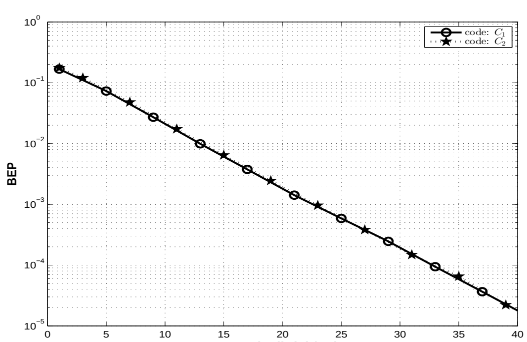


Fig. 2.22 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_5 of Example 7.

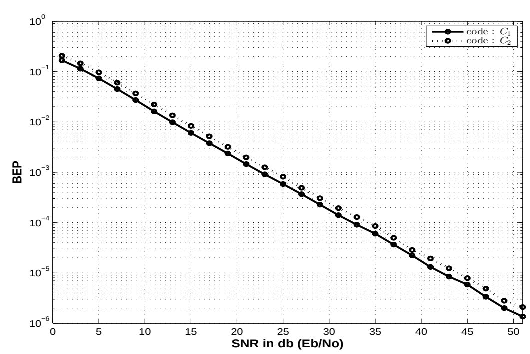


Fig. 2.23 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_6 of Example 7.

performance of codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ of Example 1. The matrices describing code $\mathfrak{C}_1$ and code $\mathfrak{C}_2$ are

$$L_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} L_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

respectively. The source uses symmetric 4-PSK signal set for transmission. The mapping used from bits to complex symbols is Gray mapping. Rayleigh fading scenario is considered first in which the fading coefficient h_j of the channel between the source and receiver R_j is $\mathcal{CN}(0,1)$. The simulation curves showing, SNR Vs. BEP for all the receivers while using code $\mathfrak{C}_1$ is given in Fig 2.24. From Fig. 2.24, we can observe that maximum error probability occurs at all receivers except R_1, R_2 and R_8. The SNR Vs. BEP curves for all the receivers while using code $\mathfrak{C}_2$ is given in Fig. 2.25. From Fig 2.25 we can observe that maximum error probability of error occurs at receiver R_3. In Fig. 2.26 we compare these maximum error probabilities by showing the SNR Vs. BEP curves for both the codes at receiver R_3. From Fig. 2.26 we are able to observe a gain of 2dB at Receiver R_3 by using code $\mathfrak{C}_1$ over code $\mathfrak{C}_2$.

In Fig. 2.27 - Fig. 2.34, SNR Vs. BEP plots for all receivers other than R_3 are given. We can observe from Fig. 2.27 and Fig. 2.28 that code $\mathfrak{C}_1$ performs better than code $\mathfrak{C}_2$ at receivers R_1 and R_2 also. However for receiver R_4, code $\mathfrak{C}_2$ performs better than code $\mathfrak{C}_1$. The reason is that the number of transmissions used by receiver R_4 in decoding its demand is more for code $\mathfrak{C}_1$ than code $\mathfrak{C}_2$. The SNR Vs. BEP for the two codes for receiver R_4 is given in Fig. 2.29. Note that the index code given by proposed Algorithm 2, does not guarantee better performance at all receivers. The algorithm ensures that the index code has minimum maximum error probability across all receivers.

Simulations were also carried out with the channel between source and receiver R_j modelled as a Rician fading channel. The fading coefficient h_j is Rician with a Rician factor 2. The source uses 4-PSK signal set along with Gray mapping. The SNR Vs. BEP curves for all receivers while

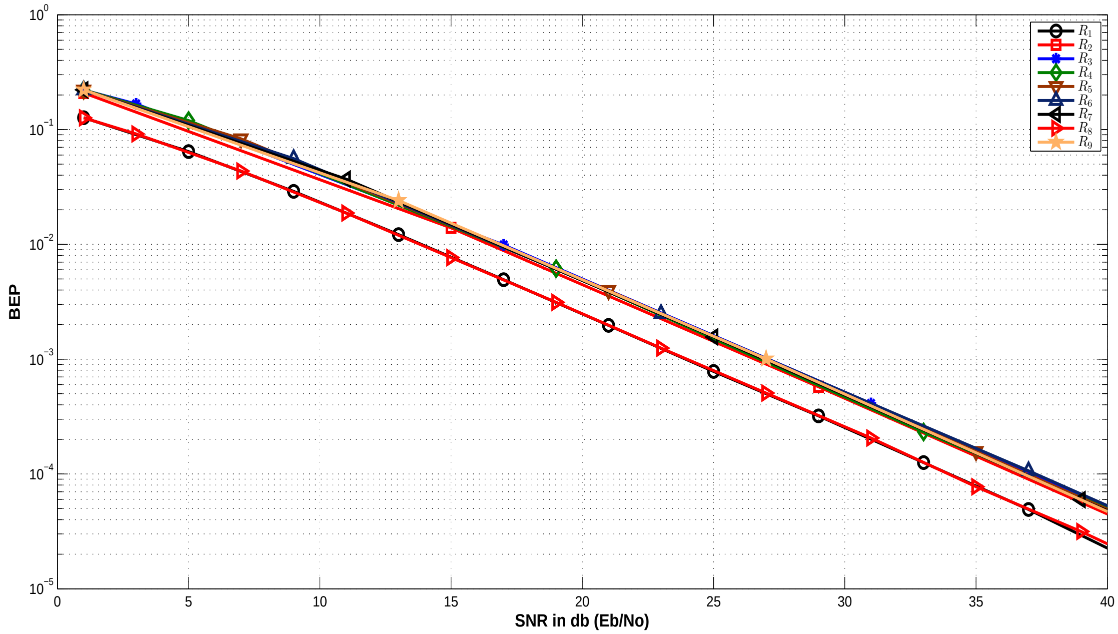


Fig. 2.24 SNR Vs BEP for code $\mathfrak{C}_1$ for Rayleigh fading scenario, at all receivers of Example 8.

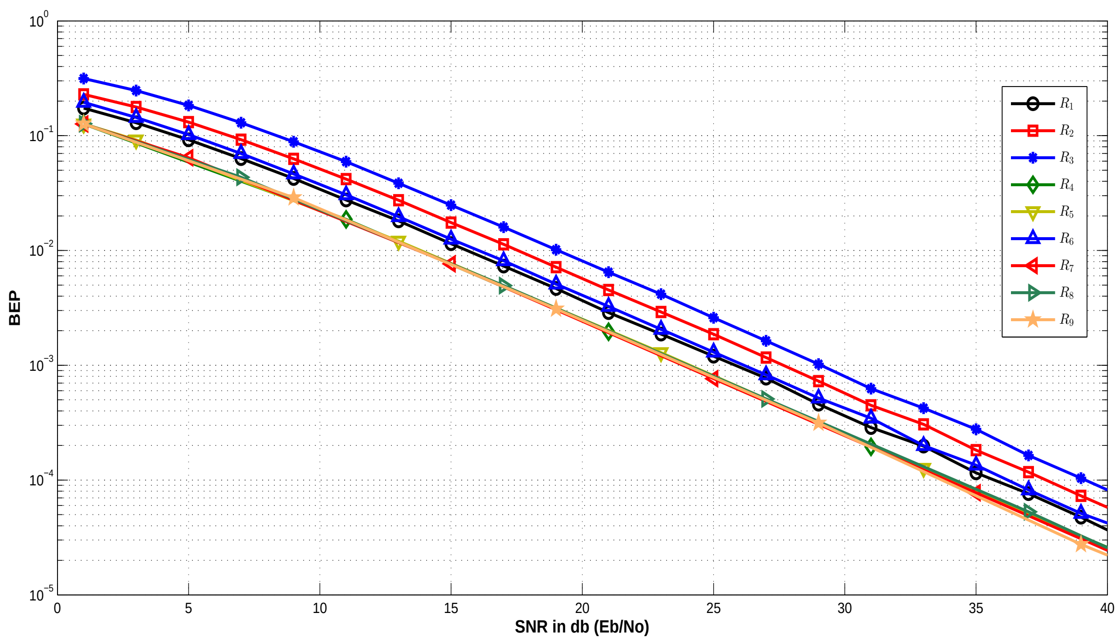


Fig. 2.25 SNR Vs BEP for code $\mathfrak{C}_2$ for Rayleigh fading scenario, at all receivers of Example 8.

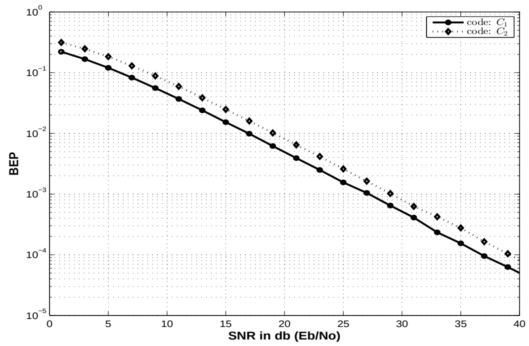


Fig. 2.26 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_3 of Example 8.

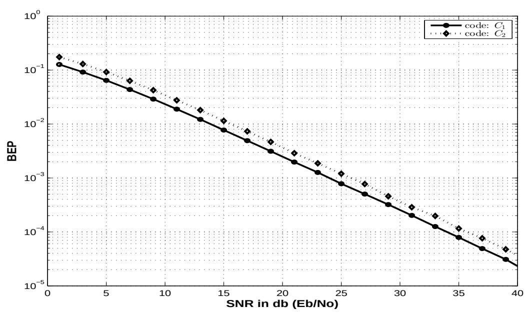


Fig. 2.27 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_1 of Example 8.

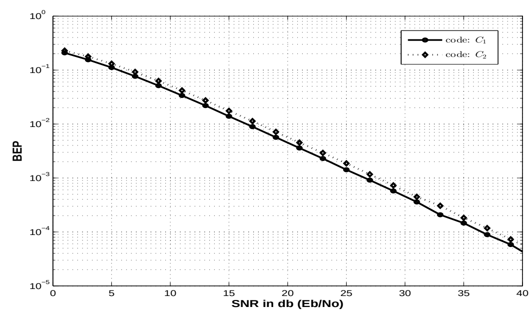


Fig. 2.28 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_2 of Example 8.

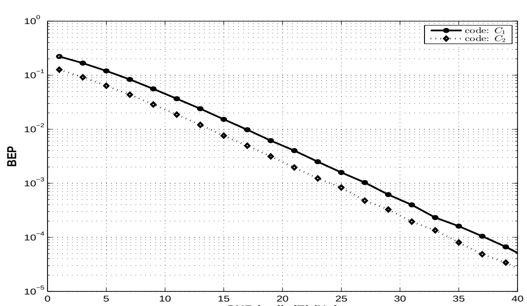


Fig. 2.29 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_4 of Example 8.

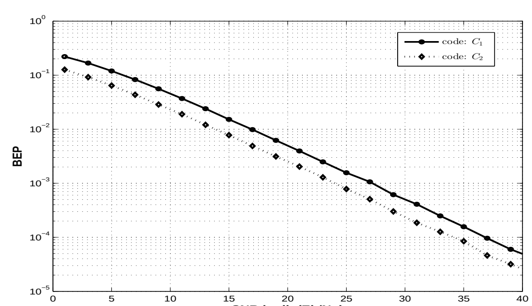


Fig. 2.30 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_5 of Example 8.

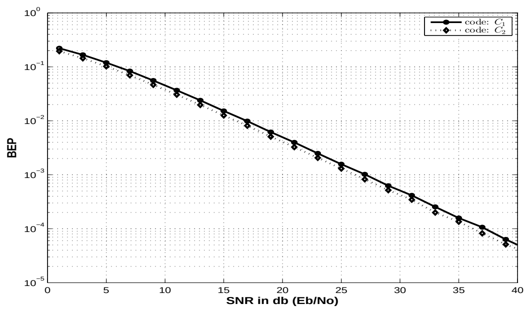


Fig. 2.31 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_6 of Example 8.

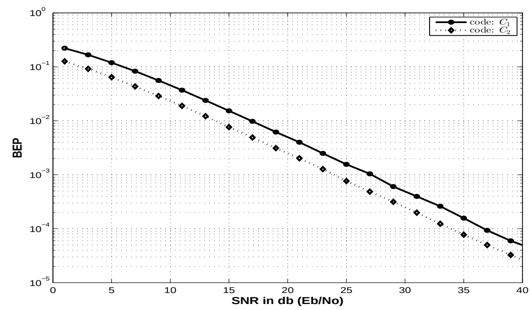


Fig. 2.32 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_7 of Example 8.

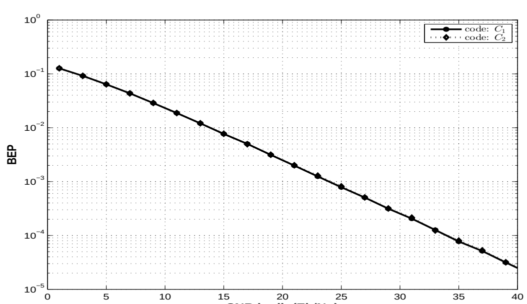


Fig. 2.33 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_8 of Example 8.

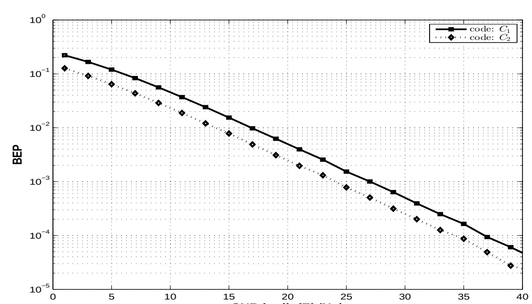


Fig. 2.34 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rayleigh fading scenario, at receiver R_9 of Example 8.

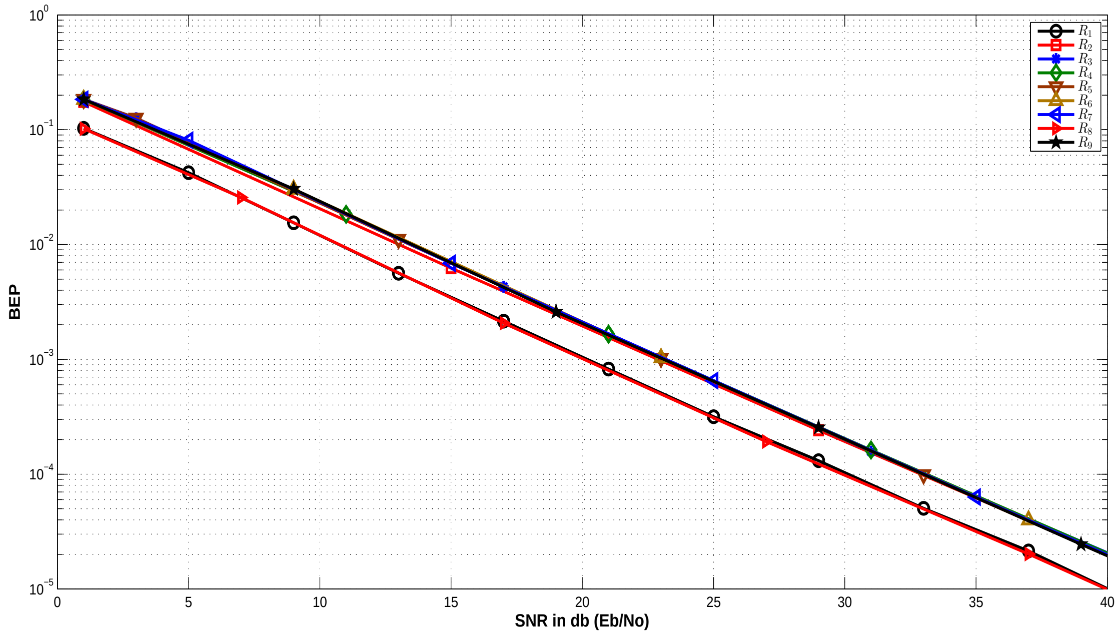


Fig. 2.35 SNR Vs BEP for code $\mathfrak{C}_1$ for Rician fading scenario, at all receivers of Example 8.

using code $\mathfrak{C}_1$ and code $\mathfrak{C}_2$ is given in Fig. 2.35 and Fig. 2.36 respectively. Similar to the Rayleigh fading scenario maximum error probability was observed at receiver R_3. The SNR Vs. BEP curves for both the codes at receiver R_3 are given in Fig. 2.37. We can observe from Fig. 2.37 that for the Rician fading scenario also, maximum error probability is less for code $\mathfrak{C}_1$. The SNR Vs. BEP plots for both the codes at receivers other than R_3 are given in Fig. 2.38-Fig. 2.45. For Rician fading also we infer the same results from the plots. Code $\mathfrak{C}_2$ performs better than code $\mathfrak{C}_1$ for few receivers where the number of transmissions used for decoding its demand is less, but in terms of minimizing maximum error probability across all receivers code $\mathfrak{C}_1$ performs better.

