

2011

Network Coding for Wireless and Wired Networks: Design, Performance and Achievable Rates

Hakan Topakkaya
Iowa State University

Follow this and additional works at: <https://lib.dr.iastate.edu/etd>

 Part of the [Electrical and Computer Engineering Commons](#)

Recommended Citation

Topakkaya, Hakan, "Network Coding for Wireless and Wired Networks: Design, Performance and Achievable Rates" (2011).
Graduate Theses and Dissertations. 10345.
<https://lib.dr.iastate.edu/etd/10345>

This Dissertation is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.

**Network coding for wireless and wired networks: Design, performance and
achievable rates**

by

Hakan Topakkaya

A dissertation submitted to the graduate faculty
in partial fulfillment of the requirements for the degree of
DOCTOR OF PHILOSOPHY

Major: Electrical Engineering

Program of Study Committee:
Zhengdao Wang, Major Professor
Aleksandar Dogandžić
Ahmed Kamal
Dan Nordman
Aditya Ramamoorthy

Iowa State University

Ames, Iowa

2011

Copyright © Hakan Topakkaya, 2011. All rights reserved.

DEDICATION

I would like to dedicate this thesis to my parents.

TABLE OF CONTENTS

LIST OF FIGURES	vi
LIST OF ACRONYMS	viii
ACKNOWLEDGEMENTS	ix
ABSTRACT	x
CHAPTER 1. INTRODUCTION	1
1.1 Network Coding	2
1.2 Cooperative Communication	6
1.2.1 Background on DMT	8
1.3 Interference Alignment	10
1.4 Contributions	11
CHAPTER 2. Effects of Delay and Links between Relays on the Min-Cut	
Capacity in a Wireless Relay Network	13
2.1 Introduction	13
2.2 System Model	14
2.2.1 Channel Model	15
2.3 Main Results	15
2.3.1 No links among relays	15
2.3.2 Links among Relays	19
2.4 Simulations	22
2.5 Conclusions	22

CHAPTER 3. Wireless Network Code Design and Performance Analysis

Using Diversity-Multiplexing Tradeoff	23
3.1 Introduction	23
3.2 System Model	25
3.2.1 General System Description	25
3.2.2 Network Coded Cooperation	27
3.2.3 Deterministic and Random Network Coding	28
3.3 Performance Analysis	29
3.3.1 Diversity-Multiplexing Tradeoff	29
3.3.2 Main Result	29
3.4 Design of the Linear Network Coding Matrix	32
3.4.1 Network Code Designs from Reed-Solomon Codes	33
3.5 Discussions and Further Improvements	36
3.5.1 Strategy \mathcal{B}	36
3.5.2 RNCC	36
3.5.3 Selection Relaying	38
3.6 Comparison with Other Schemes	39
3.6.1 DMT Comparison	39
3.6.2 Monte-Carlo Simulation	40
3.7 Conclusions	42

CHAPTER 4. Interference Alignment for Wired Networks with General

Message Demands	44
4.1 Introduction	44
4.2 General System Description	45
4.3 Simple Case: Three Source Four Destination Nodes	47
4.4 General Case: K Source J Destination Nodes	52
4.5 Discussion	56
4.6 Conclusions	57

CHAPTER 5. CONCLUSION AND FUTURE WORK	58
APPENDIX A. Proof of Lemma 3	61
APPENDIX B. Proof of Theorem 3	62
BIBLIOGRAPHY	64

LIST OF FIGURES

1.1	The celebrated butterfly network, an example of a network requiring coding to achieve capacity (due to [1]). The network consists of directed unit capacity links, and a source node s multicasting the same information to two receivers y and z . The presence of the bottleneck link from w to x necessitates coding on that link in order to achieve the same multicast rate.	3
1.2	An example network that has a relay node cooperating with the source node to transmit to the destination node.	6
2.1	(a) Line network, (b) diamond network, and (c) the network with relay links	14
2.2	extended diamond network with K relays	17
2.3	extended network with K relays with links between the relays	19
2.4	Average capacity vs delay	20
2.5	The difference between Monte-Carlo and theoretical results	20
2.6	The difference between the networks with and without links among relays	21
3.1	System model: N source-destination pairs and M relays	25
3.2	Time-division allocation for the different schemes compared: (a) CC (b) NCC (c) DNCC and RNCC	27
3.3	DMT comparison of various schemes	40
3.4	Average outage probability per destination, ($N = 2, M = 1, \dots, 3$)	41
3.5	Average outage probability per destination, ($N = 3, M = 1, \dots, 3$)	41

3.6	Average outage probability per destination, ($N = 2, M = 1, \dots, 3$) . . .	42
3.7	Average outage probability per destination, ($N = 3, M = 1, \dots, 3$) . . .	43
4.1	An example network for which the proposed interference alignment can not be applied since the assumption (A2) is violated.	56

LIST OF ACRONYMS

AWGN	additive white Gaussian noise
MAC	Multiple Access Channel
DOF	Degrees Of Freedom
MIMO	Multiple-Input Multiple-Output
SNR	Signal to Noise Ratio
IA	Interference Alignment
DMT	Diversity-Multiplexing Tradeoff
BER	Bit Error Rate
TDMA	Time Division Multiple Access

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my thanks to those who helped me with various aspects of conducting research and the writing of this thesis. First and foremost, Prof. Zhengdao Wang for his guidance, patience and support throughout this research and the writing of this thesis. His insights and words of encouragement have often inspired me and renewed my hopes for completing my graduate education.

I would also like to thank my committee members for their efforts and contributions to this work: Prof. Aditya Ramamoorthy, Prof. Aleksander Dogandžić, Prof. Ahmed Kamal and Prof. Dan Nordman. I would like to thank my committee members also for the classes that they taught from which I have greatly benefitted from and which became the foundation of my research. I would like to thank Prof. Nicola Elia for his valuable suggestions about how to improve my teaching skills. I have gained important skills and experience during my teaching assistantship for his classes.

During my Ph.D, I was very lucky to have so many great friends around me. I will always remember the long conversations with Kun Qiu and the inside jokes. Special thanks to Mehmed B. Diken, Taha Khalad, Lei Ke, Burcu Colakoglu, Abdulkadir Celik, Lizandro Solano, Neevan Ramalingram among many other wonderful friends that I made along the way.

Finally, I would like to mention that I have been very lucky to have a wonderful family. I am forever grateful to my parents and my sisters for supporting me when I needed the most with their constant love, and encouragement.

ABSTRACT

Many point-to-point communication problems are relatively well understood in the literature. For example, in addition to knowing what the capacity of a point-to-point channel is, we also know how to construct codes that will come arbitrarily close to the capacity of these channels. However, we know very little about networks. For example, we do not know the capacity of the two-way relay channel which consists of only three transmitters. The situation is not so different in the wired networks except special cases like multicasting. To understand networks better, in this thesis we study network coding which is considered to be a promising technique since the time it was shown to achieve the single-source multicast capacity.

First we design and analyze deterministic and random network coding schemes for a cooperative communication setup with multiple sources and destinations. We show that our schemes outperform conventional cooperation in terms of the diversity-multiplexing tradeoff (DMT). Specifically, it can offer the maximum diversity order at the expense of a slightly reduced multiplexing rate. We derive the necessary and sufficient conditions to achieve the maximum diversity order. We show that when the parity-check matrix for a systematic maximum distance separable (MDS) code is used as the network coding matrix, the maximum diversity is achieved. We present two ways to generate full-diversity network coding matrices: namely using the Cauchy matrices and the Vandermonde matrices. We also analyze a selection relaying scheme and prove that a multiplicative diversity order is possible with enough number of relay selection rounds.

In addition to the above scheme for wireless networks, we also study wired networks, and apply network coding together with interference alignment. We consider networks with K source nodes and J destination nodes with arbitrary message demands. We first consider a

simple network consisting of three source nodes and four destination nodes and show that each user can achieve a rate of one half. Then we extend the result for the general case which states that when the min-cut between each source-destination pair is one, it is possible to achieve a sum rate that is arbitrarily close to the min-cut between the source nodes whose messages are demanded and the destination node where the sum rate is the summation of all the demanded source message rates plus the biggest interferer's rate.

CHAPTER 1. INTRODUCTION

We are living in a world that is becoming more social and connected than ever before thanks to the developments in communication. Communication is constantly altering the way we live our lives. From how we socialize with others to how we work and to how we entertain ourselves, communication has become an integral part of our day. Developments like email, social networking sites like Facebook and Twitter, instant messaging, cell phones, and video conferencing have allowed us to get in touch with each other quickly for both business and emergency needs. No matter where we use these services whether we are on travel or in the comfort of our homes, we want more “speed”, more “reliability” and more “coverage”. Hence, this ever lasting demand for higher and higher rates and reliability has become a driving factor for most of the research that is taking place in the academia and in the industry.

In this thesis, we will try to address these problems both in the wireless networks such as cellular networks, Wi-Fi, WIMAX, etc or in the wired networks such as internet, wired local area networks (LANs) and so forth. Using sophisticated tools such as diversity-multiplexing tradeoff [2], we show mathematically how the speed (rate) and the reliability affect each other. We also propose techniques to mitigate the adverse effects of problems like *multipath fading* in wireless networks that will help increasing the robustness, reliability and coverage in the network.

One of the many problems that needs to be dealt with for higher rates and reliability is “interference”. We propose to use a promising new technique called *interference alignment* [3] to deal with the interference problem. The techniques proposed in this thesis for these problems can be categorized mainly into three areas: *network coding*, *cooperative communication* and *interference alignment*. Next we elaborate on each of these areas before we get into our results.

1.1 Network Coding

In the majority of the existing communication networks such as Internet, Peer-to-Peer (P2P) networks, wireless ad hoc networks and sensor networks, data packets are typically transmitted from the source node to a prescribed set of destination nodes by a method known as “store and forward” in which data packets received by the intermediary nodes are stored and then forwarded to the next node. In such a network, the information flow is upper bounded by the value of the minimum cut between the source and the destination, which is known as the Max-flow Min-cut theorem [4]. There are many algorithms to find the maximal flow in a graph such as Ford-Fulkerson algorithm. However, in [1] Ahlswede et al. showed that simply routing is not sufficient to achieve the max-flow value when there are multiple destinations. In their seminal work, a new paradigm *network coding* was introduced to achieve the max-flow value for single-source multicast (same information by a single source node is sent to multiple destination nodes). The basic idea of network coding is to allow the intermediate nodes not only simply route the information but instead using a linear or non-linear function, encode its own information with its neighbors’ and then transmit this encoded information. It turns out that the use of network coding can provably increase network throughput and robustness.

There is a perfect example given by Ahlswede et al. [1] that shows the benefits of network coding in a very small network called the “butterfly network”. Fig. 1.1 shows this celebrated example of a network for which coding at the node w is necessary in order to achieve the maximum possible multicast transmission rate. In this thesis, we will combine network coding with interference alignment to achieve higher rates and also will apply network coding in a cooperative communication scenario to achieve higher diversity. Next we give the related work and the evolution of the network coding literature.