2.4 Results and Discussion

In this work, we considered a model for index coding problem in which the transmissions are broadcasted over a wireless fading channel. To the best of our knowledge, this is the first work that considers such a model. We have described a decoding procedure in which the transmissions are decoded to obtain the index code and from the index code messages are decoded. We have shown that the probability of error increases as the number of transmissions used for decoding the message increases. This shows the significance of optimal index codes such that the number of

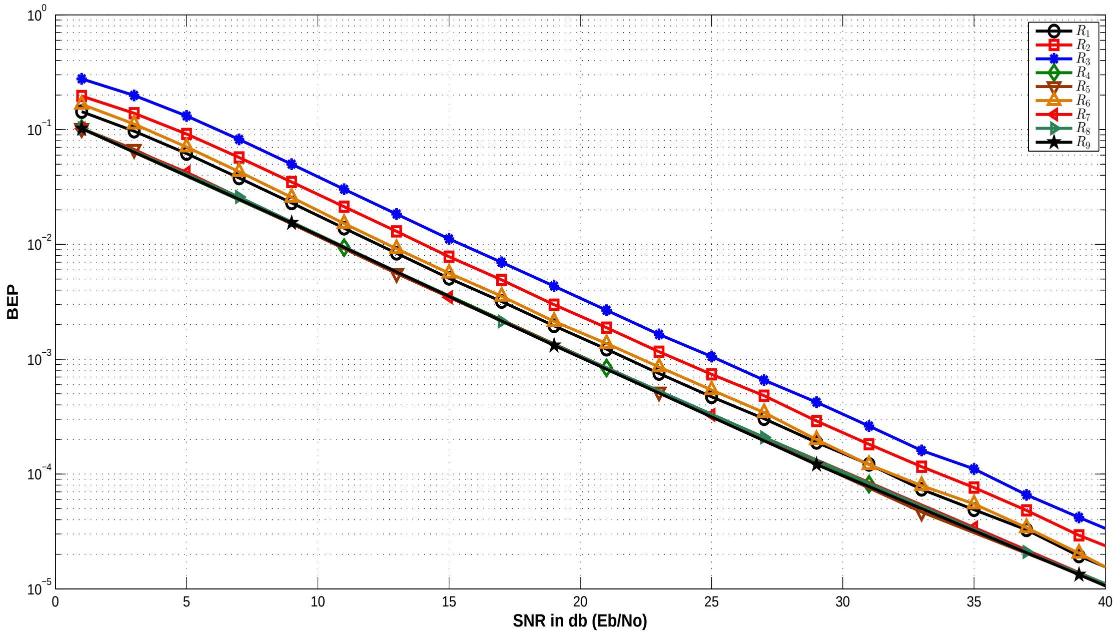


Fig. 2.36 SNR Vs BEP for code $\mathfrak{C}_2$ for Rician fading scenario, at all receivers of Example 8.

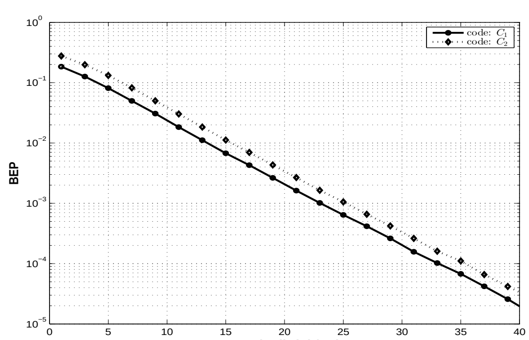


Fig. 2.37 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_3 of Example 8.

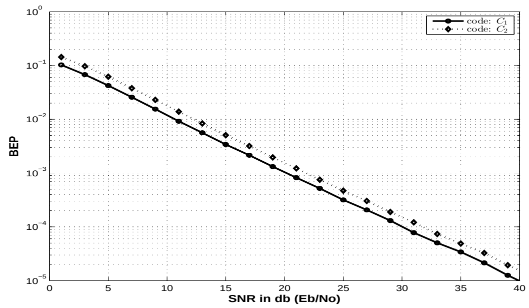


Fig. 2.38 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_1 of Example 8.

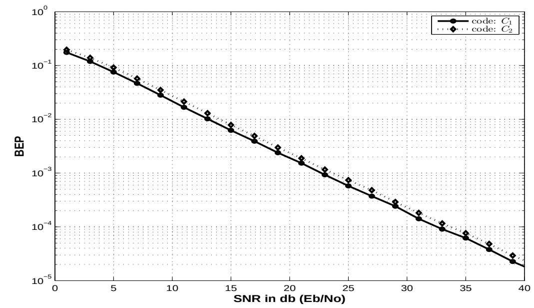


Fig. 2.39 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_2 of Example 8.

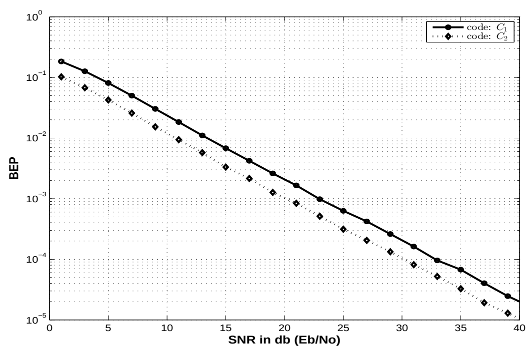


Fig. 2.40 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_4 of Example 8.

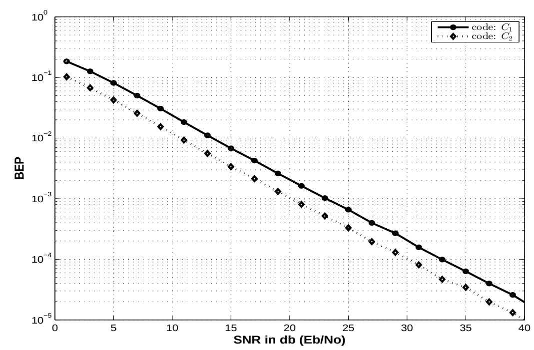


Fig. 2.41 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_5 of Example 8.

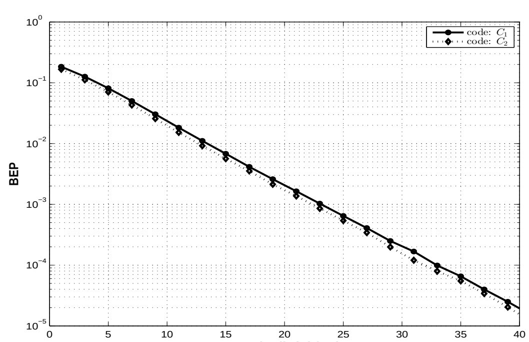


Fig. 2.42 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_6 of Example 8.

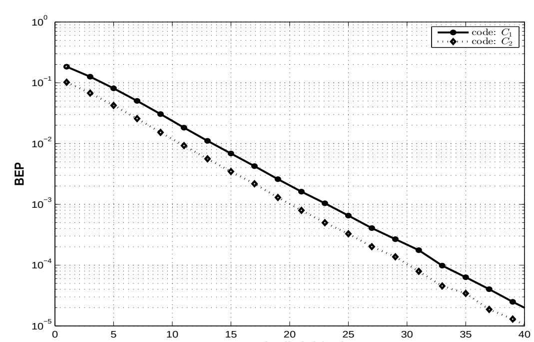


Fig. 2.43 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_7 of Example 8.

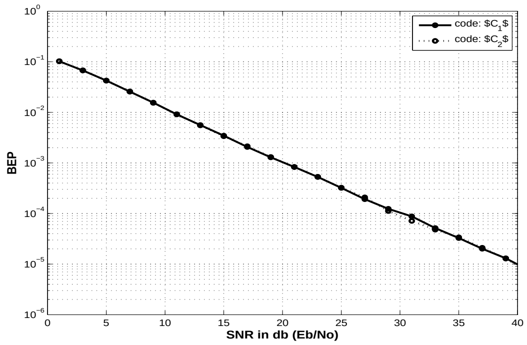


Fig. 2.44 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_8 of Example 8.

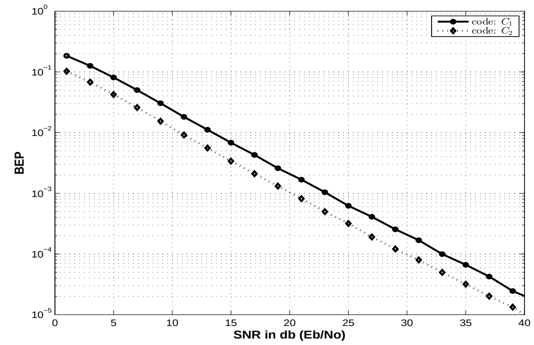


Fig. 2.45 SNR Vs BEP for codes $\mathfrak{C}_1$ and $\mathfrak{C}_2$ for Rician fading scenario, at receiver R_9 of Example 8.

transmissions used for decoding the message is minimized.

For single uniprior index coding problems, we described an algorithm to identify the index code which minimizes the maximum probability of error. We showed simulation results validating our claim. The problem remains open for all other class of index codes. For other class of index coding problems the upper bound on the number of transmissions required by receivers to decode the messages is not known. Finally other methods of decoding could also be considered and this could change the criterion required in reducing the probability of error. The optimal index codes in terms of error probability and bandwidth using such a criterion could also be explored.

Chapter 3

On the number of optimal index codes

[1] As seen before general index coding problem can be formulated as follows: There are n messages, $x_1, x_2, \ldots, x_n$ and m receivers. Each receiver wants a set of messages, $\mathcal{W}_i$ and knows a set of messages $\mathcal{K}_i$. For a general unicast problem, $\mathcal{W}_i \cap \mathcal{W}_j = \emptyset$, for $i \neq j$. The special case when $m = n$ and $\mathcal{W}_i = \{x_i\}$ is called a single unicast problem. We focus on a single unicast problem in this chapter. A general unicast problem can always be reduced to a single unicast problem with $\mid \mathcal{W}_i \mid = 1$ by replication of receivers. Hence the observations in this work applies to a general unicast problem as well. The best linear solution in terms of minimum-maximum error probability among all codes with the optimal length is identified. Also, a lower bound on the total number of linear index coding solutions with the optimal length for a single unicast problem is identified. Any single unicast problem can be represented by an equivalent network coding problem as in Fig.3.1. This was proposed by El Rouayheb *et. al.* in [5].

Here each of the messages $x_1, x_2, \ldots, x_n$ is represented by a source node and $g_1, g_2, \ldots, g_N$ represent the broadcast channel and $l_1, l_2, \ldots, l_N, l'_1, l'_2, \ldots, l'_N$ represent the intermediate nodes. When two or more edges have the same tail node, they carry the same message. Also l'_i transmits to its outgoing edges whatever it gets by g_i. The source nodes transmit their respective messages as such through their outgoing edges. The length of the index code is represented by N. The optimal value of N among all linear solutions of an IC problem is to be found. Our operations are over the finite field $\mathbb{F}_2$. But the results in this paper can be carried over to other fields also. The dashed

[1]A Part of this work appears in *Proc. ISIT'2015*, Wanchai, Hong Kong, June, 2015.

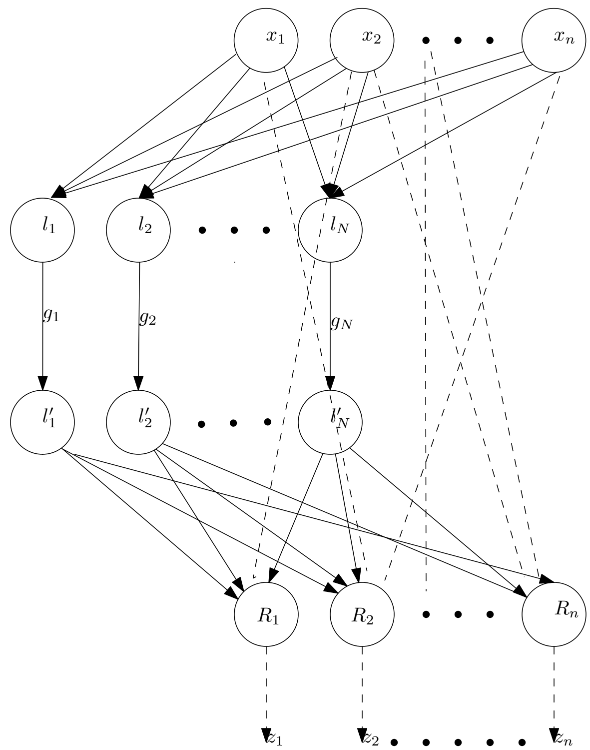


Fig. 3.1 Representation of a unicast IC problem by an equivalent network code.

lines represent the connection between a receiver node and its prior message (node) among the set of messages (nodes) i.e, they represent the side information possessed by the receivers. For every single unicast problem, we can find a graph like given in Fig.3.1. Let us call it G. The graph G can be represented as $G = (V, E)$, where $V = \{x_1, x_2, \ldots, x_n, l_1, l_2, \ldots, l_N, l'_1, l'_2, \ldots, l'_N, R_1, R_2, \ldots, R_n\}$ is the vertex set and E is the edge set. We can observe that $\mid E \mid = (2n+1)N + \sum_{i=1}^{n} \mid \mathcal{K}_i \mid$. An edge connecting vertex v_1 to v_2 is denoted by (v_1, v_2) where v_1 is the tail of the edge and v_2 is the head of the edge. For an edge e, $Y(e)$ represents the message passed in that edge. We can get a transfer matrix $M_{n \times n}$ (which is shown in section 3.1) such that $\underline{Z} = [z_1 \ z_2 \ \ldots \ z_n]^T$, the vector of output messages at each of the receivers, can be expressed as

$$\underline{Z} = M \ \underline{X}, \tag{3.1}$$

where $\underline{X} = [x_1 \ x_2 \ \ldots \ x_n]^T$, the vector of input messages. Hence, we can solve the IC in N number of transmissions if M is an identity matrix.

$$
\begin{aligned}
\underline{\mathrm{Y}}^T = [&Y((x_1,l_1))\ Y((x_1,l_2))\ \ldots\ Y((x_1,l_N))\\
&Y((x_2,l_1))\ Y((x_2,l_2))\ \ldots\ Y((x_2,l_N))\\
&\vdots\\
&Y((x_n,l_1))\ Y((x_n,l_2))\ \ldots\ Y((x_n,l_N))\\
&Y((x_{\mathcal{K}_{1,1}},R_1))\ Y((x_{\mathcal{K}_{1,2}},R_1))\ldots\ Y((x_{\mathcal{K}_{1,|\mathcal{K}_1|}},R_1))\\
&Y((x_{\mathcal{K}_{2,1}},R_2))\ Y((x_{K_{2,2}},R_2))\ \ldots\ Y((x_{\mathcal{K}_{2,|\mathcal{K}_2|}},R_2))\\
&\vdots\\
&Y((x_{\mathcal{K}_{n,1}},R_n))\ Y((x_{\mathcal{K}_{n,2}},R_n))\ Y((x_{\mathcal{K}_{n,|\mathcal{K}_n|}},R_n))]
\end{aligned} \tag{3.5}
$$

3.1 Problem Formulation

For a general single unicast problem, we can find a matrix $M_{n\times n}$ such that the vector of output bits $\underline{\mathrm{Z}} = M\ \underline{\mathrm{X}}$. We can observe that M is a product of three matrices as given in (3.3).[2] We will give the structure of each of these matrices first and then explain how we derived (3.3).

$$M = B\ F\ A \tag{3.2}$$

The matrix A relates the input messages and the messages flowing through the outgoing edges of all the source nodes. A satisfies the following relation.

$$M = B\ F\ A \tag{3.3}$$

The matrix A relates the input messages and the messages flowing through the outgoing edges of all the source nodes. A satisfies the following relation.

$$\underline{\mathrm{Y}} = A\ \underline{\mathrm{X}}, \tag{3.4}$$

where $\underline{\mathrm{Y}}^T$ is as in (3.5). $\underline{\mathrm{Y}}$ is the vector of messages flowing through the outgoing edges of all the source nodes and is of order $((nN + \sum_{i=1}^{n} \mid \mathcal{K}_i \mid) \times 1)$. Here $\mathcal{K}_{i,j}$ denotes the index of j-th message in

[2] We are not following Koetter and Medard's approach [6]. If we had followed their approach in a strict sense we would have got matrix A of order $(\mid E \mid \times n)$, F of order $(\mid E \mid \times \mid E \mid)$and B of order $(n\times \mid E \mid)$. We give a simpler formulation for the matrices A, F and B for a given index coding problem.

the side information set of receiver R_i and $\underline{X} = [x_1\ x_2\ x_3 \ldots\ x_n]^T$ is the vector of input messages. The matrix A is of order $(nN + \sum_{i=1}^{n} \mid \mathcal{K}_i \mid) \times n$ and it can be split in the form,

$$A = \begin{bmatrix} A_B \\ A_{SI} \end{bmatrix} \tag{3.6}$$

where A_B is of order $nN \times n$ and A_{SI} is of order $\sum_{i=1}^{n} \mid \mathcal{K}_i \mid \times n$. The matrix A_B is a matrix formed by row-concatenation of matrices A_i, $i = 1, \ldots n$ where each A_i is a $N \times n$ matrix in which all elements in the i-th column are ones and the rest all are zeros as given in (3.7).

$$\begin{matrix} A_1 \left\{ \begin{matrix} \\ \\ \\ \\ \\ \end{matrix} \right. \\ A_2 \left\{ \begin{matrix} \\ \\ \\ \\ \\ \end{matrix} \right. \\ . \\ . \\ A_n \left\{ \begin{matrix} \\ \\ \\ \\ \\ \end{matrix} \right. \end{matrix} \begin{bmatrix} 1 & 0 & 0 & 0 & \ldots & 0 \\ 1 & 0 & 0 & 0 & \ldots & 0 \\ . & & & & & \\ . & & & & & \\ 1 & 0 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & 0 & \ldots & 0 \\ . & & & & & \\ . & & & & & \\ 0 & 1 & 0 & 0 & \ldots & 0 \\ . & & & & & \\ . & & & & & \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ . & & & & & \\ . & & & & & \\ 0 & 0 & 0 & 0 & \ldots & 1 \end{bmatrix} \tag{3.7}$$

Each A_i corresponds to the message passed by the source node x_i to the intermediate nodes, l_j, $j = 1, \ldots, N$. The matrix A_{SI} has only one non-zero element (which is one) in each row. This matrix corresponds to the side information possessed by the receivers and each successive set of

$$
\begin{aligned}
\underline{\mathrm{Y}}'^T = [&Y((l'_1, R_1))\ Y((l'_1, R_2))\ \ldots Y((l'_1, R_n)) \\
&Y((l'_2, R_1))\ Y((l'_2, R_2))\ \ldots Y((l'_2, R_n)) \\
&\vdots \\
&Y((l'_N, R_1))\ Y((l'_N, R_2))\ \ldots\ Y((l'_N, R_n)) \\
&Y((x_{\mathcal{K}_{1,1}}, R_1))\ Y((x_{\mathcal{K}_{1,2}}, R_1)) \ldots Y((x_{\mathcal{K}_{1,|\mathcal{K}_1|}}, R_1)) \\
&Y((x_{\mathcal{K}_{2,1}}, R_2))\ Y((x_{\mathcal{K}_{2,2}}, R_2))\ \ldots Y((x_{\mathcal{K}_{2,|\mathcal{K}_2|}}, R_2)) \\
&\vdots \\
&Y((x_{\mathcal{K}_{n,1}}, R_n))\ Y((x_{\mathcal{K}_{n,2}}, R_n)) \ldots Y((x_{\mathcal{K}_{n,|\mathcal{K}_n|}}, R_n))]
\end{aligned}
\tag{3.9}
$$

$$
F_B = \begin{bmatrix}
\beta_{(x_1,l_1)} & 0 & \ldots & 0 & \beta_{(x_2,l_1)} & 0 & \ldots & 0 & \ldots & \beta_{(x_n,l_1)} & 0 & \ldots & 0 \\
\beta_{(x_1,l_1)} & 0 & \ldots & 0 & \beta_{(x_2,l_1)} & 0 & \ldots & 0 & \ldots & \beta_{(x_n,l_1)} & 0 & \ldots & 0 \\
\vdots & & & & & & & & & & & & \\
\beta_{(x_1,l_1)} & 0 & \ldots & 0 & \beta_{(x_2,l_1)} & 0 & \ldots & 0 & \ldots & \beta_{(x_n,l_1)} & 0 & \ldots & 0 \\
0 & \beta_{(x_1,l_2)} & \ldots & 0 & 0 & \beta_{(x_2,l_2)} & \ldots & 0 & \ldots & 0 & \beta_{(x_n,l_2)} & \ldots & 0 \\
0 & \beta_{(x_1,l_2)} & \ldots & 0 & 0 & \beta_{(x_2,l_2)} & \ldots & 0 & \ldots & 0 & \beta_{(x_n,l_2)} & \ldots & 0 \\
\vdots & & & & & & & & & & & & \\
0 & \beta_{(x_1,l_2)} & \ldots & 0 & 0 & \beta_{(x_2,l_2)} & \ldots & 0 & \ldots & 0 & \beta_{(x_n,l_2)} & \ldots & 0 \\
\vdots & & & & & & & & & & & & \\
0 & 0 & \ldots & \beta_{(x_1,l_N)} & 0 & 0 & \ldots & \beta_{(x_2,l_N)} & \ldots & 0 & 0 & \ldots & \beta_{(x_n,l_N)} \\
0 & 0 & \ldots & \beta_{(x_1,l_N)} & 0 & 0 & \ldots & \beta_{(x_2,l_N)} & \ldots & 0 & 0 & \ldots & \beta_{(x_n,l_N)} \\
\vdots & & & & & & & & & & & & \\
0 & 0 & \ldots & \beta_{(x_1,l_N)} & 0 & 0 & \ldots & \beta_{(x_2,l_N)} & \ldots & 0 & 0 & \ldots & \beta_{(x_n,l_N)}
\end{bmatrix}
\tag{3.10}
$$

$|\ \mathcal{K}_i\ |$ rows correspond to the side information possessed by R_i for $i = 1$ to n. In each set of $|\ \mathcal{K}_i\ |$ rows, each row is distinct and has only one non-zero element (which is one as we operate over the finite field $\mathbb{F}_2$.) which occupies the respective column-position of one of the messages in the prior set of R_i. Hence the matrix A is fixed for a fixed N.

The matrix F relates to the messages sent in the broadcast channel and the side information possessed by the the receivers and is of order $(nN + \sum_{i=1}^{n} |\ \mathcal{K}_i\ |) \times (nN + \sum_{i=1}^{n} |\ \mathcal{K}_i\ |)$. It is the matrix that satisfies the following relation.

$$
\underline{\mathrm{Y}}' = F\ \underline{\mathrm{Y}} = F\ A\ \underline{\mathrm{X}}, \tag{3.8}
$$

where $\underline{\mathrm{Y}}'^T$ is as in (3.9). $\underline{\mathrm{Y}}'$ is the vector of messages flowing to each of the receiver. We can observe that F can be split into four block matrices as given below.

$$B_B = \left[\begin{array}{ccccccccccccccc} \epsilon_{(l_1,R_1)} & 0 & 0 & \dots & 0 & \epsilon_{(l_2,R_1)} & 0 & 0 & \dots & 0 & \dots & \epsilon_{(l_N,R_1)} & 0 & 0 & \dots & 0 \\ 0 & \epsilon_{(l_1,R_2)} & 0 & \dots & 0 & 0 & \epsilon_{(l_2,R_2)} & 0 & \dots & 0 & \dots & 0 & \epsilon_{(l_N,R_2)} & 0 & \dots & 0 \\ \dots & & & & & & & & & & & & & & & \\ \dots & & & & & & & & & & & & & & & \\ \dots & & & & & & & & & & & & & & & \\ 0 & 0 & 0 & \dots & \epsilon_{(l_1,R_n)} & 0 & 0 & 0 & \dots & \epsilon_{(l_2,R_n)} & \dots & 0 & 0 & 0 & \dots & \epsilon_{(l_N,R_n)} \end{array} \right] \tag{3.13}$$

$$F = \begin{bmatrix} F_B & 0 \\ 0 & I \end{bmatrix} \tag{3.11}$$

Matrix F_B is a square matrix of order nN which is of the form given in (3.10) and I is the identity matrix. The elements $\beta_{(x_i,l_j)}, \forall i = 1,\dots,n$ and $j = 1,\dots,N$ belong to the finite field $\mathbb{F}_2$. Every $((i-1)n+1)$-th to $((i-1)n+n)$-th row are identical for $i = 1,2,\dots,N$. If $((i-1)n+1)$-th row is denoted as t_i,

$$t_i \; A_B \; \underline{\mathrm{X}} = g_i \tag{3.12}$$

for $i = 1,2,\dots,N$. The matrix B is of order $n \times (nc + \sum_{i=1}^{n} \mid \mathcal{K}_i \mid)$. It relates to the decoding operations done at the receivers. It is the matrix that satisfies the following relation,

$$\underline{\mathrm{Z}} = B \; \underline{\mathrm{Y}}' = B \; F \; A \; \underline{\mathrm{X}}, \tag{3.14}$$

where $\underline{\mathrm{Z}} = [z_1 \; z_2 \; z_3 \dots \; z_n]^T$, is the vector of output messages decoded at the receivers. The matrix B can be split into two block matrices as below.

$$B = \begin{bmatrix} B_B & B_{SI} \end{bmatrix}, \tag{3.15}$$

where B_B is a matrix of order $n \times nN$ and in every row only N elements are non-zero and the non-zero elements corresponds to whether or not R_i uses that particular transmission to decode its wanted message. The matrix B_{SI} is of order $n \times \sum_{i=1}^{n} \mid \mathcal{K}_i \mid$. It relates to the side information possessed by the receivers. In this matrix all elements except the i-th element in every successive set of $\mid \mathcal{K}_i \mid$ columns are strictly zeros, for all $i = 1$ to n. The rest of the elements are either one or zero and it depends on the messages used by a receiver to decode its wanted message. The matrix B_B is as in (3.13). The elements ϵ_{l_j,R_i} for $j = 1,\dots,N$ and $i = 1,\dots,n$ belong to the finite field

$\mathbb{F}_2$. From (3.4), (3.8) and (3.14), we get

$$\underline{Z} = B\ F\ A\ \underline{X}. \tag{3.16}$$

So,

$$M = B\ F\ A. \tag{3.17}$$

An index code is solvable with N number of transmissions if we can find variables (β's and ϵ's) such that M is an identity matrix. Now we will illustrate an example.

Example 9. Let $m = n = 3$. Each R_i wants x_i and knows x_{i+1}, where $+$ is mod-3 addition. The optimal length of a linear IC solution for this problem is 2, which we prove in section 3.2. The graph G for $N = 2$ is as in Fig.3.2:

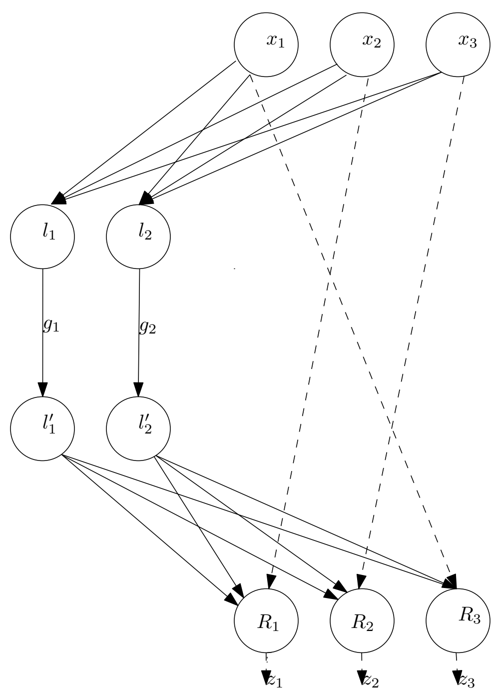


Fig. 3.2 Equivalent network code corresponding to the IC problem in Example 9

$\underline{Y}^T = [Y((x_1, l_1))\ Y((x_1, l_2))\ Y((x_2, l_1)\ Y((x_2, l_2)\ Y((x_3, l_1))\ Y((x_3, l_2))\ Y((x_2, R_1))\ Y((x_3, R_2))$ $Y((x_1, R_3))]$, i.e., the set of all outgoing messages from the source nodes. The vector of input messages is $\underline{X} = [x_1\ x_2\ x_3]^T$. The vector $\underline{Y}'^T = [Y((l'_1, R_1))\ Y((l'_1, R_2))\ Y((l'_1, R_3))\ Y((l'_2, R_1))Y((l'_2, R_2))$ $Y((l'_2, R_3))\ Y((x_2, R_1))\ Y((x_3, R_2))\ Y((x_1, R_3)]$, i.e., the vector of messages flowing to each of the

$$F_B = \begin{bmatrix} \beta_{(x_1,l_1)} & 0 & \beta_{(x_2,l_1)} & 0 & \beta_{(x_3,l_1)} & 0 \\ \beta_{(x_1,l_1)} & 0 & \beta_{(x_2,l_1)} & 0 & \beta_{(x_3,l_1)} & 0 \\ \beta_{(x_1,l_1)} & 0 & \beta_{(x_2,l_1)} & 0 & \beta_{(x_3,l_1)} & 0 \\ 0 & \beta_{(x_1,l_2)} & 0 & \beta_{(x_2,l_2)} & 0 & \beta_{(x_3,l_2)} \\ 0 & \beta_{(x_1,l_2)} & 0 & \beta_{(x_2,l_2)} & 0 & \beta_{(x_3,l_2)} \\ 0 & \beta_{(x_1,l_2)} & 0 & \beta_{(x_2,l_2)} & 0 & \beta_{(x_3,l_2)} \end{bmatrix} \tag{3.19}$$

$$B = \begin{bmatrix} \epsilon_{(l_1,R_1)} & 0 & 0 & \epsilon_{(l_2,R_1)} & 0 & 0 & \epsilon_{(x_2,R_1)} & 0 & 0 \\ 0 & \epsilon_{(l_1,R_2)} & 0 & 0 & \epsilon_{(l_2,R_2)} & 0 & 0 & \epsilon_{(x_3,R_2)} & 0 \\ 0 & 0 & \epsilon_{(l_1,R_3)} & 0 & 0 & \epsilon_{(l_2,R_3)} & 0 & 0 & \epsilon_{(x_1,R_3)} \end{bmatrix} \tag{3.20}$$

receivers. The output at the receivers after decoding, is $Z = [z_1\ z_2\ z_3]^T$. The A matrix is as below.

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \tag{3.18}$$

The F_B is as in (3.19) and B matrix is as in (3.20). The number of linear codes which are optimal in terms of length is three. They are $\mathfrak{C}_1 : x_1 \oplus x_2,\ x_2 \oplus x_3$, $\mathfrak{C}_2 : x_1 \oplus x_3,\ x_3 \oplus x_2$, $\mathfrak{C}_3 : x_1 \oplus x_3,\ x_1 \oplus x_2$. For the code $\mathfrak{C}_1$, the matrices F_B and B are as in (3.21). For the code $\mathfrak{C}_2$, the matrices F_B and B are as in (3.22). For the code $\mathfrak{C}_3$, the matrices F_B and B are as in (3.23).