Network coding was proposed in the work of Ahlswede et al. [1]. It was shown that if we allow encoding at the intermediary nodes in a network, a source can transmit (multicast) information at a rate approaching the smallest minimum cut between the source and any of the receivers. Otherwise (when no coding at the intermediary nodes) they showed that it would be impossible to achieve the minimum cut. The celebrated butterfly example Fig. 1.1 illustrates

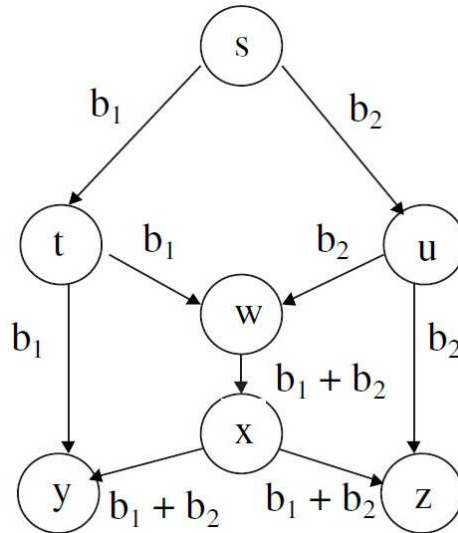


Figure 1.1 The celebrated butterfly network, an example of a network requiring coding to achieve capacity (due to [1]). The network consists of directed unit capacity links, and a source node s multicasting the same information to two receivers y and z . The presence of the bottleneck link from w to x necessitates coding on that link in order to achieve the same multicast rate.

this fact. Later, Li et al. [5] showed that to achieve the capacity for single-source multicasting, linear coding at the intermediate nodes would be sufficient. Another key paper in the area is by Koetter and Médard [6] which presents an algebraic framework for linear network coding extending previous results to not only arbitrary networks, but also prove the achievability of the min-cut max-flow bound for networks with delay and cycles. Specifically, reference [6] gives the algebraic characterization of the feasibility of a multicast problem by showing that validity of a network coding solution is equivalent to the existence of a transfer matrix whose determinant is nonzero. In [7], a distributed randomized network coding approach is introduced, and the result in [6] is used to obtain a tighter upper bound on the required field size than the previous bound. Various works have considered the characteristics of network codes needed for achieving capacity on different types of networks and connections. Reference provides [8] graph-specific upper bounds based on the number of clashes between flows. Dougherty et al. showed in [9] that for non-multicast networks linear coding is insufficient in general.

In [10] they also showed that the existence of a solution in some alphabet does not imply

the existence of a solution in larger field alphabets. Following that work, Li and Li [11] showed that in undirected networks network coding does not increase throughput for a single unicast or broadcast session, while any increase in throughput is bounded by a factor of two in the case of a single multicast session. In [12] scalar coding solutions seem to be insufficient for some non-multicast problems and instead vector coding solutions is proposed as a solution. Reference [12] also provides necessary and sufficient conditions for an arbitrary set of connections to be achievable on any network. Lehman et al. [13] provides a classification of the complexity of network coding problems and shows that there exists an instance of special networks where determining a scalar linear network code solution is an NP-hard problem. It has been shown in [12] by construction that for some networks scalar linear network coding is not sufficient over any finite alphabet. Similarly Riis [14], reported the insufficiency of scalar linear network coding over binary alphabet field for an example acyclic directed network. It has been shown in [15] that for every set of integer polynomial equations, there exists a directed acyclic network which is scalar linear solvable over a finite field if and only if the set of polynomial equations has a solution over the same finite field.

Researchers have extended the above results to a variety of areas including lossy networks [16], [17], secrecy [18], error-correcting [18], content distribution [19], and distributed storage [20]. Next we look at the development of network coding in wireless networks in more detail.

In the original papers of network coding [1], [5], it was proposed that intermediary nodes would apply network coding at the network layer, hence links between nodes in the network were assumed to be lossless. The immediate question was whether network coding could be applied at the lower layers so that for example the lossy wireless medium could be taken into consideration. Recently several studies suggested that network coding indeed can be performed at the physical layer for further performance improvement [21], [22], [23]. In these papers, physical layer network coding (PNC) was introduced, in which network coding is performed by suitable modulation and demodulation at the relay. The main idea is to recognize that the relay does not need to determine each message but only to compute the desired function of transmitted messages. In [22], analog network coding (ANC) was introduced where the relay

does not compute the desired function but simply amplifies and forwards incoming signals from multiple links. Then the destination node can compute the desired function of messages. Later, from an information theoretic point of view, Nazer et al. considered the problem of recovering a function of sources over a multiple-access channel (MAC) [23]. In [23], an achievable rate was provided and furthermore the importance of structured codes in these networks was explained. In this thesis, we studied the network coded cooperation schemes for N source-destination pairs assisted with M relays. We studied two different traffic network models: multicast and unicast. The proposed schemes allow the relays to apply network coding on the data it has received from its neighbors. We allow the relays to linearly combine the packets with coefficients either deterministically pre-designed or drawn from a finite field randomly. We showed the advantage over the existing schemes when the coding matrix is optimized the proposed schemes for any network coding matrix. Specifically, it is capable of achieving the maximum diversity order at the expense of a slightly reduced multiplexing rate. We derived the necessary and sufficient conditions to achieve the maximum diversity order. When a relay selection is possible, we show that a multiplicative effect on the diversity order is possible when enough rounds of relay selection is performed.

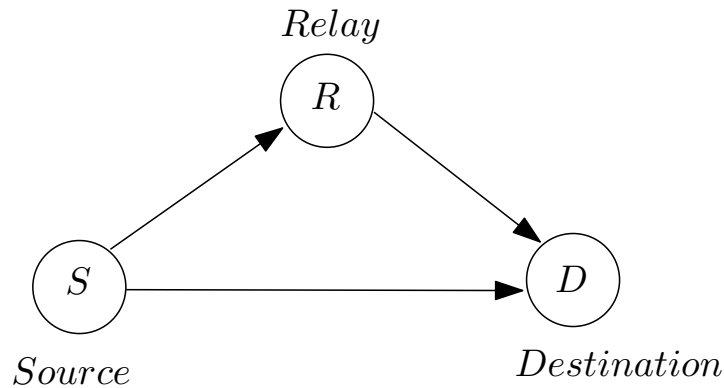


Figure 1.2 An example network that has a relay node cooperating with the source node to transmit to the destination node.

1.2 Cooperative Communication

Basic idea of cooperative communications can be summarized as pooling the resources of distributed nodes to improve the overall performance of a wireless network. It essentially consists of a class of techniques which seek to improve reliability and throughput in wireless systems. This cooperation can occur at different layers of the protocol including physical layer and network layer.

In Fig. 1.2, an example of single-relay cooperative scenarios is shown. Here, a source terminal S is transmitting a signal to a destination terminal D through its direct path ($S-D$). Thanks to the wireless medium, other terminals such as the relay terminal R can overhear the signal. Hence, if terminal R is in a cooperative mode, it can forward the source message to the destination D . This way D receives two replicas of the signal: the original one transmitted from S through the direct path ($S-D$) and the relayed one forwarded by R through the relayed path ($S-R-D$). Now, these two received signals at the destination terminal can be combined to achieve a better spatial diversity compared to the one achieved with a single direct path. There is no restriction on how many relays can participate in this cooperation. In this thesis, we consider multiple source and destination nodes and also multiple relay nodes.

There are various protocols for implementing cooperative communications at the relays. Some of the most popular relaying protocols are Decode-and-Forward (DF) and Amplify-and-Forward (AF), Compress-and-Forward (CF), and Coded Cooperation. In the Decode-and-

Forward [24], [25], [26] relay decodes the sources message and re-encodes it before forwarding it to the destination. Since the decoding can be erroneous, there is potential error propagation which can degrade the system performance. To overcome this, tools like CRC can be used to make sure decoding is correctly done at the relay and participate in the cooperation only in this case.

In the Amplify-and-Forward [27], [25] relay nodes just amplify the signal from the source terminal without performing any sort of decoding. The relay multiplies the sources signal as it is received (noisy version) with certain gain under a certain constraint, e.g., power constraint, and then transmits the resulting signal to the destination. Though it is a very practical protocol thanks to its simplicity, it suffers from noise amplification especially in the low SNR regime.

In the Compress-and-Forward [27], [28] the key idea is that the relay quantizes and compresses the received signal and transmits the compressed version to the destination. Then, at the destination the received message from the source and its quantized version from the relay is combined. This protocol has better performance over DF when the relay is close to the destination.

Finally, in the coded cooperations each source node partitions its codeword into two parts. At the first time slot, each source transmits the first part of its codeword and tries to decode the first part of the other source's codeword [29], [30], [31]. If it can decode the codeword successfully, it transmits the remaining part of its partners codeword. If it can not decode the codeword successfully, the source switches to no-cooperation mode and transmits second part of its own codeword. In this scheme, sources are assumed to be transmitting orthogonally. Next, we give a short literature review on cooperative communications.

The research in the area of cooperative communications dates back to the pioneering work of [32] in the 1970s, where the capacity of relay channels was studied for the problem of information transmission over three terminals. Applications of this general idea have been widely studied in the literature [33], [34], [35]. Reference [36] gives an excellent survey of the field from a information-theory perspective. Many important aspects of relay networks have been extensively studied. The diversity-multiplexing tradeoff of DF and AF relays has

been investigated in [35], [25]. In addition, some distributed space-time codes designed for relay networks have been proposed in [35], [25], [33], [26]. User cooperation which is the generalization of relay networks to multiple sources has been investigated in [33], [34]. Recently, the relaying method has already been incorporated into the WiMAX standard and is expected to spread into many other commercial standards [37].

Relay selection was proposed in the cooperative diversity systems in [26]. The basic idea of selection relaying is to pick a “best” relay according to some criterion like best channel quality, distance, etc and improve performance with less resources compared to no selection case. Later, the idea was extended to multi-source cooperative networks [38], and further to more general fading channels [39]. In [40], a network-coded cooperation (NCC) with relay selection was proposed. NCC was shown to outperform conventional cooperation (CC) schemes which includes space-time coded protocols [35] and selection relaying [26]: It requires less bandwidth, and yield similar or reduced system outage probability while achieving the same diversity order. However, these results are based on an optimistic assumption that any destination node should receive the packets that are not intended for it without any error so that the intended packet can be recovered from the XOR’ed packet sent by the relay. When this assumption is removed the scheme can no longer achieve the full diversity order of $M + 1$, where M is the number of cooperating relays, but only a reduced diversity order of 2.

1.2.1 Background on DMT

Unlike the conventional multiple-input multiple-output channels, cooperative cooperation allows users to simulate a virtual array of antennas in a distributed way. However, most of the tools from the MIMO literature are still applicable to the cooperative communication scenarios. Diversity-multiplexing tradeoff is one of the useful tools that can be borrowed from the MIMO literature. As explained above, the underlying idea behind diversity is to average over multiple path gains (fading coefficients) to increase the reliability. For example, in a system with N transmit and M receive antennas, the maximal diversity gain that can be obtained is MN . But if we use each transmit-receive antenna pair for communication of independent information in

parallel, then we can efficiently increase the data rate of the system. It was shown in [41] that in the high SNR regime the capacity of a channel with N transmit, M receive antennas and i.i.d. Rayleigh faded gains between each antenna pair is given by:

$$C(SNR) = \min(N, M) \log SNR + O(1) \text{ bps.}$$

The maximum multiplexing gain in this case is given by $\min(N, M)$. In [2], it was shown that given a MIMO channel, although both gains can in fact be simultaneously obtained, there is a fundamental tradeoff between each other. To capture this tradeoff, they considered a scheme as a family of codes $\{\mathcal{C}(SNR)\}$ of block length l , one for each SNR level and take $\mathcal{R}(SNR)$ (b/symbol) be the rate of the code. Then the diversity-multiplexing trade-off was formalized as [Def.1, [2]]:

Definition 1. [2] A scheme $\mathcal{C}(SNR)$ is said to achieve spatial multiplexing gain r and diversity gain d if the data rate

$$\lim_{SNR \rightarrow \infty} \frac{\mathcal{R}(SNR)}{\log SNR} = r$$

and average error probability

$$\lim_{SNR \rightarrow \infty} \frac{\log P_e(SNR)}{\log SNR} = -d$$

For each r , define $d^*(r)$ to be the supremum of the diversity advantage achieved by any scheme.

Define

$$d_{\max}^* \triangleq d^*(0)$$

$$r_{\max}^* \triangleq \sup \{r : d^*(r) > 0\}$$

which are respectively the maximal diversity gain and the maximal spatial multiplexing gain in the channel.

From the given definition, one can interpret the spatial multiplexing gain to be the fraction of the capacity at high SNR; and the diversity gain as the reliability at high SNR.

1.3 Interference Alignment

Interference alignment is a new technique combining precoding at the transmitters to align the interference at the receivers and nulling out the interference at the receivers. This way, interference alignment maximizes interference free space for the desired signal. It was shown in [3] that all the interference can be concentrated roughly into one half of the signal space at each receiver, leaving the other half available to the desired signal and free of interference. Next, we give a quick review of the literature on interference alignment.

In [42], Maddah- Ali, Motahari et al. introduced this concept and showed its capability in achieving the full Degrees-Of-Freedom (DOF) for certain classes of two-user X channels. In [3], Cadamba and Jafar showed that in a K user setup, it is possible for each user to achieve half of the rate that is possible in the absence of interference. Later, in [43], it is shown that the same result can be achieved using a simple approach based on a particular pairing of the channel matrices. The assumption of varying channel gains, particularly noting that all the gains should be known at the transmitters sides, is unrealistic which limits the application of these important theoretical results in practice. In [44], Sridharan et al. showed that the DOF of a class of 3-user GICs with fixed channel gains can be greater than one. This result was obtained using layered lattice codes along with successive decoding at the receiver. In [45], it was shown that interference can be aligned using properties of rational and irrational numbers and their relations using the results from the field of Diophantine approximation in Number Theory.

The result of [3] is extended to J destination nodes with arbitrary messages in [46]. Also recently, authors in [47, 48] proposed to use the interference alignment technique in the wired networks. In a three source three destination node setup, they were able to show that each user can achieve a rate of one half when the min-cut is one and the network transfer functions satisfy certain conditions. In this thesis, we extend the idea of using interference alignment in wired networks to more general networks. We consider networks with K source nodes and J destination nodes with arbitrary message demands. We first consider a simple network consisting of three source nodes and four destination nodes and show that each user can achieve

a rate of one half. Then we give the result for the general case which states that a sum rate of all the demanded source messages plus the biggest interferer's rate has to be smaller than the min-cut between the source nodes whose messages are demanded and the destination node.

1.4 Contributions

Here we summarize the contributions of this thesis. In Chapter 2, we study the effect of the delay on the average capacity (min-cut capacity) of wireless relay networks. We define delay as the number of independent channel uses and study the effect of it on the average capacity of the network. For different types of networks, we give closed-form expressions of the capacity as a function of the delay, under the assumption of large delay. The network we consider consists of one source, one destination, and multiple relays where all the relays are connected to each other. We come to an interesting conclusion that the average capacity of this network and the same network but in which the relays are not connected to each other are asymptotically same.

In Chapter 3, we study the network coded cooperation schemes for N source-destination pairs assisted with M relays for two different traffic network models: multicast and unicast. The proposed schemes allow the relays to apply network coding on the data it has received from its neighbors. We propose two ways for the application of network coding at the relays, the linear combination coefficients are either deterministically pre-designed or drawn from a finite field randomly. We derive the necessary and sufficient conditions for achieving the maximum diversity order. For both of these proposed schemes, we establish the diversity-multiplexing tradeoff performance, which turns out to be a function of a special property of the network coding matrix. Then we optimize the scheme according to this property of the network coding matrix and achieve maximum available diversity in the system. We show that when the parity-check matrix for a $(N + M, M, N + 1)$ systematic MDS code is used as the network coding matrix, the maximum diversity is achieved. We present two ways to construct the network coding matrix: using either the Cauchy matrices or the Vandermonde matrices. Both constructions guarantee maximum diversity order. When a relay selection is possible, we

show that a multiplicative effect on the diversity order is possible when enough rounds of relay selection is performed.

In Chapter 4, we first consider a simple network consisting of three source nodes and four destination nodes and show that each user can achieve a rate of one half. Then we extend the result for a more general network consisting of K source nodes and J destination nodes. We show that when the min-cut between each source-destination pair is one, it is possible to achieve a sum rate that is arbitrarily close to the min-cut between the source nodes whose messages are demanded and the destination node where the sum rate is the summation of all the demanded source message rates plus the biggest interferer's rate.

CHAPTER 2. Effects of Delay and Links between Relays on the Min-Cut Capacity in a Wireless Relay Network

2.1 Introduction

Consider a source node in a graph that needs to transfer some information to a destination node, with the help of some relay nodes. The information flow in this case is upper bounded by the value of the minimum cut between the source and the destination, which is known as the Max-flow Min-cut theorem [4]. There are many algorithms to find the maximal flow in a graph such as Ford-Fulkerson algorithm. In our work, we investigate the effect of delay on the min-cut capacity of wireless relay networks.

Being an important factor in the performance of the networks, delay has been previously studied in the literature. Several different definitions of delay have been proposed: delay as the waiting time in the buffer, delay as the propagation time from the communication channel or delay as the time spent for processing information like encoding or decoding, etc. The delay throughput relationship has been treated from the network layer perspective in e.g., [49]. The relationship has also been studied from the physical layer perspective. Information-theoretic results include [50, 51, 52, 53]. In [50], a notion of *delay-limited capacity* has been introduced. In [51], the power-delay trade-off and buffer control policies are examined for time varying channels. In [52], how the delay scales with the size of the ad hoc networks has been studied as a continuation of the work in [54] which studied the problem how the throughput scales with the size of the networks. Delay has been studied in network coding literature too. In [55], the delay performance of network coding with or without channel side information has been compared to conventional scheduling methods. In [56], plain routing is compared against network coding in terms of delay, throughput trade-offs. In [57], a delay sensitive scheduling

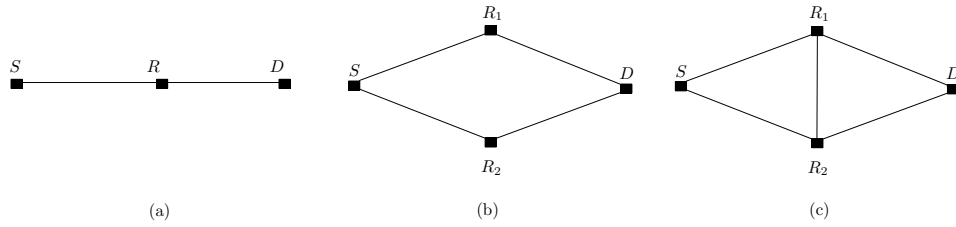


Figure 2.1 (a) Line network, (b) diamond network, and (c) the network with relay links

algorithm based on only XOR operation is proposed.

In this thesis, we define delay as the number of independent channel uses (number of different channel realizations) and we investigate the effect of delay on the average capacity (min-cut capacity) of wireless relay networks. The nodes in the network are considered to be connected via Rayleigh flat fading channels. The motivation is that in order to exploit the averaging effect of multiple channel realizations, buffering and coding across multiple channel realizations is needed. For certain types of networks closed-form expressions of the capacity as a function of delay are derived.

The type of network that we study is a network where there is only one source, one destination and K relays where all the relays are connected to each other through wireless links subject to Rayleigh flat-fading. One interesting result is that the average capacity of this network and the same network in which the relays are not connected to each other are not very different. We give some upper bound on the ratio of the capacities of these two networks. The contributions of this chapter are i) a study of the delay-throughput relationship, and ii) an analysis of the contribution of the links among relays on the average capacity of the transmission from source node to the destination node.

2.2 System Model

We consider a network consisting of single source, single destination, and K relays. The source node is trying to convey information to the destination with the help of the relays. Relays are only one hop away from both the source and the destination node.

2.2.1 Channel Model

The channel model used in this chapter is a time-varying Rayleigh flat fading model. We assume that the channel coherence interval T_c is long compared to the symbol duration T_s , such that $T_c/T_s \gg 1$. For each channel realization h_i between two nodes, a reliable transmission rate of $R(h_i) = \log(1 + \rho|h_i|^2)$ can be achieved, where ρ is the signal to noise ratio (SNR). Since h_i is a random variable, the reliable transmit rate $R(h_i)$ is also a random variable.

If a transmission interval of DT_c can be used, so that D independent channel fading coefficients can be experienced by the transmission, then an average transmission rate of

$$Z(D) = \frac{1}{D} \sum_{i=1}^D R(h_i) = \frac{1}{D} \sum_{i=1}^D \log(1 + \rho|h_i|^2) \quad (2.1)$$

can be achieved.

The parameter D plays the role of delay. The benefit of using a larger D , however, is that the channel appears to be less varying — in the limit of infinite D , the reliable transmission rate $R(D)$ converges to the ergodic capacity of the fading channel. We assume that all the links between the nodes are i.i.d. . At each relay node, information symbols of duration DT_c seconds are buffered. Our goal is to quantify how D affects the average minimum-cut capacity of the relay network.

2.3 Main Results

We will consider first a simple case where there is no links among the relays. Then we will consider the case with links among relays.

2.3.1 No links among relays

Let us consider first a simple linear network as shown in Fig. 2.1. There is no direct link from the source to the destination node, and all communication is performed through the relay node. In order to find the expected value of the min-cut we first need to find the probability density function (PDF) of the random variable corresponding to the min-cut value.

Using the moment generating function (MGF) of the random variable $U = \log(1 + \rho|h_i|^2)$, the PDF of Z can be found as:

$$f_z(z) = \frac{1}{2\pi j} \int_{-\infty}^{\infty} \left(\sum_{i=0}^{s/D} i! \lambda^i \right)^D e^{-zs} ds \quad (2.2)$$

where λ is the mean of the exponentially distributed $|h_i|^2$. Using (2.2), we can write the PDF for $W = \min(C_1, C_2) = \min(Z_1, Z_2)$ as:

$$f_w(w) = 2f_z(w)[1 - F_z(w)] \quad (2.3)$$

where $F_z(w)$ is the cumulative distribution function (CDF) of the random variable Z . Hence the expected value of W is given as:

$$E[W] = \int_0^{\infty} 2wf_z(w)[1 - F_z(w)]dw \quad (2.4)$$

The integral expression in (2.4) makes it difficult to be analyzed. Therefore, since Z is a sum of multiple independent random variables, we can approximate Z with a Gaussian random variable by Central Limit Theorem. For this we need the expected value and the variance of Z . The expected value and the variance of Z can be found to be:

$$\begin{aligned} E[Z] &= \exp(1/(\rho\lambda)) Ei(1/(\rho\lambda)) \\ Var[Z] &= \frac{f(\rho, \lambda)}{D} \\ f(\rho, \lambda) &= E[\log(1 + \rho|h_i|^2)^2] - E^2[Z] \end{aligned} \quad (2.5)$$

Let X_1, X_2 be two independent Gaussian random variables with distribution $N(\mu, \sigma^2)$, then the expected value of the minimum of them ($Y = \min(X_1, X_2)$) is given by:

$$E[Y] = E[\min(X_1, X_2)] = \mu - \frac{\sigma}{\sqrt{\pi}} \quad (2.6)$$

Proposition 1. *The expected value of the min-cut for the line network given in Fig. 2.1(a) is given by*

$$E[W] = E[\min(Z_1, Z_2)] = E[Z] - \frac{\sigma_Z}{\sqrt{\pi D}} \quad (2.7)$$

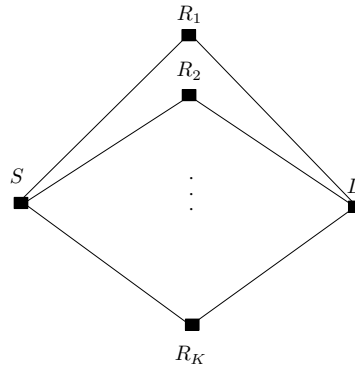


Figure 2.2 extended diamond network with K relays

As can be seen from (2.7) the delay decreases the expected value of the capacity in a square-root fashion and for the large values of D the effect of delay becomes negligible. In this case, the capacity simply converges to the mean value of Z , since by the law of large numbers we have,

$$\frac{1}{D} \sum_{i=1}^D \log(1 + |h_i|^2 \rho) \rightarrow E[\log(1 + |h|^2 \rho)] = E[Z] \quad (2.8)$$

Hence for large D we have,

$$E[W] = E[\min(Z_1, Z_2)] \quad (2.9)$$

$$= E[\min(E[Z_1], E[Z_2])] = E[Z] \quad (2.10)$$

Proposition 2. *The expected value of the min-cut for the K -relay network with i.i.d. links given in Fig. 2.2 (without the relay links) is given by*

$$E[W] = E[\min_i(C_i)] = K \left(E[Z] - \frac{\sigma_Z}{\sqrt{\pi D}} \right) \quad (2.11)$$

Before proving the theorem we give two lemmas which will be used to simplify the proof.