3.2 Method to Identify the Optimal Length for a Linear solution

We have analysed the structures of the three matrices in the previous section. We need $M = B\ F\ A$ to be I, the identity matrix. Here for a fixed length N, A is fixed and as can be verified all the columns of A are independent. Hence the rank of A is n. So columns of I_n (identity matrix of order

$$F_B = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{3.21}$$

$$F_B = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{3.22}$$

$$F_B = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{3.23}$$

---

n) lies in the column space of A^T. Hence the equation $A^T T_{(nN+\sum_{i=1}^{n}|\mathcal{K}_i|)\times n} = I_n$ has at least one solution for T. Observe that the number of free variables in T is $(n^2N - n^2 + n\sum_{i=1}^{n} \mid \mathcal{K}_i \mid)$ and the number of pivot variables is n^2 [7]. Hence the number of right inverses of A^T is $2^{n^2N-n^2+n\sum_{i=1}^{n}|\mathcal{K}_i|}$. We need to find a matrix T which is a right inverse of A^T as well is a product of some F^T and B^T in the required form. Let us call the set of all such matrices which satisfy both the conditions as $S(N)$. It is a function of N. The cardinality of the set $S(N)$ for a given length N is unknown. To analyse it, let us assume that $S(N)$ is non-empty. Take a T which belongs to $S(N)$. So, there exists a B and F such that $B\ F = T^T$. Let,

$$T^T = \begin{bmatrix} T_B & T_{SI} \end{bmatrix}, \tag{3.24}$$

where T_B is a $n \times nN$ matrix. Hence,

$$\begin{bmatrix} B_B B_{SI} \end{bmatrix} \begin{bmatrix} F_B & 0 \\ 0 & I \end{bmatrix} = T^T . \tag{3.25}$$

This gives $T_{SI} = B_{SI}$. So the positions which are to be strictly occupied by zeros in B_{SI} are zeros in T_{SI} also. Therefore, T_{SI} which is of order $n \times \sum_{i=1}^{n} \mid \mathcal{K}_i \mid$ has $(n-1)(\sum_{i=1}^{n} \mid \mathcal{K}_i \mid)$ zeroes and when the rest of the elements of T_{SI} are fixed, B_{SI} also gets fixed. Keeping this in mind, we find out how many such T's are possible at the most. As the rank of A is n, the total number of right inverses of A^T with restrictions said above (regarding the presence of zeroes at specific places) is $2^{n^2N - n^2 + \sum_{i=1}^{n} |\mathcal{K}_i|}$. Let us call this set $S'(N)$. Clearly $S(N) \subseteq S'(N)$. Hence,

$$|S(N)| \leq 2^{n^2N - n^2 + \sum_{i=1}^{n} |\mathcal{K}_i|}. \tag{3.26}$$

We will have to identify the elements in the set $S'(N)$ which also belong to $S(N)$. But a matrix belongs to $S(N)$ if and only if at least one pair of (B, F) exists such that their product is the transpose of the matrix itself. For each T from $S(N)$, how many (B, F) pairs are possible is unknown. First of all, when we fix T, B_{SI} gets fixed. So for a pair (B, F) whose product is T^T (which belongs to set $S(N)$),

$$B_B F_B = T_B. \tag{3.27}$$

From (3.27) we get relations of the form,

$$\begin{bmatrix} \epsilon_{l_i,R_1} \\ . \\ . \\ \epsilon_{l_i,R_n} \end{bmatrix} \beta_{(x_k,l_i)} = \begin{bmatrix} T_{col_{(k-1)N+i}} \end{bmatrix} \tag{3.28}$$

$\forall k \in \{1, 2...n\}$ and $\forall i \in \{1, 2....N\}$ where T_{col_i} is the i-th column of T_B.

Lemma 2. Any matrix T which belongs to $S'(N)$ also belongs to $S(N)$ if and only if the following condition is satisfied:

The space spanned by the set of columns $\{T_{col_i}, T_{col_{N+i}} ... T_{col_{(n-1)N+i}}\}$ in T_B is one or zero dimensional for all i.

Proof. Proof of only-if part: If $T \in S(N)$, From (3.28), we get relations of the form as below.

$$\begin{bmatrix} \epsilon_{l_i,R_1} \\ \epsilon_{l_i,R_2} \\ . \\ . \\ \epsilon_{l_i,R_n} \end{bmatrix} \beta_{(x_k,l_i)} = \begin{bmatrix} T_{col_{(k-1)N+i}}. \end{bmatrix} \tag{3.29}$$

Also,

$$\begin{bmatrix} \epsilon_{l_i,R_1} \\ \epsilon_{l_i,R_2} \\ . \\ . \\ \epsilon_{l_i,R_n} \end{bmatrix} \beta_{(x_{k'},l_i)} = \begin{bmatrix} T_{col_{(k'-1)N+i}}. \end{bmatrix} \tag{3.30}$$

Hence $T_{col_{(k'-1)N+i}}$ has to be expressible as a multiple of $T_{col_{(k-1)N+i}}$ or vice verse, $\forall\ k,\ k' \in \{1, 2...n\}$ and for every $i \in \{1, 2...N\}$. This is not possible unless any such set of columns is one dimensional or has only all-zero columns which makes it zero dimensional.

Proof of if part : If the space spanned by the set of columns $\{T_{col_i}, T_{col_{N+i}} ... T_{col_{(n-1)N+i}}\}$ in T_B is one or zero dimensional for all i for a $T \in S'(N)$, one can always find values for variables (ϵ's and β's) satisfying (3.28) for each of these sets. Hence one can get a pair (B, F) such that (3.27) is satisfied by substituting these values. Hence $T \in S(N)$. Hence the proof is complete. □

However for a $T \in S(N)$, if any such set of columns in T_B (i.e., the set $\{T_{col_i}, T_{col_{N+i}}, \ldots, T_{col_{(n-1)N+i}}$ $\}, \forall i)$ has only all-zero columns, then either all the β's or ϵ's corresponding to that set are completely zeros. When the β's are zeros, the ϵ's can take any of the 2^n values possible and vice versa. Hence the number of possibilities for such a set of all-zero columns is $2^{n+1} - 1$. Hence the total number of (B, F) possible for a T matrix is $(2^{n+1} - 1)^{\lambda}$, where λ, $0 \leq \lambda \leq N$ is the number of sets of columns whose all elements are all-zero columns among the sets $\{T_{col_i}, T_{col_{N+i}}, \ldots, T_{col_{(n-1)N+i}}\}, \forall i$.

Theorem 2. A length N is optimal for a linear index coding problem if and only if all the matrices in $S(N)$ have $\lambda = 0$.

Proof. proof for only if part: We need to prove that if there exists a $T \in S(N)$ whose $\lambda \neq 0$ for a particular length N, then N is not the optimal transmission length. When such a set exists, as described above, either all the β's or ϵ's corresponding to that are completely zeros. If all the ϵ are zeroes, that means that one particular transmission is not even used by any of the receivers. Else if all the β's corresponding are kept zeroes, then we transmit no message in one particular transmission. So we can remove at least one transmission. Hence the proof of only if part is complete.

The proof for if part goes as follows: We prove this by contradiction. Assume that a length N exists such that it is feasible but not optimal and all the matrices in $S(N)$ have $\lambda = 0$. Assume further that $N' = N - r$ for some $r > 0$, is the optimal length. Then take one feasible solution with length N'. Add extra nr rows to the corresponding F_B matrix and some extra nN all zero columns to B_B. Let us call the new matrices F'_B and B'_B. Let $g'_i, i = 1, \ldots N$ be the set of broadcast messages given by F'_B and g_i be those which are given by F_B. One can observe that $\{g'_1, g'_2, \ldots, g'_N\}$ is nothing but $\{g_1, g_2, \ldots, g_{N'}\}$ plus some additional information. Hence when one sends $\{g'_1, g'_2, \ldots, g'_N\}$, the receivers get whatever they would have got if $\{g_1, g_2, \ldots, g_{N'}\}$ was sent. Hence even if they do not use the extra transmissions given by F'_B, they will be able to decode their wanted messages. Hence the product of F'_B and B'_B matrices should belong to $S(N)$ (as it is a feasible index code) and has $\lambda \neq 0$, which is a contradiction. Hence c is the optimal length.

□

Example 9. *(continued).* We will illustrate Theorem 1 for the problem in Example 9. We will prove $N = 1$ is not possible in this case. We can observe that $n = 3$. Hence, from (3.26), $2^3 = 8$ matrices are there which belong to $S'(1)$. We found them by brute force among 2^{12} matrices which has zeros at places which are occupied by zeros strictly in the corresponding B_{SI}. Let us denote them by $T_1, T_2, ...T_8$. They are as given below.

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Denote by $T_{B,k}$, the matrix formed by taking the first nc columns of T_k^T and $T_{col_i,k}$ is the i-th column of $T_{B,k}$, for $k = 1, \ldots, 8$. As can be seen none of the T_k matrices satisfy the criterion of having dimension 1 or less for the sets of columns of $T_{B,k}$ (the set $\{T_{col_i,k}, T_{col_{N+i},k}, \ldots, T_{col_{(n-1)N+i,k}}\}, \forall i$). Hence, there does not exist a solution with $N = 1$.

Example 10. Let $m = n = 3$ and R_i wants x_i, $\forall i \in \{1, 2, 3\}$. R_1 knows x_2 and x_3. R_2 knows x_3. R_3 knows x_1.

The optimal value of N is 2. For $N = 1$, size of $S'(N) = 16$ (from (3.26)). The matrices $T_k,\ k = 1, \ldots, 16$ which belong to $S'(1)$ are found by brute force among 2^{13} matrices which has zeros at places, which are to be occupied strictly by zeros in the corresponding B_{SI}. They are :

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

As can be seen none of the T_k matrices satisfy the criterion of having dimension 1 for the sets of columns of $T_{B,k}$ (the set $\{T_{col_i,k}, T_{col_{N+i},k}, \ldots, T_{col_{(n-1)N+i},k}\}, \forall i$). Hence $N = 1$ is not a feasible length for this case. If $N = 3$ is taken, one would get a matrix T which belongs to the set $S(3)$, as in (3.31). For this matrix, $\lambda \neq 0$. Also dimension of every set of columns (i.e., the set $\{T_{col_i}, T_{col_{N+i}}, \ldots, T_{col_{(n-1)N+i}}\}$, $\forall i$) is 1 or 0. Hence $N = 3$ is not optimal. Therefore, $N = 2$ should be the optimal length.

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{3.31}$$

3.3 Minimum Number of Codes Possible for an Optimal N

In this section, we find the lower bound on the number of linear codes which are optimal in terms of bandwidth for a single unicast index coding problem. For the optimal N, the number of matrices which are right inverses of A^T and whose transpose is a product of some B and F gives the number of codes possible with that length, which is also the size of the set $S(N)$. But for any $T \in S(N)$,

$$A_B^T T_B^T = I - A_{SI}^T T_{SI}^T \tag{3.32}$$

$$\begin{pmatrix} \beta_{x_1,l_1} & \beta_{x_1,l_2} & \dots & \beta_{x_1,l_N} \\ \beta_{x_2,l_1} & \beta_{x_2,l_2} & \dots & \beta_{x_2,l_N} \\ . & & & \\ . & & & \\ \beta_{x_n,l_1} & \beta_{x_n,l_2} & \dots & \beta_{x_n,l_N} \end{pmatrix} \begin{pmatrix} \epsilon_{l_1,R_1} & \epsilon_{l_1,R_2} & \dots & \epsilon_{l_1,R_n} \\ . & & & \\ . & & & \\ \epsilon_{l_N,R_1} & \epsilon_{l_N,R_2} & \dots & \epsilon_{l_N,R_n} \end{pmatrix} \tag{3.33}$$

---

where LHS will be of a form as in (3.33).

Theorem 3. The number of linear index coding solutions having optimal length N for a single unicast IC problem is at-least

$$\frac{\prod_{i=0}^{N-1}(2^N - 2^i)}{N!} \tag{3.34}$$

Proof. : Consider (3.32) and (3.33). Here if both RHS of (3.32) and first matrix in (3.33) are fixed, solution which is the second matrix in (3.33) will exist only if the column space of RHS of (3.32) is spanned by the columns of first matrix in (3.33). But the rank of the first matrix in (3.33) is atmost N. Hence this is possible only if the rank of the RHS matrix in (3.32) is less than or equal to N. The number of possible T_{SI}^T matrices is $2^{\sum_{i=1}^{n}|\mathcal{K}_i|}$. As we know N is the optimal length, there should be at least one T_{SI}^T such that RHS of (3.32) is of rank N. For any such RHS of (3.32), we can take the first matrix in (3.33) in $(2^N-1)\prod_{i=1}^{N-1}(2^N-1-\binom{i}{i}-\binom{i}{i-1}.......-\binom{i}{1})$ ways such that the column spaces of both the matrices are same. Each such matrix is an index code, which is feasible, and each column of the matrix represents a transmission. As order of transmission does not matter, we need to neglect those matrices which are column-permuted versions of one another. Hence, total number of distinct transmission schemes possible is $\frac{(2^N-1)}{N!}\prod_{i=1}^{N-1}(2^N-1-\binom{i}{i}-\binom{i}{i-1}.......-\binom{i}{1}) = \frac{\prod_{i=0}^{N-1}(2^N-2^i)}{N!}$. But there may be more than one T_{SI}^T matrices which are of rank N and whose column spaces are different. Hence the total number of index codes possible can be more than (3.34) also as we take into account all possible basis sets of each of the different column spaces. Example 11 is such a case. Hence (3.34) is a lower bound on the number of index codes possible. □

Note that all possible matrices occupying RHS of (3.32) are exactly the collection of matrices which fits the index coding problem as per the definition of a fitting matrix in [2]. Hence algebraically we have proved the already established result [2] that the optimal length of a linear

$$L_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_4 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$L_5 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_6 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_7 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_8 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

$$L_9 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{10} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{11} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

$$L_{13} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{14} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_{15} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_{16} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

$$L_{17} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{18} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{19} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{20} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$L_{21} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_{22} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{23} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad L_{24} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

$$L_{25} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{26} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{27} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_{28} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

$$L_{29} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{30} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_{31} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_{32} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Table 3.1 Fitting matrices for Example 11

solution is the minimum among the ranks of all the matrices which fits the IC problem.

Corollary 1. The number of index codes possible with the optimal length N for a single unicast IC problem is given by

$$\frac{\mu \prod_{i=0}^{N-1} (2^N - 2^i)}{N!}, \tag{3.35}$$

where μ is the number of T_{SI}^T matrices out of the $2^{\sum_{i=1}^{n} |\mathcal{K}_i|}$ possible ones which give a N-rank RHS matrix of (3.32) with unique column space.

Proof. The Proof of this follows from the proof of Theorem 2. □

Note that $\mu = 1$ for Examples 9, 10 and 12.

Example 11. Let $m = n = 4$. R_i wants x_i and knows x_{i+1} where $+$ is modulo-4 operation. x_3 knows x_1 also.

The optimal length is $N = 3$. The RHS matrices of (3.32) possible for this case are as in Table 3.1. As can be seen L_5, L_{20}, L_{26} and L_{27} are of rank three. But column space of L_5 and L_{20} are same. Similarly column space of L_{26} and L_{27} are same. Hence $\mu = 2$. The number of optimal linear codes are 56 in number thus satisfying corollary 2. They are listed in Table 3.2.