Lemma 1. *The min-cut capacity for the diamond network ($K=2$ case) is given as*

$$W = \min_i \{C_i\} = \min\{Z_{SR_1}, Z_{R_1D}\} + \min\{Z_{SR_2}, Z_{R_2D}\} \quad (2.12)$$

Proof. The cut capacities for the diamond network for $K=2$ case can be computed as [58],

$$\begin{aligned} C_1 &= Z_{SR_1} + Z_{SR_2}; C_2 = Z_{R_1D} + Z_{R_2D}; \\ C_3 &= Z_{SR_1} + Z_{R_2D}; C_4 = Z_{SR_2} + Z_{R_1D}; \end{aligned} \quad (2.13)$$

Then,

$$\begin{aligned} W &= \min_i \{C_i\} = \min\{Z_{SR_1} + Z_{SR_2}, \\ &\quad Z_{R_1D} + Z_{R_2D}, Z_{SR_1} + Z_{R_2D}, Z_{SR_2} + Z_{R_1D}\} \\ &= \min\{\min\{Z_{SR_1} + Z_{SR_2}, Z_{SR_1} + Z_{R_2D}\}, \\ &\quad \min\{Z_{R_1D} + Z_{R_2D}, Z_{SR_2} + Z_{R_1D}\}\} \\ &= \min\{Z_{SR_1} + \min\{Z_{SR_2}, Z_{R_2D}\}, \\ &\quad Z_{R_1D} + \min\{Z_{SR_2}, Z_{R_2D}\}\} \\ &= \min\{Z_{SR_2}, Z_{R_2D}\} + \min\{Z_{SR_1}, Z_{R_1D}\} \end{aligned}$$

□

Lemma 2. *The min-cut capacity for the K -relay network without the relay links is given as*

$$\begin{aligned} W &= \min_i \{C_i\} = \min\{Z_{SR_1}, Z_{R_1D}\} + \\ &\quad \min\{Z_{SR_2}, Z_{R_2D}\} + \cdots + \min\{Z_{SR_K}, Z_{R_KD}\} \end{aligned} \quad (2.14)$$

We skip the proof of Lemma 2 because it involves the same arguments used in the proof of Lemma 1.

Now we can prove the Proposition 2.

Proof. All the min terms in the Lemma 2 involves i.i.d. random variables, hence we can write the expected value of W as a summation of the individual expectation of each of the min terms. Using Lemma 2 and Proposition 1 we have the desired result. □

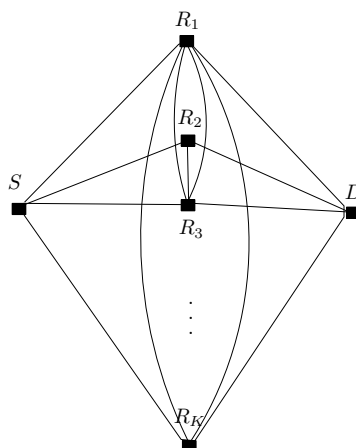


Figure 2.3 extended network with K relays with links between the relays

2.3.2 Links among Relays

The next intuitive step is to look at a network with all the relays connected to each other, unlike the diamond network. The presence of relay links prevents us from obtaining a decomposition similar to such as that in Lemma 2.

To make the analysis tractable, we first make a simplifying assumption. Assume that the relay links have infinite capacity. This will make the relay nodes act together as a virtual unified node. With this assumption we are ready to give the main result of this section.

Proposition 3. *The ratio of the min-cut capacities of the networks with i.i.d. links given in Fig. 2.2 and Fig. 2.3 (without and with the relay links, respectively) is given by*

$$\frac{E[W_d]}{E[W_{rl}]} \xrightarrow{K \rightarrow \infty} 1 - \frac{1}{E[Z]} \frac{\sigma_Z}{\sqrt{\pi D}} \quad (2.15)$$

where K is the number of relays, $E[Z]$ average capacity of the point to point channel between any two nodes, $E[W_d]$ and $E[W_{rl}]$ are the expected value of the min-cut capacities of the networks without and with the relay links, respectively.

Proof. Let C_S and C_D denote the cut capacities around the source and the destination respectively:

$$C_S = \sum_{i=1}^K Z_{SR_i}, \quad C_D = \sum_{i=1}^K Z_{R_i D} \quad (2.16)$$

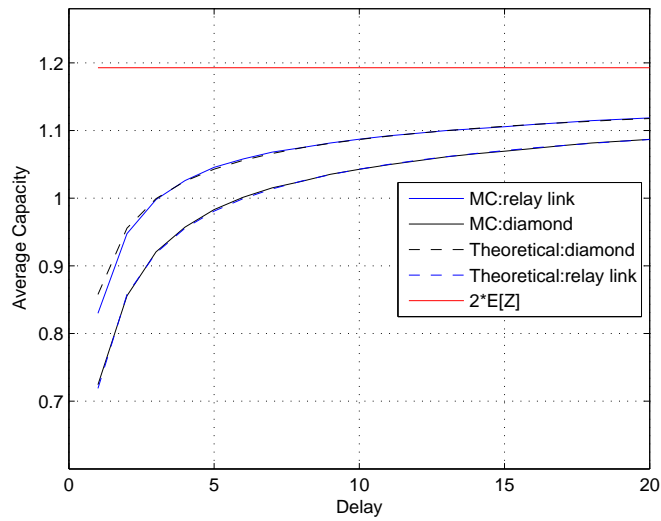


Figure 2.4 Average capacity vs delay

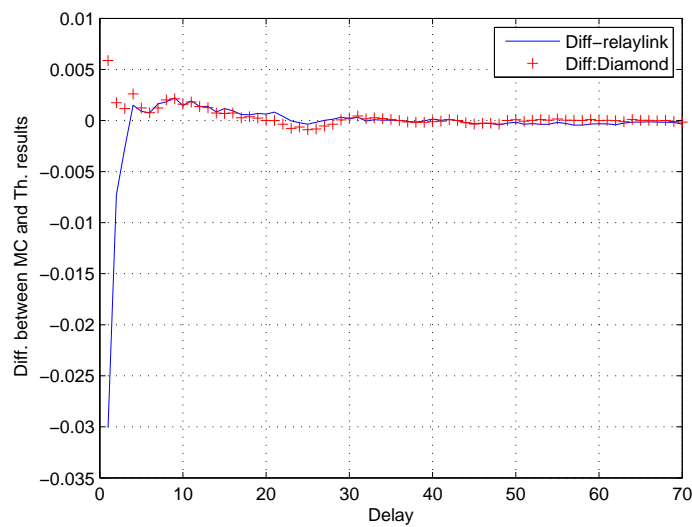


Figure 2.5 The difference between Monte-Carlo and theoretical results

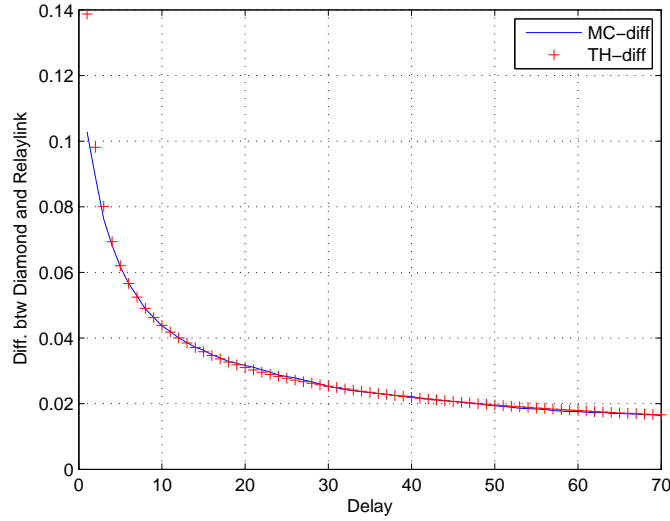


Figure 2.6 The difference between the networks with and without links among relays

But, since we have an infinite capacity assumption for the links between the relays ($Z_{R_i R_j} = \infty, \forall i, j \in \{1, 2 \dots K\}$), the min-cut for this network can be written as

$$W_{rl} = \min_i \{C_i\} = \min\{C_S, C_D\}. \quad (2.17)$$

Now, since all the terms inside the summation in (2.16) are i.i.d. with distribution $N(E[Z], \frac{\sigma_Z^2}{D})$ (using (2.5)) for both C_S and C_D , their distribution is $N(KE[Z], K\frac{\sigma_Z^2}{D})$. Therefore using (2.6), we have

$$E[W_{rl}] = KE[Z] - \sqrt{K} \sqrt{\frac{\sigma_Z}{\pi D}}. \quad (2.18)$$

Using Proposition 2 and taking the limit we get the desired result (2.15). \square

This asymptotic upper bound on the ratio of the min-cuts of the two networks tells us that they are converging to the same value as $K \rightarrow \infty$ and $\rho \rightarrow \infty$ which suggests that the links between the relays do not have a major impact on the capacity of the source-destination transmission, when the number of relays is large.

2.4 Simulations

In this section we compare Monte-Carlo simulation results with the theoretical results. We considered the case $K = 2$, and compared the two networks with and without relay links, namely between the last two types of networks in Fig. 2.1. All the links are i.i.d. The parameters are chosen to be $\rho = 1$ and $\lambda = 1$. As can be seen from Fig. 2.4, both of the average capacities converge to two times of the average capacity of a link $E[Z]$, which was expected from law of large numbers. Fig. 2.5 shows the difference between the Monte-Carlo and theoretical results. The difference converges to zero as D increases (Gaussian assumption justified), which verifies our theoretical results. Fig. 2.6 shows the difference between the two networks with and without links among relays. The difference goes to zero as D increases, which verifies Proposition 3.

2.5 Conclusions

In this chapter we studied the effect of the delay on the average capacity (min-cut capacity) of wireless relay networks. We defined delay as the number of independent channel uses and study the effect of it on the average capacity of the network. For different types of networks, we were able to find closed-form expressions of the capacity as a function of the delay, under the assumption of large delay. The network type we consider was a network where there is one source, one destination, and multiple relays where all the relays are connected to each other. We arrived at an interesting result that the average capacity of this network and the same network but in which the relays are not connected to each other are asymptotically same.

Future studies include extension of the analysis to arbitrary networks and study the effect of delay on different aspects of the wireless networks other than the capacity such as outage probability. Another interesting topic is the matching between the source information symbols arrival statistics and channel variation statistics for this model.

CHAPTER 3. Wireless Network Code Design and Performance Analysis Using Diversity-Multiplexing Tradeoff

3.1 Introduction

Channel fading is one significant cause of performance degradation in wireless networks. In order to combat fading, diversity techniques that operate in time, frequency or space are commonly employed. The basic idea is to send the signals that carry same information through different paths, allowing the receiver to obtain multiple independently faded replicas of the data symbols. Cooperative diversity tries to exploit spatial diversity using a collection of distributed antennas belonging to different terminals, hence creating a virtual array.

In [1] Ahlswede et al. introduced *network coding* to achieve the max-flow rate for single-source multicast that could be impossible to achieve by simply routing the data. Since then, network coding has been recognized as a useful technique in increasing the throughput of a wired/wireless network. The basic idea of network coding is that an intermediate node does not simply route the information but instead combines several input packets from its neighbors with its own packets and then forwards it to the next hop. However, since network coding is devised at the network layer, error-free communication from the physical and medium-access layer is usually assumed, which is a simplifying assumption for wireless communications. Efforts have also been made to apply network coding to the physical layer, e.g. in [21, 59, 60]. Studies have been conducted to determine whether network coding provides any advantages over existing cooperative communication techniques [61, 40, 62, 63, 64, 65, 66].

Relay selection was proposed in the cooperative diversity systems in [26]. Later, the idea was extended to multi-source cooperative networks [38], and further to more general fading channels [39]. In [40], a network-coded cooperation (NCC) with relay selection was proposed.

NCC was shown to outperform conventional cooperation (CC) schemes which includes space-time coded protocols [35] and selection relaying [26]: It requires less bandwidth, and yield similar or reduced system outage probability while achieving the same diversity order. However, these results are based on an optimistic assumption that any destination node should receive the packets that are not intended for it without any error so that the intended packet can be recovered from the XOR'ed packet sent by the relay. When this assumption is removed the scheme can no longer achieve the full diversity order of $M + 1$, where M is the number of cooperating relays, but only a reduced diversity order of 2.

To improve the system diversity performance, in this chapter we propose network coded cooperation schemes for N source-destination pairs assisted with M relays. The proposed scheme allows the relays to apply network coding on the data they have received using random or pre-designed coefficients. Our main contributions in this chapter are as follows:

- (i) We derive the DMT performance of the proposed scheme under multicast and unicast network models, and show that it is superior to previous NCC and CC schemes.
- (ii) We show that a maximum diversity order $M + 1$ is achievable with slightly reduced multiplexing rate.
- (iii) We design the maximum diversity coding matrices, which is related to the conventional MDS error-control codes. We give two constructions for such matrices: using the Cauchy matrices and the Vandermonde matrices.
- (iv) We also analyze a selective relaying scheme, which possesses superior diversity performance under certain conditions.

The rest of the chapter is organized as follows. Sec. 3.2 discusses the system model and a description of the proposed scheme. In Sec. 3.3.1, performance analysis is established using DMT. Sec. 3.4 presents our network code design. In Sec. 3.5, we discuss unicast, random network coding, and selection relaying. In Sec. 3.6, the performance of the proposed scheme is compared in terms of DMT and average outage probability with the existing schemes in the literature. Sec. 3.7 concludes the chapter.

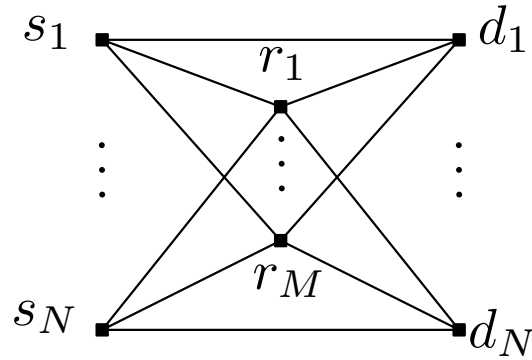


Figure 3.1 System model: N source-destination pairs and M relays

3.2 System Model

3.2.1 General System Description

The network studied in the chapter is composed of N source-destination pairs denoted as $(s_1, d_1), \dots, (s_N, d_N)$, and M relays denoted as r_1, \dots, r_M in a single-cell where all the nodes can hear the transmissions of each other as shown in Fig. 3.1. We assume that each packet is composed of L bits: $b_i = [b_{i,1}, b_{i,2}, \dots, b_{i,L}]$. We divide b_i into smaller blocks of equal length l and represent the k^{th} block $[b_{i,kl+1}, b_{i,kl+2}, \dots, b_{i,(k+1)l}]$, $k \in \{1, \dots, K\}$ a finite-field element $\theta_{i,k} \in \mathbb{F}_q$ where $q = 2^l$ and $K = L/l$. Therefore, each packet is represented as a K -tuple $\Theta_i = [\theta_{i,1}, \theta_{i,2}, \dots, \theta_{i,K}] \in \mathbb{F}_q^{1 \times K}$; see e.g., [67], [68] for representations of finite-field elements. Dividing each packet into small blocks enables us to work with a smaller field size which in return significantly reduces the complexity of the arithmetic operations. This is to be contrasted to the scheme in [6] where the field size is taken to be $q = 2^L$. We will give a lower bound on the field size in Sec. 3.4. We consider two different transmission scenarios. In the first scenario, each source node s_i is trying to transmit the data packet Θ_i to all the destinations $d_i, i = 1, \dots, N$ which is known as the *multicast* scenario. In the second scenario, each source node s_i is trying to transmit the data packet Θ_i to only destination d_i and we will refer to this scenario as the *unicast* scenario. All the nodes are assumed to be equipped with half-duplex (i.e. cannot transmit and receive at the same time) single-antennas. Each data packet Θ_i is coded and modulated, and transmitted in T time slots.

The channel between any pair of nodes is assumed to be frequency flat fading with additive white Gaussian noise (AWGN). Let $x_i \in \mathbb{C}$ denote the transmitted symbols from node i and $y_j \in \mathbb{C}$ the received symbols at node j . The additive noise $z_i \sim \mathbb{CN}(0, 1)$ has independent and identically distributed (i.i.d.) circularly symmetric entries. Let $h_{i,j} \in \mathbb{C}$ denote the instantaneous channel realization. We assume that the channel coefficient $h_{i,j}$ remains constant during the transmission time of a packet. Then, the channel within one block can be written as

$$y_j(t) = \sqrt{\rho} h_{i,j} x_i(t) + z_i(t), \quad t = 1, 2, \dots, T, \quad (3.1)$$

where ρ is the average received signal to noise ratio (SNR) at the destination. All the transmissions are made with equal power. In the above equation, the transmitter could be any of the sources or relays, the receiver could be any of the relays or destinations, as long as the transmitter and receiver are different (i.e., not the same relay). The channel coefficient $h_{i,j}$ between any two nodes is modeled as i.i.d. with zero-mean, circularly symmetric complex Gaussian random variables with common variance $1/\beta$. Therefore, $|h_{i,j}|^2$ is exponentially distributed with parameter $\beta \forall i, j$.

A total of NL bits are transmitted by all sources in $(N + M)T$ channel uses, therefore the system rate is $R = NL/[(N + M)T]$ bits per channel use (BPCU). The transmission rate R_0 for each packet transmission is identical, equal to $R_0 = L/T = R(N + M)/N$ BPCU.

The instantaneous mutual information of the channel model in (3.1) with Gaussian input is:

$$I(X_i; Y_j) = \log(1 + |h_{i,j}|^2 \rho), \quad (3.2)$$

where X_i and Y_j denote the transmitted symbol by node i and received symbol by node j . We assume that powerful enough channel codes can be applied within each packet such that if $I(X_i; Y_j) > R_0$, the packet can be decoded correctly. In case errors occur, we assume they can be detected. This can be realized through cyclic redundancy check (CRC) code or other parity check codes. When $I(X_i; Y_j) \leq R_0$, we say that the channel $h_{i,j}$ is in *outage*. Otherwise, we say that the channel $h_{i,j}$ is *operational*. Define $\tau = [2^{[R(N+M)]/N} - 1]/\rho$. Since $|h_{i,j}|^2$ is

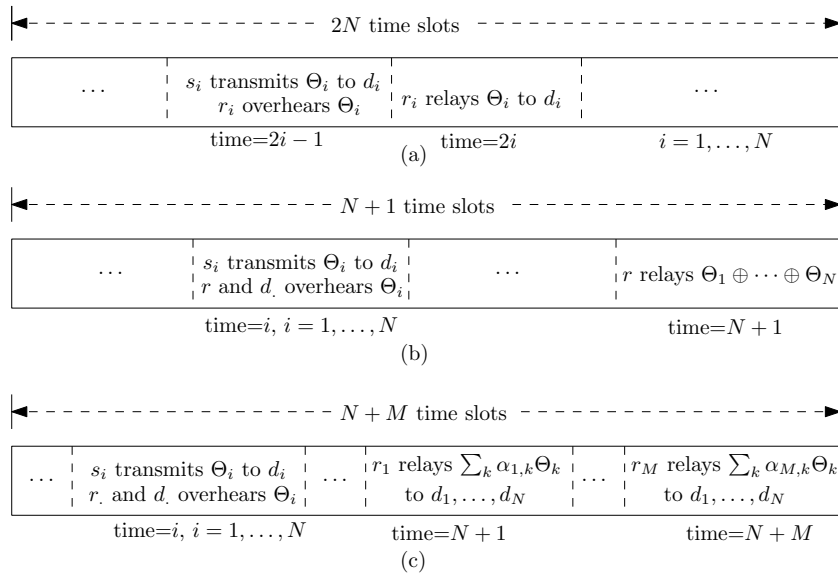


Figure 3.2 Time-division allocation for the different schemes compared: (a) CC (b) NCC (c) DNCC and RNCC

exponentially distributed, the outage probability for the channel in (3.1) is given by:

$$\begin{aligned}
 P_0 &= Pr(I(X_i; Y_j) < R_0) = Pr(|h_{i,j}|^2 < \tau) \\
 &= 1 - \exp(-\beta\tau) \cong \beta\tau,
 \end{aligned} \tag{3.3}$$

where we write $a(\tau) \cong b(\tau)$ if $\lim_{\tau \rightarrow 0} [a(\tau)/b(\tau)] = 1$.

3.2.2 Network Coded Cooperation

Our transmission scheme consists of two stages; see Fig. 3.2. In the first stage, direct transmissions from the sources to the destinations take place in N orthogonal time slots. Thanks to the broadcast nature of the wireless medium, all the destinations and the relays overhear the transmissions. At the end of the first stage, each relay tries to decode all N packets. Here one of the two strategies is possible:

1. Strategy \mathcal{A} : If a relay can successfully decode all the packets, then it participates in the second stage. Otherwise, it remains silent. In the second stage, the participating relays perform network coding. Specifically, relay i will transmit the linear combination

$$\sum_{k=1}^N \alpha_{ik} \Theta_k.$$

2. Strategy \mathcal{B} : If a relay can successfully decode at least one packet, then it participates in the second stage. Specifically, if relay i was able to decode the packets correctly from the sources in the set S_i where $S_i \subset \{1, \dots, N\}$, then it will transmit the linear combination $\sum_{k \in S_i} \alpha_{i,k} \Theta_k$.

Unless otherwise specified, we study the first case when the Strategy \mathcal{A} is used until Sec. 3.5. Strategy \mathcal{B} will be discussed in Sec. 3.5.

3.2.3 Deterministic and Random Network Coding

We will consider two network coding schemes for the user cooperation: random coding and deterministic coding. In the random coding approach, which we will refer to as Random Network Coded Cooperation (RNCC), relay r_i draws α_{ij} randomly from the finite field \mathbb{F}_q . After the random coefficients are drawn, a new packet is created by making a linear combination of the source data packets using the α_{ij} 's. In the deterministic approach which will be referred to as Deterministic Network Coded Cooperation (DNCC), the coefficients α_{ij} 's are predetermined and they are designed in a way to maximize the probability that the received linear combinations are actually decodable at the destination. We will discuss the problem of how to choose these predetermined coefficients in detail in Sec. 3.4.

In order to express the overall transmitted signal, we define the following matrix:

$$A := \begin{bmatrix} 1 & \dots & 0 & \alpha_{1,1} & \dots & \alpha_{M,1} \\ \vdots & \ddots & \vdots & \vdots & \dots & \vdots \\ 0 & \dots & 1 & \alpha_{1,N} & \dots & \alpha_{M,N} \end{bmatrix}^T \quad (3.4)$$

where $(\cdot)^T$ denotes transpose. Also define the $N \times K$ finite field vector corresponding to the original source packets as $\Theta = [\Theta_1^T, \Theta_2^T, \dots, \Theta_N^T]^T$. Using matrices A and Θ , we can express the potential transmitted signals by all the N sources and M relays, in that order, as $\Pi = A\Theta$ where $\Pi \in \mathbb{F}_q^{(N+M) \times K}$. Note that Π represents the *potential* transmitted signals, since due to severe fading some of the channels might be in outage and therefore only a subset of packets can be successfully decoded by some relays. Under Strategy \mathcal{A} , such relays will not participate in the second stage and the rows of A corresponding to these relays can be considered to

be deleted. Under Strategy \mathcal{B} , however, only the coefficients in A that correspond to the unsuccessful packets would be zero, as opposed to a whole row being deleted. Note that, from the destination d_i 's perspective, some of the channels might also be in outage. We denote the corresponding submatrix of A for destination d_i by A_i which satisfies $\Pi_i = A_i\Theta$ where Π_i denotes all correctly decoded packets at destination d_i .