Code	Encoding	r_{min}
$\mathfrak{C}_1$	$x_1 + x_2, x_2 + x_3, x_3 + x_4$	0
$\mathfrak{C}_2$	$x_1 + x_2, x_2 + x_3, x_2 + x_4$	1
$\mathfrak{C}_3$	$x_1 + x_2, x_2 + x_3, x_1 + x_2 + x_3 + x_4$	1
$\mathfrak{C}_4$	$x_1 + x_2, x_2 + x_3, x_1 + x_4$	0
$\mathfrak{C}_5$	$x_1 + x_2, x_3 + x_4, x_1 + x_3$	1
$\mathfrak{C}_6$	$x_1 + x_2, x_3 + x_4, x_2 + x_4$	1
$\mathfrak{C}_7$	$x_1 + x_2, x_3 + x_4, x_1 + x_4$	0
$\mathfrak{C}_8$	$x_1 + x_2, x_1 + x_3, x_2 + x_4$	0
$\mathfrak{C}_9$	$x_1 + x_2, x_1 + x_3, x_1 + x_2 + x_3 + x_4$	0
$\mathfrak{C}_{10}$	$x_1 + x_2, x_1 + x_3, x_1 + x_4$	1
$\mathfrak{C}_{11}$	$x_1 + x_2, x_2 + x_4, x_1 + x_2 + x_3 + x_4$	0
$\mathfrak{C}_{12}$	$x_1 + x_2, x_1 + x_2 + x_3 + x_4, x_1 + x_4$	1
$\mathfrak{C}_{13}$	$x_2 + x_3, x_3 + x_4, x_1 + x_3$	1
$\mathfrak{C}_{14}$	$x_2 + x_3, x_3 + x_4, x_1 + x_2 + x_3 + x_4$	1
$\mathfrak{C}_{15}$	$x_2 + x_3, x_3 + x_4, x_1 + x_4$	0
$\mathfrak{C}_{16}$	$x_2 + x_3, x_1 + x_3, x_2 + x_4$	0
$\mathfrak{C}_{17}$	$x_2 + x_3, x_1 + x_3, x_1 + x_2 + x_3 + x_4$	0
$\mathfrak{C}_{18}$	$x_2 + x_3, x_1 + x_3, x_1 + x_4$	1
$\mathfrak{C}_{19}$	$x_2 + x_3, x_2 + x_4, x_1 + x_2 + x_3 + x_4$	0
$\mathfrak{C}_{20}$	$x_2 + x_3, x_2 + x_4, x_1 + x_4$	1
$\mathfrak{C}_{21}$	$x_3 + x_4, x_1 + x_3, x_2 + x_4$	0
$\mathfrak{C}_{22}$	$x_3 + x_4, x_1 + x_3, x_1 + x_2 + x_3 + x_4$	0
$\mathfrak{C}_{23}$	$x_1 + x_3, x_2 + x_4, x_1 + x_4$	0
$\mathfrak{C}_{24}$	$x_1 + x_3, x_1 + x_2 + x_3 + x_4, x_1 + x_4$	0
$\mathfrak{C}_{25}$	$x_2 + x_4, x_1 + x_2 + x_3 + x_4, x_1 + x_4$	0
$\mathfrak{C}_{26}$	$x_3 + x_4, x_2 + x_4, x_1 + x_2 + x_3 + x_4$	0
$\mathfrak{C}_{27}$	$x_3 + x_4, x_2 + x_4, x_1 + x_4$	1
$\mathfrak{C}_{28}$	$x_3 + x_4, x_1 + x_2 + x_3 + x_4, x_1 + x_4$	1
$\mathfrak{C}_{29}$	$x_3 + x_2, x_2 + x_1, x_1 + x_4 + x_3$	0
$\mathfrak{C}_{30}$	$x_3 + x_2, x_2 + x_1, x_4$	1
$\mathfrak{C}_{31}$	$x_3 + x_2, x_2 + x_1, x_1 + x_4 + x_2$	1
$\mathfrak{C}_{32}$	$x_1 + x_2, x_2 + x_3, x_2 + x_4 + x_3$	1
$\mathfrak{C}_{33}$	$x_1 + x_2, x_4, x_1 + x_4 + x_3$	0
$\mathfrak{C}_{34}$	$x_1 + x_2, x_1 + x_3, x_1 + x_4 + x_3$	1
$\mathfrak{C}_{35}$	$x_1 + x_2, x_2 + x_4 + x_1, x_1 + x_4 + x_3$	0
$\mathfrak{C}_{36}$	$x_1 + x_2, x_1 + x_3, x_4$	1
$\mathfrak{C}_{37}$	$x_1 + x_2, x_4, x_2 + x_4 + x_3$	0
$\mathfrak{C}_{38}$	$x_1 + x_2, x_1 + x_3, x_1 + x_4 + x_2$	1
$\mathfrak{C}_{39}$	$x_1 + x_2, x_1 + x_3, x_2 + x_4 + x_3$	0
$\mathfrak{C}_{40}$	$x_1 + x_2, x_2 + x_3 + x_4, x_1 + x_4 + x_2$	0
$\mathfrak{C}_{41}$	$x_3 + x_2, x_4, x_1 + x_4 + x_3$	0
$\mathfrak{C}_{42}$	$x_3 + x_2, x_1 + x_3, x_1 + x_4 + x_3$	1
$\mathfrak{C}_{43}$	$x_3 + x_2, x_2 + x_3 + x_4, x_1 + x_4 + x_3$	0
$\mathfrak{C}_{44}$	$x_3 + x_2, x_1 + x_3, x_4$	1
$\mathfrak{C}_{45}$	$x_3 + x_2, x_4, x_1 + x_4 + x_2$	0
$\mathfrak{C}_{46}$	$x_3 + x_2, x_1 + x_3, x_1 + x_4 + x_2$	0
$\mathfrak{C}_{47}$	$x_3 + x_2, x_1 + x_3, x_2 + x_4 + x_3$	1
$\mathfrak{C}_{48}$	$x_3 + x_2, x_2 + x_4 + x_1, x_2 + x_4 + x_3$	0
$\mathfrak{C}_{49}$	$x_1 + x_2 + x_4, x_4, x_1 + x_4 + x_3$	1
$\mathfrak{C}_{50}$	$x_3 + x_2 + x_4, x_4, x_1 + x_4 + x_3$	1
$\mathfrak{C}_{51}$	$x_3 + x_1, x_2 + x_4 + x_1, x_1 + x_4 + x_3$	0
$\mathfrak{C}_{52}$	$x_3 + x_2 + x_4, x_2 + x_1 + x_4, x_1 + x_4 + x_3$	0
$\mathfrak{C}_{53}$	$x_3 + x_1, x_4, x_1 + x_4 + x_2$	0
$\mathfrak{C}_{54}$	$x_3 + x_1, x_4, x_2 + x_4 + x_3$	0
$\mathfrak{C}_{55}$	$x_4, x_1 + x_2 + x_4, x_1 + x_4 + x_3$	1
$\mathfrak{C}_{56}$	$x_3 + x_1, x_2 + x_3 + x_4, x_1 + x_4 + x_3$	0

Table 3.2 Optimal linear solutions for Example 11.

$$\begin{bmatrix} 1 & 0 & 0 & \dots & p_{1,\{j:\mathcal{K}_j=x_1\}} & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & p_{2,\{j':\mathcal{K}_{j'}=x_2\}} & 0 & \dots & 0 \\ . & & & & & & & \\ . & & & & & & & \\ 0 & 0 & 0 & \dots & p_{n,\{j'':\mathcal{K}_{j''}=x_n\}} & 0 & \dots & 1 \end{bmatrix} \tag{3.36}$$

$$L_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_4 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$L_5 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_6 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_7 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_8 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

$$L_9 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{10} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{11} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

$$L_{13} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad L_{14} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_{15} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad L_{16} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Table 3.3 Fitting matrices for Example 12

Corollary 2. The bound in Theorem 2 is satisfied with equality by a single unicast single uniprior problem.

Proof. : For a single unicast single uniprior problem the RHS of (3.32) will be of the form (3.36), where all $p_{i,\{j:\mathcal{K}_j=x_i\}}$ for $i = 1, \dots, n$ can be 1 or 0. Hence total number of matrices that can be of the form (3.36) is 2^n. As can be verified only one matrix among them has rank equal to $n-1$, which is the optimal transmission length for this single unicast problem and that one matrix is that whose all $p_{i,\{j:\mathcal{K}_j=x_i\}}$ values are one. We will prove this by contradiction. Suppose any other matrix exists with atleast one $x_{i,j}$ zero and is of rank $n-1$, it means that receiver R_j does not use its side information x_i. This is equivalent to the case where R_j does not have any prior information. For this case, the optimal length of transmission is n, which is a contradiction. Hence the number of optimal index codes is exactly what is given by (3.34). □

Example 9. was a single unicast single uniprior problem. The optimal length is $N = 2$ and three solutions are possible with that length, satisfying Corollary 2.

Example 12. Let $m = n = 4$. R_i wants x_i and knows x_{i+1}, where + is modulo-4 addition.

Here all possible matrices of the form (3.36) denoted by L_i, $i = 1, \dots, 16$ are as in Table 3.3. Only L_5 has dimension four. The set of all optimal index codes is given by the collection of all

Code	Encoding
$\mathfrak{C}_1$	$x_1+x_2, x_2+x_3, x_3+x_4$
$\mathfrak{C}_2$	$x_1+x_2, x_2+x_3, x_2+x_4$
$\mathfrak{C}_3$	$x_1+x_2, x_2+x_3, x_1+x_2+x_3+x_4$
$\mathfrak{C}_4$	$x_1+x_2, x_2+x_3, x_1+x_4$
$\mathfrak{C}_5$	$x_1+x_2, x_3+x_4, x_1+x_3$
$\mathfrak{C}_6$	$x_1+x_2, x_3+x_4, x_2+x_4$
$\mathfrak{C}_7$	$x_1+x_2, x_3+x_4, x_1+x_4$
$\mathfrak{C}_8$	$x_1+x_2, x_1+x_3, x_2+x_4$
$\mathfrak{C}_9$	$x_1+x_2, x_1+x_3, x_1+x_2+x_3+x_4$
$\mathfrak{C}_{10}$	$x_1+x_2, x_1+x_3, x_1+x_4$
$\mathfrak{C}_{11}$	$x_1+x_2, x_2+x_4, x_1+x_2+x_3+x_4$
$\mathfrak{C}_{12}$	$x_1+x_2, x_1+x_2+x_3+x_4, x_1+x_4$
$\mathfrak{C}_{13}$	$x_2+x_3, x_3+x_4, x_1+x_3$
$\mathfrak{C}_{14}$	$x_2+x_3, x_3+x_4, x_1+x_2+x_3+x_4$
$\mathfrak{C}_{15}$	$x_2+x_3, x_3+x_4, x_1+x_4$
$\mathfrak{C}_{16}$	$x_2+x_3, x_1+x_3, x_2+x_4$
$\mathfrak{C}_{17}$	$x_2+x_3, x_1+x_3, x_1+x_2+x_3+x_4$
$\mathfrak{C}_{18}$	$x_2+x_3, x_1+x_3, x_1+x_4$
$\mathfrak{C}_{19}$	$x_2+x_3, x_2+x_4, x_1+x_2+x_3+x_4$
$\mathfrak{C}_{20}$	$x_2+x_3, x_2+x_4, x_1+x_4$
$\mathfrak{C}_{21}$	$x_3+x_4, x_1+x_3, x_2+x_4$
$\mathfrak{C}_{22}$	$x_3+x_4, x_1+x_3, x_1+x_2+x_3+x_4$
$\mathfrak{C}_{23}$	$x_1+x_3, x_2+x_4, x_1+x_4$
$\mathfrak{C}_{24}$	$x_1+x_3, x_1+x_2+x_3+x_4, x_1+x_4$
$\mathfrak{C}_{25}$	$x_2+x_4, x_1+x_2+x_3+x_4, x_1+x_4$
$\mathfrak{C}_{26}$	$x_3+x_4, x_2+x_4, x_1+x_2+x_3+x_4$
$\mathfrak{C}_{27}$	$x_3+x_4, x_2+x_4, x_1+x_4$
$\mathfrak{C}_{28}$	$x_3+x_4, x_1+x_2+x_3+x_4, x_1+x_4$

Table 3.4 All possible optimal linear solutions for Example 12.

possible basis of the column space of this matrix. They are 28 in number. Hence Corollary 2 is satisfied. We list out those codes in Table 3.4.

3.4 Optimal Codes with Minimum-Maximum Error Probability

As seen in the last section, there can be several linear optimal solutions in terms of least bandwidth for an IC problem but among them we try to identify the index code which minimizes the maximum number of transmissions that is required by any receiver in decoding its desired message. The motivation for this is that each of the transmitted symbols is error prone and the lesser the number of transmissions used for decoding the desired message, lesser will be its probability of error. Hence among all the codes with the same length of transmission, the one for which the maximum number of transmissions used by any receiver is the minimum, will have minimum-maximum error probability. We give a method to find the best linear solution in terms of minimum-maximum error probability among all codes with the optimal length N. For a $T \in S(N)$, if we take a row say,$[r_1 r_2 .....r_{nN}]$, $r_i \in \{1, 0\}$, of the corresponding sub-matrix T_B (formed by taking the first nN columns of its transpose), we define r_{sum} for the row as follows:

$$r_{sum} = \sum_{i=1}^{N} (I_{r_i=0} I_{r_{N+i}=0} ... I_{r_{(n-1)N+i}=0}) \tag{3.37}$$

where I_z is the indicator function which is one when event z occurs. Also, we define r_{min} for a $T \in S(N)$ as the minimum among the row-sums of all the rows of the sub-matrix T_B (formed by taking the first nN columns of its transpose).

Theorem 4. For the optimal length N, that matrix in $S(N)$ whose r_{min} is the maximum, is the one which gives the IC with the minimum-maximum error probability. Also,the matrix formed by taking every n-th row of the corresponding F_B matrix is the optimal linear solution in terms of minimum-maximum error probability using N number of transmissions.

Proof. The number of transmissions used by i-th receiver is given by the number of non-zero entries in i-th row of B_B. When for example t-th ϵ element in the i-th row of B_B is zero, the i-th element of every $(t+(k-1)N)$-th column for $k = 1$ to n, in T_B turns 0. Hence the number of transmissions unused by it is proportional to the r_{min} of the i-th row. Therefore, our claim is proved. Moreover F_B is the matrix which decides the message flowing in the broadcast channels. So the matrix formed by taking every n-th row of F_B is the corresponding Index code . □

Now, consider there is a priority among different users indicated by weights, $w_1, w_2 ... w_n$. Let the number of transmissions used by receiver R_i to decode its wanted message be t_i. We assume the cost paid due to user R_i is $t_i w_i$. Our aim is to minimize the total cost paid due to all the users for the optimal length c. Then we would take the T matrix in $S(N)$ for which $\sum_{i=1}^{n} r_{sum,i} w_i$ is the maximum, where $r_{sum,i}$ is the row sum of i-th row of the corresponding T_B matrix.

For Example 9, we found out the optimal IC's : They are 1. $\mathfrak{C}_1 : x_1 \oplus x_2,\ x_2 \oplus x_3$ 2. $\mathfrak{C}_2 : x_1 \oplus x_3,\ x_3 \oplus x_2$ 3. $\mathfrak{C}_3 : x_1 \oplus x_3,\ x_1 \oplus x_2$. For all the three, the maximum number of transmissions used by any receiver is 2. This is verified below. We find the T_B matrices for each case as follows:

$$T_{B,1} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$T_{B,2} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$T_{B,3} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Minimum row sum for all the three is 0. Hence 2 transmissions at most are used by any receiver to decode in all the three cases. The BEP (Bit Error Probability) versus SNR curves for each of the three codes at various receivers are given in Fig.3.3, Fig. 3.4, Fig. 3.5. We considered BPSK modulation in rayleigh faded channel. In Fig.3.6, the worst case BEP curves for each of the three codes are plotted. We can see that the curves lie on top of each other which proves our claim that all the three codes are equally good in terms of minimum-maximum error probability.

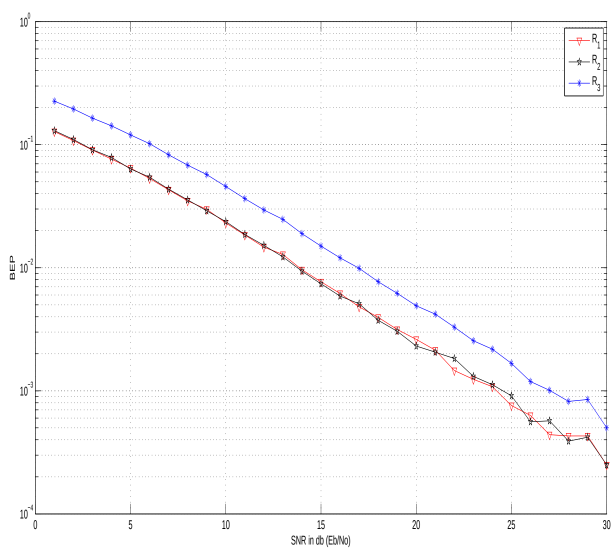


Fig. 3.3 BER versus SNR (db) curve for $\mathfrak{C}_1$ at all the receivers for Example 9.

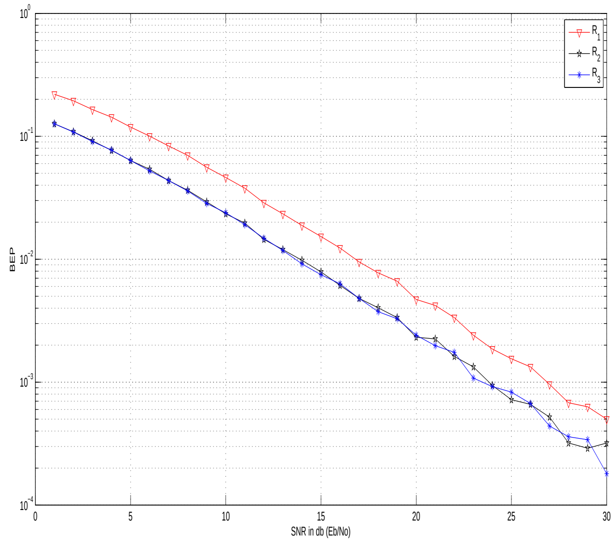


Fig. 3.4 BER versus SNR (db) curve for $\mathfrak{C}_2$ at all the receivers for Example 9.

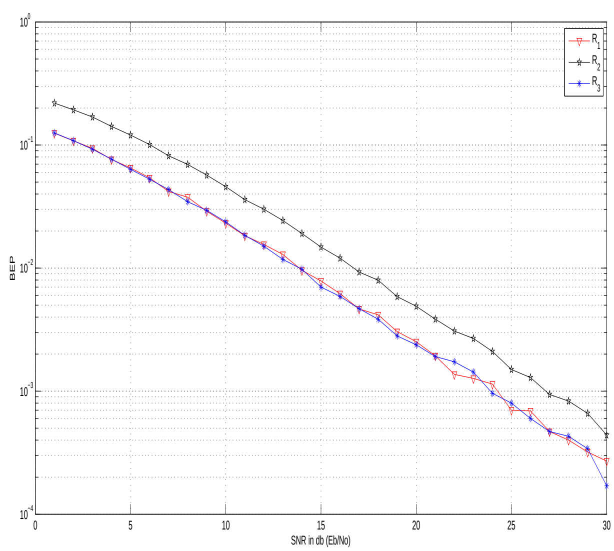


Fig. 3.5 BER versus SNR (db) curve for $\mathfrak{C}_3$ at all the receivers for Example 9.