3.3 Performance Analysis

3.3.1 Diversity-Multiplexing Tradeoff

As mentioned in the introduction, we will investigate the performance of the proposed scheme via DMT. DMT is accepted as a useful performance analysis tool in cooperative systems [40, 26]. For completeness, we give the formal definitions as in [2]. Let $P_e^i(\rho)$ denote packet error probability of user i at SNR ρ . Define $P_e = \min_i P_e^i$, $i = 1, \dots, N$, then a scheme is said to achieve spatial multiplexing gain r and diversity gain d if the data rate is $\lim_{\rho \rightarrow \infty} R(\rho)/\log(\rho) = r$, and the minimum error probability satisfies $\lim_{\rho \rightarrow \infty} \log(P_e(\rho))/\log(\rho) = -d$.

3.3.2 Main Result

Next we define a new parameter which plays a key role in the derivation of the outage probability and hence the achieved diversity order. For any integer $i \in [1, \min(m, n)]$, we define the Γ -rank, $\Gamma_i(C)$, of a $m \times n$ matrix C as an integer γ such that 1) any collection of γ rows of C is at least rank i , and 2) there exists a collection of $\gamma - 1$ rows of C that has rank $i - 1$. Next, we derive the DMT of the system as a function of $\Gamma_N(A)$.

Theorem 1. *The DMT of DNCC with N source-destination pairs and M intermediate relay nodes which choose their linear combination coefficients from the matrix A for multicast using Strategy \mathcal{A} is given by:*

$$d(r) = (N + M - (\Gamma_N(A) - 1)) \left[1 - \frac{N + M}{N} r \right], \quad (3.5)$$

where $r \in \left(0, \frac{N}{N+M}\right)$.

Proof. **3.3.2.1 Multicast**

In the multicast problem, the necessary and sufficient condition for destination d_i to recover Θ_i is $\text{rank}(A_i) = N$. To analyze the outage probability, we define the following events: $E_i \triangleq \{\text{rank}(A_i) < N\}$, and $E_i^{up} \triangleq \{A_i \text{ has at most } \Gamma_N(A) - 1 \text{ rows}\}$. Notice that, $E_i \subset E_i^{up}$ by the first condition in the definition of Γ -rank. By the second condition in the definition of Γ -rank, there exist a collection of rows of A that are rank $N - 1$. Let \tilde{A}_i denote a $(\Gamma_N(A) - 1) \times N$ submatrix of A that consists of such rows. Let F_m denote the event that m relays fail to receive all the Θ_i 's correctly. Define $E_i^{low} \triangleq \{F_0 \cap \{A_i = \tilde{A}_i\}\}$. It follows that $E_i^{low} \subset E_i$. Notice that the probability that any relay can successfully decode all N packets in the first stage is $P(S) = \prod_{i=1}^N Pr(I_{s_{i\tau}}(X; Y) > R_0) = \prod_{i=1}^N \exp(-\beta\tau) = \exp(-N\beta\tau)$. As a result,

$$P(F_m) = \binom{M}{m} P(S)^{M-m} (1 - P(S))^m. \quad (3.6)$$

Having N direct transmission from the sources and $M - m$ transmissions from the relays, each destination can potentially receive and decode $N + M - m$ packets. Let $E(N + M - m, l)$ denote the event that l out of $N + M - m$ channels were operational:

$$P(E(N + M - m, l)) = \binom{N + M - m}{l} P_0^{N+M-m-l} (1 - P_0)^l \quad (3.7)$$

where P_0 is given by (3.3). Since $E_i^{low} \subset E_i \subset E_i^{up}$, using (3.6) and (3.7) we have the following upper and lower bounds:

$$\begin{aligned} P(E_i) &\leq P(E_i^{up}) \\ &= \sum_{m=0}^M P(F_m) \cdot \sum_{l=0}^{\Gamma_N(A)-1} P(E(N + M - m, l)), \end{aligned} \quad (3.8)$$

$$\begin{aligned} P(E_i) &\geq P(E_i^{low}) \\ &= P(F_0) P_0^{N+M-(\Gamma_N(A)-1)} (1 - P_0)^{\Gamma_N(A)-1}. \end{aligned} \quad (3.9)$$

In (3.8), the first summation stands for the probability of the event that m of the relays fail to receive all Θ_i 's correctly, leaving us with only $M - m$ relays which will participate in the second stage. In total $N + M - m$ transmissions will be made. The destination d_i may not be able to recover all Θ_i 's, if only $\Gamma_N(A) - 1$ or less number of transmissions are successful.

Notice that, as $\rho \rightarrow \infty$, $\tau \rightarrow 0$. We need to find the following limit:

$$\lim_{\tau \rightarrow 0} \frac{P(E_i)}{\tau^{N+M-(\Gamma_N(A)-1)}}. \quad (3.10)$$

We consider the individual terms in the summations one-by-one and find the term with the smallest order of τ . Observe that $\lim_{\tau \rightarrow 0} (1 - P(S)) = N\beta$ and $P(F_m) \cong K_m \tau^m$ where K_m is:

$$\lim_{\tau \rightarrow 0} \frac{P(F_m)}{\tau^m} = \binom{M}{m} (N\beta)^m. \quad (3.11)$$

Similarly, $P(E(k, l)) \cong K_{k,l} \tau^{k-l}$ where $K_{k,l} = \binom{k}{l} \beta^{k-l}$. The smallest order τ term happens when l is equal to $\Gamma_N(A) - 1$. Hence, we have:

$$\lim_{\tau \rightarrow 0} \frac{P(F_m)}{\tau^m} \cdot \frac{P(E(N+M-m, \Gamma_N(A)-1))}{\tau^{N+M-m-(\Gamma_N(A)-1)}} = K_m K_{N+M-m, \Gamma_N(A)-1} \triangleq K_{up},$$

and

$$P(E_i^{up}) \cong K_{up} \tau^{N+M-(\Gamma_N(A)-1)} = K_{up} \left(\frac{2^{\frac{N+M}{N}} R - 1}{\rho} \right)^{N+M-(\Gamma_N(A)-1)}. \quad (3.12)$$

Similarly, $P(E_i^{low}) \cong K_{low} \tau^{N+M-(\Gamma_N(A)-1)}$, where $K_{low} = \beta^{N+M-(\Gamma_N(A)-1)}$. Now, choosing the fixed rate to be $R = r \log \rho$ and substituting into (3.12), we obtain:

$$P(E_i) \cong K \rho^{\left(\frac{N+M}{N} r - 1\right)(N+M-(\Gamma_N(A)-1))} \quad (3.13)$$

where $K_{low} \leq K \leq K_{up}$, which is the desired result.

3.3.2.2 Unicast

In unicast we have a different problem: given the received packets Y_i at destination d_i , we would like to recover only Θ_i from the set of linear equations $Y_i = A_i \Theta$. The error can only happen when the direct link is in outage. Notice that this implies that A_i does not contain e_i (the i 'th row of the $N \times N$ identity matrix $I_{N \times N}$). In this case, a necessary and sufficient condition for Θ_i to be recoverable is that $e_i \in \text{span}(A_i)$, where $\text{span}(A_i)$ is the row-space of A_i . Here, we make another rank definition that will be useful for the proof of the unicast scenario. We define the Λ_i -rank, $\Lambda_i(C)$ of a $m \times n$ matrix C as an integer λ such that 1) any collection of λ rows of C spans a space that contains e_i but 2) there exists a collection of $\lambda - 1$ rows of C

which does not span a space that contains e_i . The DMT of the system as a function of $\Lambda_i(A)$ is given by the following lemma.

Lemma 3. *DMT of DNCC for unicast for the i^{th} destination is*

$$d_i(r) = (N + M - (\Lambda_i(A) - 1)) \left[1 - \frac{N + M}{N} r \right], \quad (3.14)$$

where $r \in \left(0, \frac{N}{N+M}\right)$.

Proof. See the Appendix A. □

Notice that from the definition of Γ -rank, we have $\Gamma_N(A) = \max_i \Lambda_i(A)$. Since the error probability P_e is defined to be the minimum of individual error probabilities, we have $d(r) = \min_i d_i(r)$. After substituting $d_i(r)$ in (3.14), we obtain the desired result in (3.5). □

Corollary 1. *The maximum diversity is achieved if and only if $\Gamma_N(A) = N$.*

Proof. The result follows immediately from (3.5). □

3.4 Design of the Linear Network Coding Matrix

In this section, we try to design a network coding matrix A that can yield the maximum diversity order. Notice that, by definition we have $\Gamma_N(A) \geq N$. Therefore, it is clear from Corollary 1 that we need to pick an A that satisfies $\Gamma_N(A) = N$. Before going into the discussion on the design of the matrix A , we would like to give another important rank definition that will be used in the design of A .

The *row Kruskal-rank* [69, 70] of A , denoted by $\kappa(A)$, is the number r such that every set of r rows of A is linearly independent, but there exist one set of $r + 1$ rows that are linearly dependent.

Lemma 4. $\kappa(A) = N \Leftrightarrow \Gamma_N(A) = N$.

Proof. We prove $\Gamma_N(A) = N \Rightarrow \kappa(A) = N$; the other case is straightforward. When $\Gamma_N(A) = N$, from the definition of Γ -rank any collection of N rows of A is at least rank N . But since

$\text{rank}(A) \leq N$, we have the first condition for the Kruskal-rank. Also since $\text{rank}(A) \leq N$, any $N + 1$ rows will be linearly dependent. \square

The minimum Hamming distance d_{\min} between any two codewords for a (n, k) error-correcting code is upper bounded by the Singleton bound as $d_{\min} \leq n - k + 1$. The codes that achieve this bound are called MDS codes [71]. The following result relates the column Kruskal-rank of the parity-check matrix H of a linear block code to its minimum distance d_{\min} : $d_{\min} = \kappa(H) + 1$. This follows from a theorem in [71, p. 318], which states that a code is MDS if and only if (iff) every $n - k$ columns of its parity check matrix H are linearly independent.

The transpose H^T of the parity check matrix of a systematic $(N + M, M, N + 1)$ MDS code can be used as an encoding matrix A for our DNCC scheme to minimize the total number of packets necessary at the destinations for decoding the source packets. If such an A is used, then each destination needs and only needs N packets (from the sources and relays) for correct decoding. Note that depending on the sizes N and M , finding a $(N + M, M, N + 1)$ MDS code may or may not be possible in a given finite field \mathbb{F}_q [71, 72].

3.4.1 Network Code Designs from Reed-Solomon Codes

Reed-Solomon (RS) Codes are MDS codes. There are two ways of constructing an RS Code: either using the Vandermonde matrices [73] or using the Cauchy matrices [74, Sec. 4.3]. Because of the special structure of A in (3.4), we will be working on systematic RS codes.

3.4.1.1 Construction based on Cauchy Matrices

The systematic generator matrix for the $\text{RS}(n, k)$ code has the form $G = [I|C]$ where I is the identity matrix of order k and C is a $k \times (n - k)$ matrix [74] and G satisfies $\kappa(G^T) = n - k$. C is known as Cauchy matrix and is given by:

$$C_{i,j} = \frac{u_i v_j}{x_i + y_j}, \quad 0 \leq i \leq k - 1, \quad 0 \leq j \leq n - k - 1. \quad (3.15)$$

where u_i, v_j, x_i and y_j are elements of $GF(2^m)$ and are defined as:

$$\begin{aligned} x_i &= \beta^{n-1-i}, \quad 0 \leq i \leq k-1, \\ y_j &= \beta^{n-1-k-j}, \quad 0 \leq j \leq n-k-1, \\ u_i &= \frac{1}{\prod_{0 \leq l \leq k-1, l \neq i} (\beta^{n-1-i} - \beta^{n-1-l})}, \quad 0 \leq i \leq k-1, \\ v_j &= \prod_{0 \leq l \leq k-1} (\beta^{n-1-k-j} - \beta^{n-1-l}), \quad 0 \leq j \leq n-k-1, \end{aligned}$$

where β is the primitive element for \mathbb{F}_q . Therefore, choosing $n = N + M$ and $k = M$, we construct the network code $A = [I|\alpha]$ by choosing $\alpha_{i,j} = C_{i,j}$ which gives $\kappa(A) = N$.

3.4.1.2 Construction based on Vandermonde Matrices

The Vandermonde matrices are defined from a vector of m distinct generating elements $\{t_1, \dots, t_m\}$ of \mathbb{F}_q as:

$$V_{m \times n} := \begin{bmatrix} 1 & t_1 & t_1^2 & \dots & t_1^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & t_m & t_m^2 & \dots & t_m^{n-1} \end{bmatrix}. \quad (3.16)$$

The determinant for the square Vandermonde matrix is given by $\det(V_{n \times n}) = \prod_{1 \leq i < j \leq n} (t_j - t_i)$ and V_n is nonsingular iff all the t_i 's are distinct. To construct A for given N and M , we do the following:

1. Choose a suitable \mathbb{F}_q with $q = 2^l \geq N + M$.
2. Choose $N + M$ distinct elements t_1, t_2, \dots, t_{N+M} of \mathbb{F}_q .
3. Construct the Vandermonde matrix $V_{N \times N}$ from t_1, \dots, t_N and $V_{M \times N}$ from t_{N+1}, \dots, t_{N+M} .
4. Then $\alpha_{i,j} = (V_{M \times N} V_{N \times N}^{-1})_{i,j}$ and $A = [I|\alpha^T]^T$.

Note that the generating elements that are needed in the construction of RS codes from Vandermonde matrices requires an extra property that they should be the consecutive powers of the primitive element $\beta \in \mathbb{F}_q$, i.e. $\beta, \beta^2, \dots, \beta^{2t}$ for a t -error correcting RS code. We do not need or impose this requirement.

Lemma 5. Let $T \in \mathbb{F}_q^{n \times n}$ be an invertible matrix. Then, for any $H \in \mathbb{F}_q^{m \times n}$: $\Gamma_i(H) = \Gamma_i(HT)$ and $\kappa(H) = \kappa(HT)$, $\forall 1 \leq i \leq \min(m, n)$.

Proof. Pick $i \in (1, \min(m, n))$ arbitrary rows from H and denote the resulting matrix by H' . We need to show that if the rows of H' are linearly dependent or linearly independent then so are the rows of $H'T$. This is the case because T is full-rank and hence $xH' = 0$ implies and is implied by $xH'T = 0$ for any $x \in \mathbb{F}_q^{1 \times i}$. \square

Picking $H = [V_{N \times N} | V_{M \times N}]$ and $T = V_{N \times N}^{-1}$ and using Lemma 5 we have $\Gamma_N(G) = \kappa(G) = N$. Note that since we need $N + M$ distinct elements of the finite field \mathbb{F}_q , it is enough to have $q \geq N + M$. Next, we give an example for the case when $N = 2$ and $M = 2$ [24].

Example: Consider a $[n, k, d] = [4, 2, 3]$ MDS code \mathcal{C} over $\mathbb{F}_4 = \{0, 1, \alpha, \beta = \alpha^2 = \alpha + 1\}$ with symbol representations as $\{0 = (0, 0), 1 = (0, 1), \alpha = (1, 0), \beta = (1, 1)\}$. Constructing the Vandermonde matrices from the set $\{0, 1, \alpha, \beta\}$ and multiplying with the inverse, we have

$$V = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha & \beta \end{pmatrix}^T \quad A = \begin{pmatrix} 1 & 0 & \beta & \alpha \\ 0 & 1 & \alpha & \beta \end{pmatrix}^T. \quad (3.17)$$

Let $K = 1$ and $b_i = [b_{i,1}, b_{i,2}]$, $\Theta_i = [\theta_{i,1}]$, $i = \{1, 2\}$. If the above encoder matrix is used, relays will transmit the linear combinations $\beta\theta_{1,1} + \alpha\theta_{2,1}$, $\alpha\theta_{1,1} + \beta\theta_{2,1}$ respectively. For example for the first relay, this operation will be performed using regular addition in \mathbb{F}_2 as $(b_{1,2} + b_{2,1} + b_{2,2}, b_{1,1} + b_{1,2} + b_{2,1})$ and for the second relay $(b_{1,1} + b_{1,2} + b_{2,2}, b_{1,1} + b_{2,1} + b_{2,2})$ which can be put in the matrix form as:

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} b_{1,1} \\ b_{1,2} \\ b_{2,1} \\ b_{2,2} \end{pmatrix}. \quad (3.18)$$

Notice that since $\kappa(A) = 2$ and the destination will be able to recover Θ_1, Θ_2 when at least two of the transmissions are successful. It is important to emphasize that unlike MDS code construction that we gave earlier, here we do not have any restrictions on the code size for any given N and M , we can find a large enough finite field \mathbb{F}_q satisfying $q = 2^l, l \geq N + M$.

3.5 Discussions and Further Improvements

In the previous sections, we have established the DMT of DNCC for a given network coding matrix A , and designed the network coding matrix A for maximum diversity order. In this section, we study Strategy \mathcal{B} , and the case when only some selected relays are allowed to transmit. We also investigate the performance of RNCC.

3.5.1 Strategy \mathcal{B}

The assumption that the relay has to decode all the packets in order to be able to cooperate may be too restrictive for such schemes. We could relax this assumption and assume that the relays will participate cooperation even though they have not been able to decode all the packets.

Denote the outage event under Strategy \mathcal{B} by $E_i^{\mathcal{B}}$. Notice that under Strategy \mathcal{B} , not only the $M - m$ relays as in (3.6) but also the rest of the m relays contributes to the decoding at the destinations. Clearly the probability of not being able to solve the linear system of equations will decrease and hence the performance will get better, i.e. $P(E_i^{\mathcal{B}}) \leq P(E_i)$. Taking $\Gamma_N(A) = N$, the probability of E_i^{low} becomes $P(E_i^{low}) = P(F_0)P_0^{M+1}(1 - P_0)^{N-1}$. We have $P(E_i^{low}) \leq P(E_i^{\mathcal{B}}) \leq P(E_i)$. But using a similar analysis as in the proof of Theorem 1, it can be shown that even though Strategy \mathcal{B} offers lower packet error rate, the DMT is the same as that of Strategy \mathcal{A} . That is, even though Strategy \mathcal{B} improves the packet error rate performance, the DMT remains unchanged.

3.5.2 RNCC

In RNCC the linear combination coefficients $\alpha_{i,j}$'s are chosen randomly from a finite field \mathbb{F}_q . Similar to the deterministic case, destination d_i cannot recover Θ_i when the submatrix A_i is rank deficient, i.e. $E_i = \text{rank}(A_i) < N$. However, unlike the deterministic case there are two possible reasons to have a rank deficient A_i : one is due to fading and the other is due to the choice of the random coefficients α_{ij} 's. The former happens when at most $N - 1$ channels are operational resulting in an A_i matrix that has at most $N - 1$ rows. We define this event

to be the deterministic error event: $E_i^{det} = \{A_i \text{ has at most } N - 1 \text{ rows}\}$. The probability of this event is given by $P(E_i^{det}) = \sum_{m=0}^M P(F_m) \cdot \sum_{l=0}^{N-1} P(E(N + M - m, l))$. Notice that $E_i^{det} \subset E_i$. On the other hand, due to the random choice, relays may choose linearly dependent coefficients which will result in an A_i matrix such that $rank(A_i) < N$. Denote this event by E_i^{ran} . But by the Corollary 1, this event will result in the outage events that have diversity order less than $M + 1$. Therefore, the key idea of this proof is to isolate such events, and show that the probability of such events can be bounded by the field size as follows:

$$\begin{aligned} P(E_i) &= P(E_i|E_i^{det})P(E_i^{det}) + P(E_i|E_i^{ran})P(E_i^{ran}) \\ &= P(E_i^{det}) + P(E_i|E_i^{ran})P(E_i^{ran}) \\ &\leq P(E_i^{det}) + P(E_i|E_i^{ran}). \end{aligned}$$

Lemma 6. *The probability that any $N \times N$ square submatrix A'_i of A_i is rank deficient is upper bounded by $P(E_i|E_i^{ran}) \leq N/q$.*

Proof. The proof consists of an application of the Schwartz-Zippel Lemma to a carefully chosen error event as in the proof of [75, Thm. 2]. The worst case scenario happens when all the channels between the sources and the destination are in outage and $A'_i = A_i$. This is the worst case scenario since if k sources are not in outage, then we only need to consider the determinant of $(N - k) \times (N - k)$ submatrix of A_i whose probability of being rank deficient is less than that of $N \times N$ matrix. And since A_i has at least N rows when we condition on the event E_i^c , it is clear that the probability of having a rank deficient A_i matrix in the case when $A'_i \neq A_i$ is smaller than the case when $A'_i = A_i$. Then considering the case when $A'_i = A_i$, since the determinant of A_i is a polynomial in terms of the indeterminate α_{ij} 's with degree N , using Schwartz-Zippel Lemma we have the desired result. The bound can be further improved as in [Lemma-4,[75]] to be $1 - \left(1 - \frac{1}{q}\right)^N$. \square

Lemma 6 indicates that if the field size is large enough, the error event will be dominated by E_i with high probability: $\lim_{q \rightarrow \infty} P(E_i) \leq P(E_i^{det}) + \lim_{q \rightarrow \infty} N/q = P(E_i^{det})$.

Note that, although the limit is taken asymptotically with $q \rightarrow \infty$, it is enough to have $q \cong \rho^{M+1}$. The rest of the proof is the same with the above proof for DNCC. Below we

summarize all the above proved results with the following theorem:

Theorem 2. *DNCC with M intermediate relay nodes which choose their linear combination coefficients from the rows of A that satisfies $\Gamma_N(A) = N$ and N source nodes achieves the DMT in both the multicast and unicast scenario and under both strategies \mathcal{A} and \mathcal{B} :*

$$d(r) = (M + 1) \left[1 - \frac{(N + M)}{N} r \right], r \in \left(0, \frac{N}{N + M} \right).$$

RNCC achieves the same DMT with probability at least $1 - \frac{N}{q}$, where q is the field size.

3.5.3 Selection Relaying

We can also consider the case where not all of the M relays transmit, but only K selected relays transmit. The same selection rule based on the instantaneous wireless channel conditions can be adapted as in [40]. Define

$$h_i \triangleq \min\{|h_{s_1 r_i}|^2, |h_{r_i d_1}|^2, \dots, |h_{s_N r_i}|^2, |h_{r_i d_N}|^2\}. \quad (3.19)$$

Then, select the K relays that maximizes h_i , namely first choose r with the rule: $r = \arg \max_{r_i} h_i$ and continue the same process of choosing the maximum in the beginning of each relay transmission. Note that a relay can be selected more than one time. This selection mechanism can be implemented using a distributed protocol at the network layer as in [26]: relays choose a timer that is inversely proportional to the quality of their channels. Relays assess the quality of their channels from the request-to-send and clear-to-send (RTS-CTS) packets that were transmitted by the source and destination nodes respectively¹. No channel state information (CSI) is required at the physical layer. Next, we give the DMT of this scheme.

Theorem 3. *DNCC scheme with the selection of the best K relay nodes out of M and N source nodes, $\Gamma_N(A) = N$ in the multicast scenario achieves the DMT:*

$$d(r) = (K + 1) \left(1 - \frac{(N + K)}{N} r \right), \quad r \in \left(0, \frac{N}{N + K} \right)$$

¹Forward and backward channels between the relays and the destinations are assumed the same due to reciprocity [76].

if $K < N - 1$, and otherwise achieves the DMT:

$$d(r) = (N + M(K - (N - 1))) \left(1 - \frac{N + K}{N} r\right), \quad (3.20)$$

where $r \in \left(0, \frac{N}{N+K}\right)$.