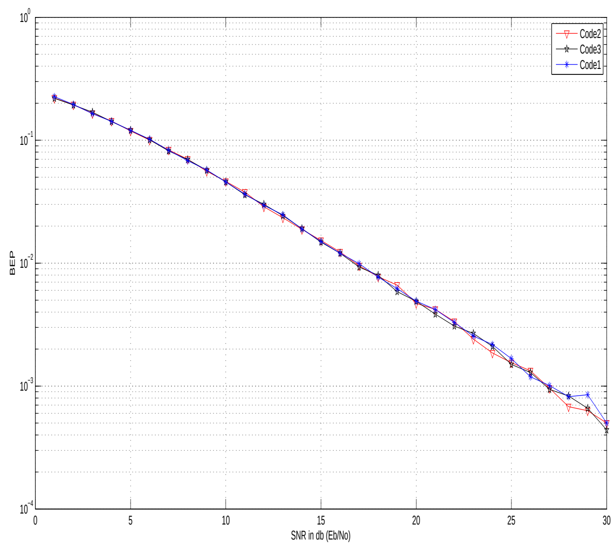


Fig. 3.6 Worst case BER versus SNR (db) curves for each of the three codes for Example 9.

For Example 11, Table 3.2 gives the r_{min} for each of the optimal linear codes. The maximum r_{min} is 1. The BER versus SNR curve for $\mathfrak{C}_{30}$ whose $r_{min} = 1$ is as in Fig .3.7. The BER versus SNR curve for $\mathfrak{C}_{29}$ whose $r_{min} = 0$ is as in Fig .3.8. The worst case Performance of both codes are plotted in Fig. 3.9.

We can observe that the worst performance of $\mathfrak{C}_{30}$ is better than worst performance of $\mathfrak{C}_{29}$.

3.5 Results and Discussion

For an optimal N, the maximum number of index codes possible is bounded by 2^{nN}. In this chapter we have given a lower bound also. [3]. This lower bound is satisfied with equality for a single unicast problem in which $\mid \mathcal{K}_i \mid = 1$ and $\mathcal{K}_i \cap \mathcal{K}_j$=0, for $i \neq j, i, j = 1$ to n . We would like to extend this work to find out least complexity algorithms which finds IC solutions by matrix completion. Harvey *et. all* in [11] gives such algorithms for multicast network codes. However what we have is a general problem and hence their results are not applicable. We have followed an approach which is different and simpler than Koetter and medard's [6] for this specific class of network coding problem.

[3]A Part of this work appears in *Proc. ISIT'2015*, Wanchai, Hong Kong, June, 2015.

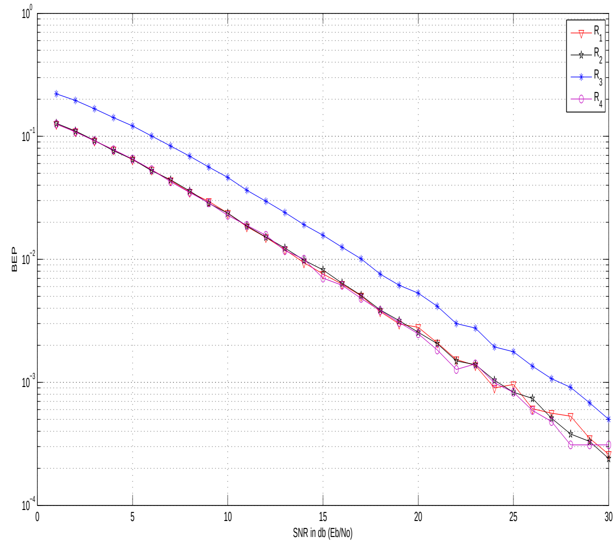


Fig. 3.7 BER versus SNR (db) curve for $\mathfrak{C}_{30}$ at all the receivers for Example 11

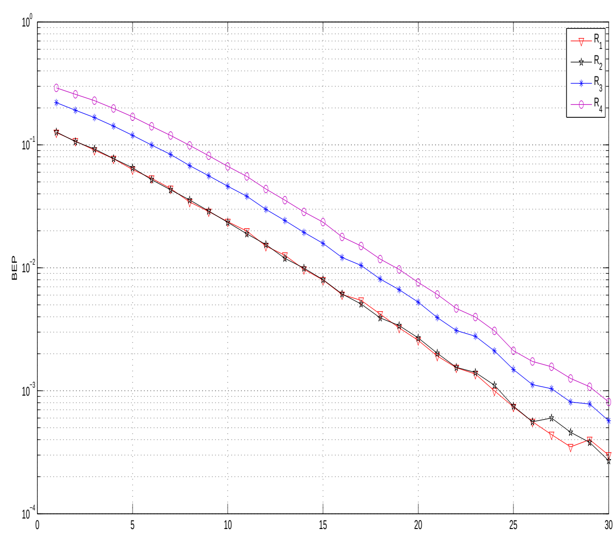


Fig. 3.8 BER versus SNR (db) curve for $\mathfrak{C}_{29}$ at all the receivers for Example 11

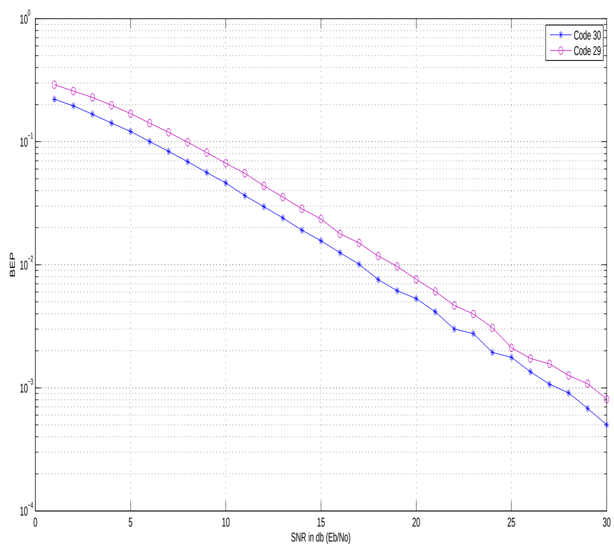


Fig. 3.9 Worst case BER versus SNR (db) curves for codes $\mathfrak{C}_{30}$ and $\mathfrak{C}_{29}$ for Example 11

Chapter 4

Index Coding with Restricted Information

A general index coding problem can be formulated as follows: There is a source with n messages, $X = \{x_1, x_2, \ldots, x_n\}$ and m receivers. Each receiver is specified by $\{\mathcal{W}_i, \mathcal{K}_i\}$ where $\mathcal{W}_i$ is the set of wanted messages and $\mathcal{K}_i$ is the set of known messages. For any positive integer n, $\lceil n \rfloor$ denotes the set of integers 1 to n. An index coding scheme is a coding scheme which ensures that the demands of all receivers are satisfied. The special case of index coding problem with restricted side information i.e, each receiver $\{\mathcal{W}_i, \mathcal{K}_i\}$ has a message set $\mathcal{N}_i$ out of which it is not supposed to receive any, is considered. In this case, we need a coding scheme which not only satisfies the demands of all receivers but also ensures that no receiver decodes any of the messages from the restricted set assigned to it.

Definition 2. A linear $(\mathbb{F}, N, \mathcal{R})$ index coding scheme [17] achieving a rate $\mathcal{R} = (\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_n)$, where $\mathcal{R}_i = \frac{L_i}{N}, \forall i \in K$ over N channel uses, corresponds to a choice of

1. a finite field $\mathbb{F}$ as the alphabet

2. $V_i \in \mathbb{F}^{N \times L_i}, \forall i \in \lceil n \rfloor$ as pre-coding matrices.

3.$D_{i,k} \in \mathbb{F}^{L_i \times N}, \forall i \in \lceil n \rfloor, \forall k \in \lceil m \rfloor$ such that $x_i \in \mathcal{W}_k$, as receiver combining matrices such that the following properties are satisfied.

Property 1: $D_{i,k} V_j = 0, \forall i, j \in \lceil n \rfloor, k \in \lceil m \rfloor$ such that $i \neq j, x_i \in \mathcal{W}_k, x_j \notin \mathcal{A}_k$

Property 2: $\det(D_{i,k} V_i) \neq 0, \forall i \in \lceil n \rfloor, k \in \lceil m \rfloor$ such that $x_i \in \mathcal{W}_k$.

where all operation are over $\mathbb{F}$.

The source transmits

$$Y = \sum_{i=1}^{n} V_i \mathcal{X}_i \tag{4.1}$$

where $\mathcal{X}_i = \{x_{i,1}, x_{i,2}, \ldots, x_{i,L_i}\}^T \in \mathbb{F}^{L_i \times 1}$ is an $L_i \times 1$ vector representing x_i i.e, message x_i is split into L_i independent scalar schemes, each of which carries one symbol from $\mathbb{F}$ and is transmitted along the corresponding column vectors of the pre-coding matrix V_i. The decoding operation [17] done at k-th receiver for message $\mathcal{X}_i \in \mathcal{W}_k$ is

$$\widehat{\mathcal{X}_i} = (D_{i,k}V_i)^{-1} D_{i,k}(Y - \sum_{x_j \in \mathcal{K}_k} \mathcal{X}_j V_j) \tag{4.2}$$

Hence if there is a restricted information $x_i \in \mathcal{N}_k$ for k-th receiver, a linear index coding scheme satisfying Definition 1 is a feasible solution iff there exists no such $U_{i,k}$ satisfying properties 1 and 2 for x_i. It is because if it is not so, $x_i \in \mathcal{N}_k$ can be resolved at k-th receiver. When $L_i = 1, \forall i \in \lceil n \rfloor$, the solution is called a scalar linear index coding scheme. Now some relevant terms mentioned in [17] is introduced.

Alignment relation [17]: A relation $x_i \overset{k}{\leftrightarrow} x_j$ is defined iff $x_i \notin \mathcal{K}_k, x_i \notin \mathcal{W}_k, x_j \notin \mathcal{K}_k$ and $x_j \notin \mathcal{W}_k$ for $k \in \lceil m \rfloor$ and distinct indices $i, j \in \lceil n \rfloor$. Occasionally notation $x_i \leftrightarrow x_j$ is used when the identity of the destination is not important.

Alignment Subsets [17]: The set of messages X is partitioned into alignment subsets , created as follows. If $x_i \leftrightarrow x_j$, then both x_i, x_j belong to the same alignment subset. Further, if $x_i \leftrightarrow x_j$ and $x_j \leftrightarrow x_k$ then x_i, x_j, x_k all belong to the same alignment subset for $i, j, k \in \lceil n \rfloor$.

4.1 Achievability of rate $\frac{1}{L+1}$

Theorem 3 in [17] is extended as below.

Theorem 5. A Rate $\frac{1}{L+1}$ is possible for $| \mathcal{W}_i |= L, \forall i \in \lceil m \rfloor$ if and only if the following conditions are satisfied: 1. There does not exist distinct indices $i, j \in \lceil n \rfloor$ such that x_i, x_j belong to the same alignment subset and $x_j \in \mathcal{W}_k$ and $x_i \notin \mathcal{K}_k$ for $k \in \lceil m \rfloor$ [17]. 2.$| (\mathcal{K}_k \cup \mathcal{W}_k)^c |> 1, \forall k \in \lceil m \rfloor$ such that $\mathcal{N}_k \neq \phi$.

Proof. Proof of if part : Assume that both the conditions are satisfied. Partition $X = \{x_1, x_2, \ldots, x_n\}$ into alignment subsets $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_T$, and define the mapping $P(m) : X \to \{1, 2, \ldots, T\}$ so that $x_m \in \mathcal{P}_{P(m)}, \forall m \in \lceil n \rfloor$. Choose q sufficiently large such that there exist T vectors $V_1, V_2, \ldots V_T$, in the $L+1$ dimensional vector space over $\mathbb{F}_q$ such that every $L+1$ of them is linearly independent. These are the coding vectors along which the aligned messages from each partition will be sent. Consider k-th receiver. Denote its want set by $\mathcal{K}_k = \{x_{k_1}, x_{k_2}, \ldots, x_{k_L}\}$. It receives

$$Y = \sum_{i=1}^{n} A_i V_{p(i)} \tag{4.3}$$

$$= \sum_{i=1}^{L} A_{k_i} V_{P(k_i)} + \sum_{i:x_i \in \mathcal{K}_k} A_i V_i + (\sum_{i:x_i \notin \mathcal{K}_k \cup \mathcal{W}_k} A_i) V_{\mathcal{P}_t} \tag{4.4}$$

The last term follows since all those messages which are not in the demand set or prior set of the receiver belongs to the same alignment subset denoted by $\mathcal{P}_t$ (else condition 1 not satisfied). The second term can be cancelled by the receiver since it knows the corresponding messages. Hence one gets a linear combination of $L+1$ vectors which are independent (because of the way by which they are chosen). Hence one can resolve $x_{k_1}, \ldots, x_{k_L}$. Also all $x_i \in \mathcal{N}_k$ are along the vector $V_{\mathcal{P}(t)}$, which is of dimension one. But since $\mid (\mathcal{K}_k \cup \mathcal{W}_k)^c \mid > 1$, it cannot be resolved . Hence proof of if part is complete.

Proof of only if part: The necessity of property 1 to hold for the rate to be achievable is already proved as Theorem 3 in [17]. The necessity of property 2 can be argued as follows. Consider $N = L+1$. Then for the messages in the want set to be resolvable, they should consume a fraction $\frac{L}{L+1}$ of the total capacity. Hence the remaining interfering messages should consume only $\frac{1}{L+1}$ of the total capacity. But each such message has rate $\frac{1}{L+1}$. The restricted messages also falls in this category. Hence it can be resolved if $\mid (\mathcal{K}_k \cup \mathcal{W}_k)^c \mid = 1$. Hence the proof is complete.

□

If all receivers have size of the restricted message set greater than 1, then only condition 1 in Theorem 1 needs to be satisfied for the rate $\frac{1}{L+1}$ to be achievable.

Upper-bound on $q_{max,\frac{1}{2}}$

Note that in the proof of the if-part of the Theorem 5, it was mentioned that for sufficiently large field size there exist T vectors $V_1, V_2, \ldots V_T$, in the $L+1$ dimensional vector space over $\mathbb{F}_q$ such that every $L+1$ of them is linearly independent. Define $q_{max,\frac{1}{L+1}}$ as the largest field size for which solution with rate $\frac{1}{L+1}$ does not exist for an index coding problem. Note that if condition 1 and 2 are not satisfied $q_{max,\frac{1}{L+1}}$ is not defined. When both are satisfied, an upper bound on $q_{max,\frac{1}{L+1}}$ is found in this work. Before explaining that, some relevant definitions from matroid theory should be mentioned.

A matroid $\mathcal{M}$ is an ordered pair $(\mathcal{E}, \mathcal{I})$ consisting of a finite set $\mathcal{E}$ and a collection $\mathcal{I}$ of subsets of $\mathcal{E}$ satisfying the following three conditions:

(I1)$\emptyset \in \mathcal{I}$

(I2) If $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$.

(I3) If I_1 and I_2 are in $\mathcal{I}$ and $|I_1| < |I_1|$, then there exists an element e of $I_2 - I_1$ such that $I_1 \bigcup e \in \mathcal{I}$.

Members of $\mathcal{I}$ are the independent sets of $\mathcal{M}$ and $\mathcal{E}$ is the ground set of $\mathcal{M}$. The notations $\mathcal{E}(\mathcal{M})$ and $\mathcal{I}(\mathcal{M})$ are used for $\mathcal{E}$ and $\mathcal{I}$ respectively. A subset of $\mathcal{E}$ that is not there in $\mathcal{I}$ is called dependent. The rank function of a matroid $\rho : 2^{\lceil \mathcal{E} \rfloor} \to \mathbb{Z}_{\geq 0}$ is defined as $\rho(m') = \max\{|m''| : m'' \subseteq m', m'' \in \mathcal{I}\}$, where $m' \subseteq \lceil \mathcal{E} \rfloor$. The rank of the matroid $\mathcal{M}$ denoted by $rank(\mathcal{M})$ is equal to $\rho(\lceil \mathcal{E} \rfloor)$. Rank of a matroid $\mathcal{M}$ is also equal to the size of largest independent set in $\mathcal{I}(\mathcal{M})$.

Proposition 1.1.1 [**8**] Let $\mathcal{E}$ be the set of column labels of an $c \times d$ matrix A over a field $\mathbb{F}$ and let $\mathcal{I}$ be the set of subsets S of $\mathcal{E}$ for which the multiset of columns labelled by S is linearly independent in the vector space $V(c, \mathbb{F})$. Then $(\mathcal{E}, \mathcal{I})$ is a matroid. The matroid obtained as explained from a matrix is called vector matroid.

Two matroids $\mathcal{M}_1$ and $\mathcal{M}_2$ are isomorphic, written $\mathcal{M}_1 \cong \mathcal{M}_2$, if there is a bijection ψ from $\mathcal{E}(\mathcal{M}_1)$ to $\mathcal{E}(\mathcal{M}_2)$ such that, for all $S \subseteq \mathcal{E}(\mathcal{M}_1)$, $\psi(S)$ is independent in $\mathcal{M}_2$ if and only if S is independent in $\mathcal{M}_1$. If a matroid $\mathcal{M}$ is isomorphic to the vector matroid of a matrix A over a field $\mathbb{F}$, then $\mathcal{M}$ is said to be $\mathbb{F}$-representable.

A matroid $\mathcal{M}$ is said to be multi-linearly representable of dimension c over $\mathbb{F}$ if there exists vector subspaces $V_1, V_2, \ldots, V_r$ of a vector space V over $\mathbb{F}$ such that $\dim(\sum_{i \in m'} V_i) = c\rho(m'), \forall m' \subseteq \lceil \mathcal{E} \rfloor$. Note that a matroid $\mathcal{M}$ is said to be $\mathbb{F}$-representable if it is multi-linearly representable of dimension 1 over $\mathbb{F}$.

Let c and d be non-negative integers such that $c \leq d$ and $\mathcal{E}$ be a d-element set and $\mathcal{I}$ be the collection of all subsets of $\mathcal{E}$ which are of cardinality less than or equal to c. Then $(\mathcal{E}, \mathcal{I})$ is a matroid denoted by $U_{c,d}$ and is called uniform matroid of rank c on an d-element set.

Theorem 6. Whenever rate $\frac{1}{L+1}$ is feasible (i.e., Theorem 5 is satisfied), it is achieved over a finite field $\mathbb{F}$ if uniform matroid $U_{L+1,T}$ is multi-linearly representable of some dimension c, $c \in \mathbb{Z}_{\geq 0}$ over $\mathbb{F}$.

Proof. In the achievablity scheme, there is a mapping from each alignment subset to an $\frac{N}{L+1}$ dimensional subspace of a N dimensional space such that every set of $L+1$ subspaces are non-intersecting. This is because the alignment subsets of L demanded messages and the alignment subset of interfering messages of any receiver should be assigned non-intersecting subspaces. So, every receiver might want a certain set of $L+1$ alignment subsets to be assigned non-intersecting subspaces. By making sure that every set of $L+1$ subspaces are non-intersecting, we take into account all possible receivers. So any set of $L+1$ or less alignment subsets should be independent as the subspaces assigned to them are non-intersecting. Hence the alignment subsets $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_T$, form the ground set of the uniform matroid $U_{L+1,T}$. Hence we can find mapping from each alignment subset to an $\frac{N}{L+1}$ dimensional subspace of a N dimensional space over $\mathbb{F}$ such that every set of $L+1$ subspaces are non-intersecting iff $U_{L+1,T}$ is multi-linearly representable of some dimension over $\mathbb{F}$.
Note that there can be cases where no receiver might want some particular sets of $L+1$ alignments subsets to be non-intersecting. Hence even if $U_{L+1,T}$ is not multi-linearly representable of some dimension over $\mathbb{F}$, a coding scheme with rate $\frac{1}{L+1}$ can still exist over $\mathbb{F}$.

□

We state Theorem 6.5.21 in [8] as below:

Theorem 7. [8] Let q be a power of prime p. When $2 \leq c \leq p$, the matroid $U_{c,d}$ is GF(q)-representable if and only if $d \leq q+1$.

Corollary 3. From above theorem, $q_{max,\frac{1}{L+1}} \leq \min(|\mathbb{F}| : (L+1) \leq char(\mathbb{F})\ \&\ (T-1) \leq |\mathbb{F}|)$ where $char(\mathbb{F})$ denotes the characteristic of the field $\mathbb{F}$.

Hence for $L = 1$ rate $\frac{1}{2}$ is achievable over any field $\mathbb{F}$ if $|\mathbb{F}| \geq (T-1)$.

Finding the optimal number of alignment subsets is a NP-hard problem. As stated in [17], two alignment subsets can be combined if there does not exist a message in either subset that cannot be aligned with a message in the other subset. Two messages cannot be aligned if one of them is desired at any destination that does not have the other message as an prior message. Let T_{min} denotes the minimum number of alignment subsets possible without affecting the alignment constraints.

Theorem 8. When $L = 1$, rate= $\frac{1}{2}$ is possible through a scalar linear coding scheme over finite field $\mathbb{F}$ iff $\mathbb{F} \geq T_{min} - 1$.

Proof. When the number of alignment subsets is optimal, ie, T_{min}, there exists atleast one receiver which wants any two alignment subsets to have non-intersecting subspaces as else they could have been combined together and T_{min} will not be optimal. Since we consider scalar index coding schemes alone, this means we need T_{min} vectors in 2-dimensional space over $\mathbb{F}$ such that any two of them are orthogonal. This is possible iff $U_{2,T_{min}}$ is $\mathbb{F}$-representable. But $U_{2,T}$ is $\mathbb{F}$-representable iff $\mathbb{F} \geq T_{min} - 1$ by Theorem 7. □

4.2 Capacity of Special Classes of Index Coding Problem with Restricted Information

The linear coding capacity of a index coding setting is defined as the maximum achievable rate over all finite fields and over all linear coding schemes. We find the linear index coding capacity of some special settings (which have been already examined in [17]) after adding an extra notion of restricted information. We examine how the capacities change in the new scenario. Theorem 5 in [17] is extended as given below.

Theorem 9. The linear capacity of an index coding problem with $m = n < \infty$ (all subscripts modulo n), $\mathcal{W}_k = x_k, \mathcal{K}_k = \{x_{k-u}, x_{k-u+1}, \ldots, x_{k-1}\} \cup \{x_{k+1}, x_{k+2}, \ldots, x_{k+t}\}$and u, t are non-negative integers, $0 \leq u \leq t$, $u + t = a < n$ is

$$C = \begin{cases} 0, & \text{if u=0 or a=n-2} \\ 1, & \text{else if a=n-1} \\ \frac{u+1}{n-a+2u}, & \text{else} \end{cases} \tag{4.5}$$

Proof. The proof for cases when $u \neq 0$ and $a \neq n-2$ will be explained first: Clearly the capacities mentioned are a upper bound since these are the capacities for the case with no restricted information. We consider finite field $\mathbb{F}_q$ having sufficiently large field size q. When $a = n-1$, $\mathcal{N}_i = \Phi, \forall i$. Hence the transmitted code is the sum of all the messages in the message set. Each receiver will be able to retrieve its wanted message by subtracting all other messages. When $a < n-1$, the achievable scheme is as follows[17]: Each message is sent through $u+1$ scalar symbols over a $u+1$ dimensional space. Adjacent messages overlap in u dimensions. Hence, the total number of dimensions occupied by the $n-a-1$ interfering messages is $n-a-1+u$. Hence the total number of channel uses is $u+1+n-a-1+u = n-a+2u$. Also, all the other messages other than what is in want set and prior set will be overlapping due to which the restricted information cannot be received.

When $u = 0$, assume each message is sent through l scalars over a l-dimensional space for some $l \geq 1$. For a receiver there are $n-a-1$ interfering messages. At the most they occupy a space of dimension $(n-a-1)l$. If they occupy a space of dimension $(n-a-1)l$, each message in the interfering set can also be retrieved by any receiver, which means every receiver decodes its restricted message also. So they should never occupy a space of dimension $(n-a-1)l$. But as can be verified due to the cyclic nature of the prior set, for any dimension less than $(n-a-1)l$, another receiver who wants some message in the interfering set will not be able to decode it. Hence solution does not exist. Hence capacity is 0. When $a = n-2$, if the wanted message spans one dimension, there is only one interfering message which should span another dimension. Hence the restricted message can be recovered. Hence the capacity is 0. □

Theorem 6 in [17] is extended as given below.

Theorem 10. The linear capacity of the index coding problem associated with $n = m = \infty$, $\mathcal{W}_k = x_k$, $\mathcal{K}_k = \{x^c_{k-u,k-u+1,\ldots,k-1,k+1,k+2,\ldots,k+t}\}$, $\mathcal{N}_k \subseteq \{x_{k-u,k-u+1,\ldots,k-1,k+1,k+2,\ldots,k+t}\}, \forall k \in \lceil m \rfloor$ and $u, t \in Z$, $0 \leq u \leq t$ is $C = \frac{1}{t+1}$ per message if $\mathcal{N}_k \subseteq \{x_{k-u,k-u+1,\ldots,k-1,k+t-(u-1),k+t-u+2,\ldots,k+t}\}, \forall k \in$

$\lceil m \rfloor$ and 0 else.

Proof. For $\mathcal{N}_k \subseteq \{x_{k-u,k-u+1,\ldots,k-1,k+t-(u-1),k+t-u+2,\ldots,k+t}\}, \forall k \in \lceil m \rfloor$: This is an upper bound on the capacity because this is the capacity when $\mathcal{N}_k = \{\phi\}, \forall k \in \lceil m \rfloor$[17]. When $\mathcal{N}_k \neq \{\phi\}$ for some $k \in \lceil m \rfloor$, the achievable scheme is same as that in [17]. How it is an achievable scheme in this case also is explained as follows: Our operations are over finite field $\mathbb{F}_2$. We consider a scalar index coding scheme where each message is sent through one scalar symbol over a $t+1$ dimensional signal space . We align u messages before each desired message with the last u messages among t messages after that desired message. Hence the total number of dimensions occupied by the interfering messages is t. Also since $\mathcal{N}_k \subseteq \{x_{k-u,k-u+1,\ldots,k-1,k+t-(u-1),k+t-u+2,\ldots,k+t}\}, \forall k \in \lceil m \rfloor$, it is overlapping with one another message in the same set. Hence it cannot be retrieved.

For other cases: Consider $\{x_{k+1\ldots,k+t-u}\}$ for some $k \in \lceil m \rfloor$. Any message in this set falls as an interference for all receivers indexed by the set $\{k-u,\ldots,k-1\}$. Also they interfere with each other when any receiver which wants any of them tries to decode it. Hence the dimension occupied by the messages in the set $x_{k-u,k-u+1,\ldots,k-1,k+1,k+2,\ldots k+t-u}$ should be T atleast. The messages $x_{k+t-(u-1),k+t-u+2,\ldots,k+t}$should not align with $x_{k+1,k+2,\ldots k+t-u}$as any other receiver who wants messages in this set cannot retrieve them. Hence k-th receiver would be able to retrieve some message in $\mathcal{N}_k$ if $\mathcal{N}_k \bigcap \{x_{k+1\ldots,k+t-u}\} \neq \phi$, which is undesirable. Hence no linear solution exists. So capacity is 0. □

Theorem 7 in [17] is extended as given below.

Theorem 11. The linear capacity of a symmetric index coding problem with $n = ml$ and $n, m \longrightarrow \infty$, where $n, m, l \in Z$ and $\mathcal{W}_k = \{x_{kl,kl+l-1,(k+1)l+l-2,\ldots,(k+i)l+l-i-1,\ldots,(k+l-2)l+1}\}$,
$K_k = \{x_{k-1)l+1:(k-1)l+l-1,\ldots,(k+i)l+1:(k+i)l+l-i-2,(k+i)l+l-i:(k+i)l+l,\ldots,(k+l-2)l+2:(k+l-2)l+l} \cup x_k\}^c$ and $\mathcal{N}_k \subseteq X \setminus \{\mathcal{W}_k \cup \mathcal{K}_k\}, \forall k \in \lceil n \rfloor$ is $C = \frac{2}{l(l+1)}$ per message.

Proof. The above rate is an outer bound because it is the capacity when there is no notion of restricted information which is proved as Theorem 7 in [17]. The achievable scheme is same as what is mentioned in [17]. This scheme works for the new case also because for k-th receiver, for any message in its interfering set one can find another message in the set $X \setminus \{\mathcal{W}_k \cup \mathcal{K}_k\}$ which is aligned in the same dimension. Hence the receiver cannot decode any of its interfering messages. □

4.3 Some special settings with $N_i = \phi, \forall i \in \lceil m \rfloor$

Theorem 12. The capacity of the index coding problem associated with $n = m = \infty$, $\mathcal{W}_k = x_k$, $\mathcal{K}_k = \{x^c_{k-u,k-u+1,\ldots,k-m',k+m',k+2,\ldots,k+t}\}$, is $C = \frac{m'}{t+m'}$ per message.

Proof. Achievability scheme: We give a vector linear encoding scheme where each message is sent through m' symbols. We consider the $t+m'$ dimensional space $\mathbb{F}_2^{t+m'}$. We take $t+m'$ independent vectors, denoted by $V_1, V_2, \ldots, V_{t+m'}$. Take an arbitrary message x_i and assign $V_1, \ldots V_{m'}$ as the beam-forming vectors for the m' symbols comprising that message. To the next message x_{i+1} assign $V_2, \ldots\ldots V_{m'+1}$. Like that align the vectors such that adjacent messages overlap over $m'-1$ dimensions. Also, the assignment is periodic with period $t+m'$. As can be seen x_i can be recovered by i-th receiver as the same vectors are assigned to other messages in the known set alone.

Proof of upper bound: We define α_j as follows where S^N denotes the N transmitted messages.

$$\alpha_j \triangleq \sum_{i=1}^{n} H(S^N | x^c_{i,i+1,\ldots,i+j-1}) \tag{4.6}$$

Our first goal is to bound $\alpha_{t-m'+1}$. We proceed as follows.

Lemma 3. For the following d and j

$$\begin{cases} d & = \lfloor \frac{t-m'+1}{m'} \rfloor, \ j = (t-m'+1) \mod (m') \\ & \text{if } t-m'+1 \mod (m') \neq 0 \\ d & = \frac{t-m'+1}{m'} - 1, \ j = m' \\ & \text{if } t-m'+1 \mod (m') = 0 \end{cases} \tag{4.7}$$

we have

$$\alpha_{t-m'+1} \geq d\alpha_1 + \alpha_j + o(N) \tag{4.8}$$

Proof. Note that $i-(m')$ -th destination can decode $x_{i-(m')}$ from $(S^N, x^c_{i,i+1,\ldots,i+j-1,i-(m')})$ with

$P_e \to 0$ as $N \to \infty$. Therefore, we can write

$$\begin{aligned} N\mathcal{R}_{i-(m')} &= H(x_{i-(m')}) && (4.9)\\ &= I(x_{i-(m')}; S^N | x^c_{i,i+1,\dots,i+j-1,i-(m')}) \\ &\quad + H(x_{i-(m')} | S^N, x^c_{,i+1,\dots,i+j-1,i-(m')}) \\ &= H(S^N | x^c_{i,i+1,\dots,i+j-1,i-(m')}) \\ &\quad - H(S^N | x^c_{i,i+1,\dots,i+j-1}) + o(N) && (4.10) \end{aligned}$$

which gives us

$$\begin{aligned} &H(S^N | x^c_{i,i+1,\dots,i+j-1,i-(m')}) = \\ &N\mathcal{R}_{i-(m')} + H(S^N | x^c_{i,i+1,\dots,i+j-1}) + o(N) && (4.11) \end{aligned}$$

Next, note that $(i - 2(m'))$-th destination does not have $x_{i,\dots,i+j-1,i-(m'),i-2(m')}$ as prior messages. So, given $(S^N, x^c_{i,\dots,i+j-1,i-(m'),i-2(m')})$ it must be able to reliably decode $x_{i-2(m')}$.

$$\begin{aligned} N\mathcal{R}_{i-2(m')} &= H(x_{i-2(m')}) \\ &= I(x_{i-2(m')}; S^N, x^c_{i,\dots,i+j-1,i-(m'),i-2(m')}) \\ &\quad + H(W_{i-2(m')} | S^N, x^c_{i,\dots,i+j-1,i-(m'),i-2(m')}) \\ &= I(x_{i-2(m')}; S^N | x^c_{i,\dots,i+j-1,i-(m'),i-2(m')}) \\ &\quad + o(N) \\ &= H(S^N | x^c_{i,\dots,i+j-1,i-(m'),i-2(m')}) \\ &\quad - H(S^N | x^c_{i,\dots,i+j-1,i-(m')}) + o(N) && (4.12) \end{aligned}$$

which along with (4.11) gives us

$$\begin{aligned} H(S^N | x^c_{i,\dots,i+j-1,i-(m'),i-2(m')}) &= N\mathcal{R}_{i-2(m')} + n\mathcal{R}_{i-(m')} \\ &\quad + H(S^N | x^c_{i,i+1,\dots,i+j-1}) \\ &\quad + o(N) && (4.13) \end{aligned}$$

Similarly, we note that $(i-lm')$-th destination, for $3 \leq l \leq d$ does not have $x_{i,\ldots,i+j-1,i-(m'),\ldots,i-l(m')}$ as prior messages, so it must be able to decode $x_{i+j-1+l(m')}$ from $(S^N, x^c_{i,\ldots,i+j-1,i-m',\ldots,i-lm'})$.

$$\begin{aligned} N\mathcal{R}_{i-lm'} = & \; H(x_{i-lm'}) & (4.14)\\ = & \; I(x_{i-lm'}; S^N, x^c_{i,\ldots,i+j-1,i-m',\ldots,i-lm'}) + \\ & \; H(x_{i-lm'}|S^N, x^c_{i,\ldots,i+j-1,i-m',\ldots,i-lm'}) & (4.15)\\ = & \; I(x_{i-lm'}; S^N|x^c_{i,\ldots,i+j-1,i-m',\ldots,i-lm'}) + o(N) & (4.16)\\ = & \; H(S^N|x^c_{i,\ldots,i+j-1,i-m',\ldots,i-lm'}) - \; H(S^N|x^c_{i,\ldots,i+j-1,i-m',\ldots,i-(l-1)m'}) + o(N) & (4.17) \end{aligned}$$

which gives us

$$\begin{aligned} H(S^N|x^c_{i,\ldots,i+j-1,i-m',\ldots,i+j-dm'}) = & \; N\mathcal{R}_{i-dm'} + \ldots + N\mathcal{R}_{i-2m'} + N\mathcal{R}_{i-m'} + H(S^N|x^c_{i,i+1,\ldots,i+j-1}) \\ & +o(N) & (4.18) \end{aligned}$$

Our goal is to bound $\alpha_{t-m'+1}$. We have

$$\begin{aligned} \alpha_{t-m+1} & = \alpha_{dm'+j} & (4.19)\\ & = \sum_{i=1}^{n} H(S^N|x^c_{i,i+1,\ldots,i+t-m'}) & (4.20)\\ & \geq \sum_{i=1}^{n} H(S^N|x^c_{i,\ldots,i+j-1,i-m',i-2m',\ldots,i-dm'}) & (4.21)\\ & = \sum_{i=1}^{n} \{N\mathcal{R}_{i-m'} + \ldots + N\mathcal{R}_{i-dm'} + \\ & \quad H(S^N|x^c_{i,i+1,\ldots,i+j-1}) + o(N)\} & (4.22)\\ & = d\alpha_1 + \alpha_j + o(N) & (4.23) \end{aligned}$$

where (4.21) is true because conditioning reduces the entropy. (4.22) is derived by replacing (4.18) into (4.21). This proves Lemma 3. □

Lemma 4. For $j = 2, 3, \ldots, m'$, we have

$$\begin{aligned} \alpha_j & \geq \alpha_{j-1} + \frac{\alpha_1}{m'} + o(N) & (4.24)\\ \Rightarrow \quad \alpha_j & \geq \frac{m'-1+j}{m'}\alpha_1 + o(N) & (4.25) \end{aligned}$$

Proof. We use Lemma Lemma 5 from [17] at each step. So we have

$$\begin{aligned}
\sum_{i=1}^{n} H(S^N, x^c_{i,i+1,\ldots,i+j-2,i-m'}) \leq\; & \sum_{i=1}^{n}\{H(S^N, x^c_{i-1,i,i+1,\ldots,i+j-2}) \\
& +H(S^N, x^c_{i-1,i,i+1,i+2,\ldots,i+j-3,i-m'}) \\
& -H(S^N, x^c_{i-1,i+2,\ldots,i+j-3})\} \qquad (4.26)\\
\leq\; & \sum_{i=1}^{n}\{H(S^N, x^c_{i-1,i,i+1,\ldots,i+j-2}) \\
& +H(S^N, x^c_{i-2,i-1,i,i+1,i+2,\ldots,i+j-3}) \\
& +H(S^N, x^c_{i-2,i-1,i,i+1,i+2,i+3,\ldots,i+j-4,i-m'}) \\
& -H(S^n, x^c_{i-2,i-1,i,i+1,\ldots,i+j-4}) \\
& -H(S^N, x^c_{i-1,i+2,\ldots,i+j-3})\} \qquad (4.27)\\
\vdots\; & \\
\leq\; & \sum_{i=1}^{n}\{H(S^N, x^c_{i-1,i,i+1,\ldots,i+j-2}) \\
& +H(S^N, x^c_{i-2,i-1,i,i+1,i+2,\ldots,i+j-3}) \\
& +\ldots + H(S^N, x^c_{i-m'+j-1,\ldots,i-m'}) \\
& -H(S^N, x^c_{i-m'+j-1,i-m'+j-2,\ldots,i-m'+1}) \\
& -\ldots - H(S^N, x^c_{i-2,i-1,\ldots,i+j-4}) - \\
& H(S^N, x^c_{i-1,i,\ldots,i+j-3})\} \qquad (4.28)
\end{aligned}$$

We note that $(i-m')$-th destination does not have $x_{i,i+1,\ldots,i+j-2,i-m'}$ as antidotes, so it must be able to decode $W_{i-m'}$ from $(S^N, x^c_{i,i+1,\ldots,i+j-2,i-m'})$.

$$\begin{aligned}
N\mathcal{R}_{i-m'} &= H(x_{i-m'}) \qquad (4.29)\\
&= I(x_{i-m'}; S^N, x^c_{i,i+1,\ldots,i+j-2,i-m'}) + \\
&\quad H(x_{i-m'}|S^N, x^c_{i,i+1,\ldots,i+j-2,i-m'}) \qquad (4.30)\\
&= I(x_{i-m'}; S^N|x^c_{i,i+1,\ldots,i+j-2,i-m'}) + o(N) \qquad (4.31)\\
&= H(S^N|x^c_{i,i+1,\ldots,i+j-2,i-m'}) - \qquad (4.32)\\
&\quad H(S^N|x^c_{i,i+1,\ldots,i+j-2}) + o(N) \qquad (4.33)
\end{aligned}$$

which gives us

$$\begin{aligned} H(S^N|x^c_{i,i+1,\ldots,i+j-2,i-m'}) = N\mathcal{R}_{i-m'} + \\ H(S^N|x^c_{i,i+1,\ldots,i+j-2}) + o(N) \end{aligned} \tag{4.34}$$

Replacing (4.34) into (4.28), we have

$$\alpha_{j-1} + \alpha_1 + o(N) \leq \alpha_j + \ldots + \alpha_j - \alpha_{j-1} - \ldots - \alpha_{j-1} \tag{4.35}$$

$$\alpha_j \geq \frac{1}{m'}\{(m')\alpha_{j-1} + \alpha_1\} + o(N) \tag{4.36}$$

Solving this recursive equation, we get

$$\alpha_j \geq \frac{m' - 1 + j}{m'}\alpha_1 + o(N) \tag{4.37}$$

This proves Lemma 4. Combining Lemma 3 and Lemma 4, we have the following

$$\alpha_{t-m+1} \geq d\alpha_1 + \frac{m' - 1 + j}{m'}\alpha_1 + o(N)$$

$$= \frac{d(m') + j + m' - 1}{m'}\alpha_1 + o(N) = \frac{t - m' + 1 + m' - 1}{m'; \\ +o(N)}\alpha_1$$

Finally, we note that $(i - m)$-th destination does not have any of the messages $x_{i,i+1,\ldots,i+t-m'}$ as prior messages. So it must be able to decode $x_{i-m'}$ from $(S^N, x_{i-m',i,i+1,\ldots,i+t-m'})$.

$$\begin{aligned} \sum_{i=1}^{n} N\mathcal{R}_{i-m'} &\leq \sum_{i=1}^{n} I\left(x_{i-m'}; S^N|x^c_{i-m',i,i+1,\ldots,i+t-m'}\right) \\ &\quad +o(N) \\ &= \sum_{i=1}^{n} H\left(S^N|x^c_{i-m',i,i+1,\ldots,i+t-m'}\right) - \\ &\quad \sum_{i=1}^{n} H(S^N|x^c_{i,i+1,\ldots,i+t-m'}) + o(N) \end{aligned}$$

$$\leq \sum_{i=1}^{n}\{N - \frac{t}{m'}NR_i\} + o(N) \tag{4.38}$$

Rearranging terms and applying the limit $N \to \infty$ we have

$$\sum_{i=1}^{n} R_i \leq \frac{m'}{t+m'}n \tag{4.39}$$

so that we have the information theoretic capacity outer bound of $\frac{m'}{t+m'}$ per message. □

□

We can see that Theorem 6 in [17] is a special case of the above theorem with $m' = 1$ giving capacity $\frac{1}{t+1}$. When $t - m + 1$ is kept fixed, and $t \longrightarrow \infty$, then $C = \frac{1}{2}$.

Theorem 13. The capacity of the index coding problem associated with $n = m$, $\mathcal{W}_k = x_k$, $\mathcal{K}_k = \{x_{k-u}, x_{k+u}\}$ is $C = \frac{2}{n}$ per message if $\frac{n}{u} \neq 3$. Else $C = \frac{3}{n}$.

Proof. Achievability scheme when $\frac{n}{u} \neq 3$: We consider $\mathbb{F}_2$. The scheme is a vector linear coding scheme, where each message is sent through 2 symbols over a n- dimensional space where any two messages which are u distance apart overlap in one dimension. Hence every receiver can decode its wanted message.

Achievability scheme in other cases: Each message x_i can share a vector in a $n/3$ dimensional space with x_{i-u} and x_{i+u}.

Proof of upper bound: Consider the initial message set. Pick the messages $x_i, x_{i+u}, \ldots\ldots x_{i-u}$ for some arbitrary i. We get a new set of messages which forms a new index coding setting identical to that in Theorem 6 with $u = t = 1$. Continue doing the previous two steps without considering messages already picked. Hence we get a series of identical index coding settings which are not related to each other and having the same number of messages, say e. Let the number of the new index coding settings be e'. No two settings involve the same message. Hence $e\ e' = n$. If $\frac{n}{u} = 3$, $e = 3$. From Theorem 6, rate of each message in each of the new index coding settings is 1 if $e = 3$ and $2/e$ else. Hence the effective rate is $1/e'$, if $e = 3$ and $2/n$ else. □

4.4 Results and Discussions

Though index coding with restricted information was introduced by Dau *et. al.* in [18] and it was proved that every code offers a certain level of security depending on certain parameters, the rate regions were not studied. In this work, we extended the results in [17] for the special case of index coding with restricted information. We identified that in this new scenario, capacities can either remain the same or drop down to zero. Also, we were able to generalise one result from [17].

Chapter 5

Conclusion

In this thesis, the idea of optimal index coding with min-max probability of error was developed. This is the first work to best of my knowledge which considers index coding in a fading environment. This was used as a motivation for analysing the number of optimal codes possible. The concept of interference alignment in index coding was studied and it was extended to the case of index coding with restricted information. The summary of results is as below.

5.1 Summary of Results

• The criterion for identifying the best code in terms of min-max probability of error among all optimal codes (over finite field $\mathbb{F}_2$) is proposed and an algorithm based on that is given.

• Towards identifying the best among the optimal codes, a lower bound on the number of optimal codes is given.

• A simpler algebraic formulation of an index coding problem is given.

• Index coding with restricted side information is studied through an interference alignment approach and the feasible rates are calculated.

• An index coding setting in [17] was generalised and feasible rates are found.

5.2 Scope for future work

While working on the problem of index coding, we came across many open problems one of which is identifying the best modulation scheme for an index coding scenario. Moreover, the work done in this thesis itself can be extended in several directions.

• Matrix completion algorithms to extend work done in Chapter 3 can be studied.

• In our work in Chapter 1, we consider only binary field. The criterion for minimum-maximum probability of error over other fields is yet open.

• Work done in Chapter 4 can be extended or generalised by considering other index coding settings similar to those in [17].

Bibliography

[1] Y. Birk and T. Kol,“Informed-source coding-on-demand (ISCOD) over broadcast channels,”in *Proc. IEEE Conf.Comput. Commun.*, San Francisco, CA, 1998, pp.1257-1264.

[2] Z. Bar-Yossef, Z. Birk, T. S. Jayram and T. Kol, “Index coding with side information,” in *Proc. 47th Annu. IEEE Symp. Found. Comput. Sci.*, 2006, pp. 197-206.

[3] E. Lubetzky and U. Stav, “Non-linear index coding outperforming the linear optimum,” in *Proc. 48thAnnu.IEEESymp.Found.Comput.Sci.*, 2007, pp.161-168.

[4] L Ong and C K Ho,“Optimal Index Codes for a Class of Multicast Networks with Receiver Side Information,” in *Proc. IEEE ICC*, 2012, pp 2213-2218.

[5] Salim El Rouayheb, Alex Sprintson and Costas Georghiades, “On the Index Coding Problem and its relation to Network Coding and Matroid Theory”, in *IEEE Trans. Inf. Theory*, vol.56, no.7, pp. 3187–3195, Jul. 2011.

[6] Ralf Koetter and Muriel Medard,“An Algebraic Approach to Network Coding”, in *IEEE/ACM transactions on networking*, vol.11, no.5, pp. 782–795, Oct. 2003.

[7] Gilbert Strang, Introduction to Linear Algebra, 3rd ed. MA:Wellesley Cambridge, 2003

[8] James G. Oxley, Matroid Theory, Oxford University Press, 1992.

[9] Anoop Thomas, Kavitha R., A. Chandramouli, and B. Sundar Rajan, “Optimal Index Coding with Min-Max Probability of Error over Fading Channels”, Available on ArXiv at http://arxiv.org/abs/1410.6038v3.

[10] Anoop Thomas, Kavitha R, Chandramouli A and B Sundar Rajan, “Optimal Index Coding with Min-Max Probability of Error over Fading Channels”, Communicated to *IEEE ICC*, 2015.

[11] Nicholas J A Harvey, David R Karger, Kazuo Murota, "Deterministic Network Coding by Matrix Completion", in *Proc. of the 16th Annu. ACM-SIAM symposium on Discrete algorithms, SODA*, pp. 489–498, 2005, DOI: 10.1145/1070432.1070499.

[12] Son Hoang Dau, Vitaly Skachek and Yeow Meng Chee, "Error Correction for Index Coding with Side Information", in *IEEE Trans. Inf. Theory*, Vol. 59, No. 3, March 2013, pp. 1517-1531.

[13] E. Lubetzky and U. Stav, "Non-linear Index Coding Outperforming the Linear Optimum", in *Proc. 48th Annu. IEEE Symp. Found. Comput. Sci.*, 2007, pp. 161-168.

[14] . J. Neely, A. S. Tehrani, Z.Zhang, "Dynamic Index Coding for Wireless Broadcast Networks", in *Proc. 31st IEEE Conf. Comput. Commun. (INFOCOM), Orlando, USA.*, March 25-30, 2012, pp. 316-324.

[15] . Langberg and A. Sprintson, "On the Hardness of Approximating the Network Coding Capacity", in *IEEE Symp. Inf. Theory. (ISIT)*, 2008, pp. 315-319.

[16] . Y. El Rouayheb, M. A. R. Chaudhry and A. Sprintson, "On the Minimum Number Of Transmissions in Single-Hop Wireless Coding Networks", in *Proc. Inf. Theory Workshop (ITW), Lake Tahoe*, Sept. 2007.

[17] Hamed Maleki, Viveck R. Cadambe, Syed A.Jafar, "Index Coding-An interference Alignment Perspective", Available on ArXiv at http://arxiv:1205.1483v1 [cs.IT] 7 May 2012.

[18] Son Hoang Dau, Vitaly Skachek, Yeow Meng Chee, "On the Security of Index Coding With Side Information", in *IEEE Trans. Inf. Theory*, Vol. 58, No. 6, March 2012, pp. 3975-3988.

Publications

Conference Papers

1. Kavitha. R and B. Sundar Rajan, "On The Number of Optimal Index Codes," appears in *Proc. ISIT'2015*, Hong Kong, June, 2015.

2. Anoop Thomas, Kavitha R., A. Chandramouli, and B. Sundar Rajan, "Optimal Index Coding with Min-Max Probability of Error over Fading Channels," to appear in *Proc. PIMRC'2015*, Hong Kong, August, 2015.

Journal Papers

1. Anoop Thomas, Kavitha R., A. Chandramouli, and B. Sundar Rajan, "Optimal Index Coding with Min-Max Probability of Error over Fading Channels," communicated to *IEEE Trans. on Vehicular Technology.*

ArXiv

1. Anoop Thomas, Kavitha R., A. Chandramouli, and B. Sundar Rajan, "Optimal Index Coding with Min-Max Probability of Error over Fading Channels", Available on ArXiv at http://arxiv.org/abs/1410.6038v3.

2. Kavitha R. and B. Sundar Rajan, "On the Number of Optimal Index Codes", Available on ArXiv at http://arxiv.or/abs/1504.05008v1.