Proof. See the Appendix B. □

In [26], for a single source single destination setup it was proved that instead of transmitting from all the M relays, if a selection is performed and only the relay with the best channel coefficient transmits then the bit error rate (BER) at the destination enjoys a M -fold diversity gain. Inspired by this idea, the authors in [40] proposed a NCC scheme for N s-d pairs and M relays where only the “best” relay selected according to (3.19), XOR’s all the source packets and transmits to the destination (Fig. 3.2 (b)). However, the M -fold diversity order can only be achieved when an unrealistic assumption is made. The assumption is that the destination has to be able to decode all the other source packets successfully. When no such assumption is made, no gain from the selection process is obtained and only a diversity order of one is achieved. The significance of our result in Theorem 3 is that if enough number of relays could be used ($K \geq N - 1$), we can achieve $N + M(K - (N - 1))$ diversity order.

3.6 Comparison with Other Schemes

3.6.1 DMT Comparison

In this section, we would like to compare DMT of the previously proposed schemes in the literature. The closest scheme in the literature is the NCC scheme considered in [40]. In NCC instead of all the relays, only one relay transmits which results in total of $N + 1$ time slots. Using fewer time-slots NCC achieves a better spectral efficiency than the proposed scheme here. However, NCC can only provide a fixed diversity order of two, while the proposed scheme achieves the maximum diversity order of $M + 1$.

In the following, for comparison we include the DMT performance of NCC and that of CC which includes space-time coded protocols [35] and selection relaying [26]. The diversity-multiplexing tradeoff of NCC is given by [40]: $d(r) = 2(1 - r(N + 1)/N)$, $r \in (0, N/(N + 1))$.

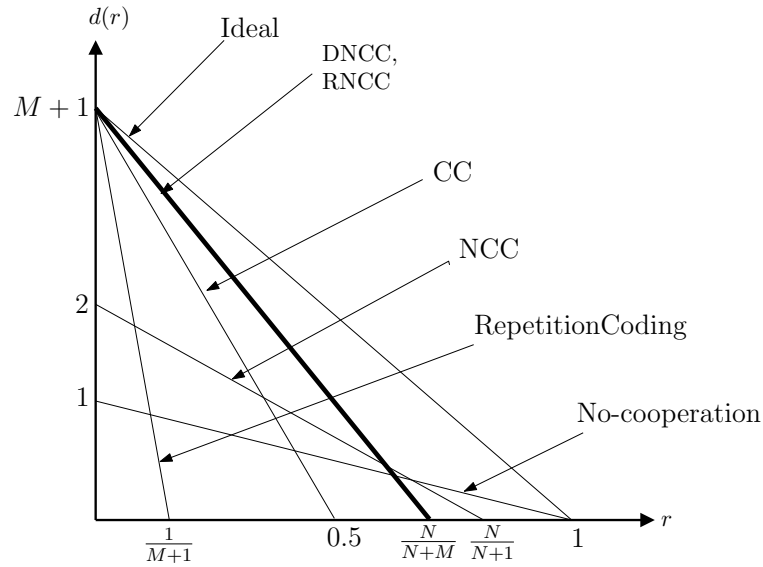


Figure 3.3 DMT comparison of various schemes

The DMT of the decode and forward strategy with M intermediate relay nodes is given by [35]: $d(r) = (M + 1)(1 - 2r)$, $r \in (0, 0.5)$.

To show the advantage of the proposed schemes, we present DMT of the existing schemes and the proposed schemes in Fig. 3.3. As can be seen from the figure, both of the proposed schemes and CC provide the maximum diversity order of $M + 1$ when $r \rightarrow 0$. However, the proposed schemes can provide a higher diversity gain than CC when the spectral efficiency increases.

3.6.2 Monte-Carlo Simulation

Here, we compare these schemes with the existing schemes via Monte-Carlo simulations. In the simulations, we only consider the channel conditions so as to isolate the diversity benefits. We generate an $(N + M) \times N$ and an $N \times N$ matrix that contains the channel coefficients for each destination and each relay, respectively. Then, we decide that the transmission is successful for any link if the instantaneous channel is strong enough to support the given data rate and we update combining coefficients accordingly. After all the transmissions take place, we perform Gaussian elimination on the updated combining coefficient matrices to conclude whether each destination d_i is able to recover the source packet Θ_i . We set $\beta = 1$ and $R_0 = 1$

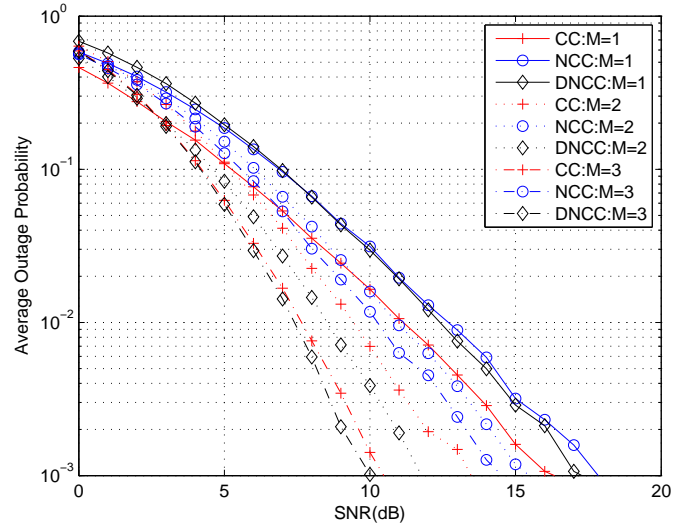


Figure 3.4 Average outage probability per destination, ($N = 2$, $M = 1, \dots, 3$)

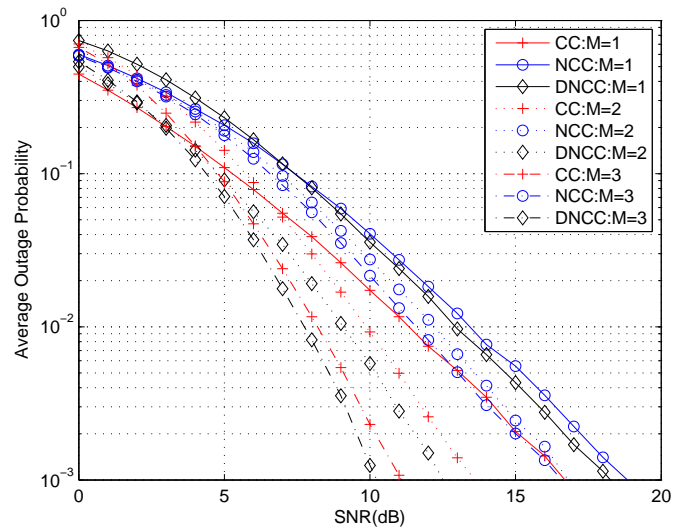


Figure 3.5 Average outage probability per destination, ($N = 3$, $M = 1, \dots, 3$)

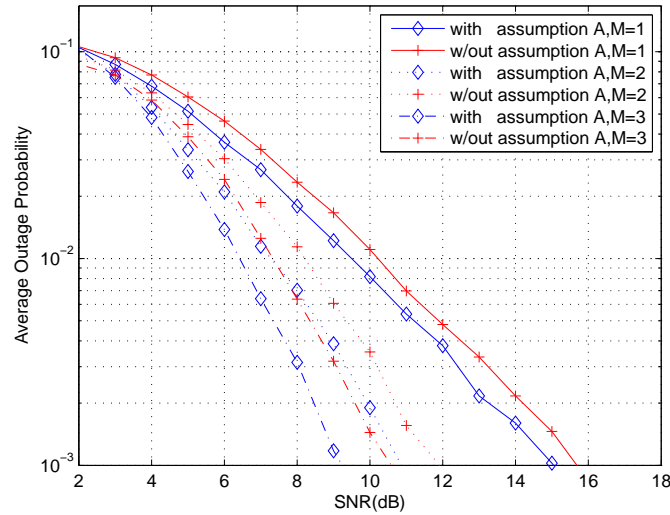


Figure 3.6 Average outage probability per destination, ($N = 2$, $M = 1, \dots, 3$)

BPCU. In all the figures only the unicast scenario is adapted since CC cannot be implemented in a multicast scenario. As can be seen from Fig. 3.4 and Fig. 3.5, the proposed schemes are able to provide the $M + 1$ diversity order and outperform the other schemes.

Theorem 2 claims that the performance loss incurred due to the assumption under Strategy \mathcal{A} is not in terms of diversity gain but it is in terms of coding gain. This is validated through Monte-Carlo simulations as shown in Fig. 3.6 and Fig. 3.7.

3.7 Conclusions

We studied the network coded cooperation schemes for N source-destination pairs assisted with M relays. We studied two different traffic network models: multicast and unicast. The proposed schemes allow the relays to apply network coding on the data it has received from its neighbors. We allow the relays to linearly combine the packets with coefficients either deterministically pre-designed or drawn from a finite field randomly. We established the diversity-multiplexing tradeoff performance of the proposed schemes for any network coding matrix, and showed its advantage over the existing schemes when the coding matrix is optimized. Specifically, it is capable of achieving the maximum diversity order $M + 1$ at the expense of

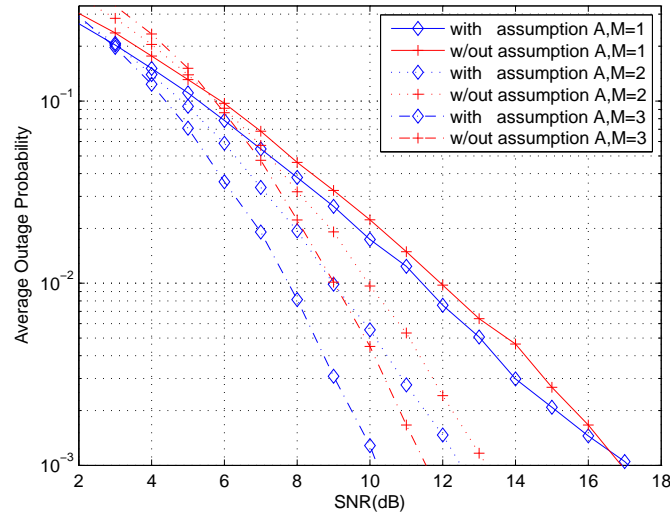


Figure 3.7 Average outage probability per destination, ($N = 3$, $M = 1, \dots, 3$)

a slightly reduced multiplexing rate. We derived the necessary and sufficient conditions to achieve the maximum diversity order. We showed that when the parity-check matrix for a $(N + M, M, N + 1)$ systematic MDS code is used as the network coding matrix, the maximum diversity is achieved. We presented two ways to generate the network coding matrix: using either the Cauchy matrices or the Vandermonde matrices. Both constructions guarantee maximum diversity order. When a relay selection is possible, we show that a multiplicative effect on the diversity order is possible when enough rounds of relay selection is performed.

CHAPTER 4. Interference Alignment for Wired Networks with General Message Demands

4.1 Introduction

Since its introduction in [1], *network coding* has been accepted as a successful technique for achieving high throughput with more robustness and energy savings. Ahlswede et al. proved that network coding achieves the max-flow value in a single-source *multicast* setup which would otherwise have been impossible to achieve by simple routing. In spite of the clear gain over routing in the multicast setup [7], the gains that network coding has to offer over routing in the *multiple unicast* setup is still yet to be understood. A conjecture appeared in 2004 by Li and Li [11] for undirected graphs which claims that use of network coding does not lead to any gain over routing. Also it was shown in [9] that there exist a solvable network which does not have a linear solution over any ring R , any finite R -module G and any vector dimension. Partly due to the difficulty in the analytical tractability of the nonlinear solutions, linear solutions are still popular and being proposed [47, 48].

Another important technique that recently emerged for wireless communications is the *interference alignment* [77, 3, 78, 42]. Because of the broadcast nature of the wireless medium, interference becomes one of the dominant factors of performance degradation in wireless networks. In [3], Cadamba and Jafar showed that if interference at the receivers are aligned by choosing appropriate precoding matrices at the source nodes, then interference space could be minimized. In a K user setup, they showed that it is possible for each user to achieve half of the rate that is possible in the absence of interference. Later, this result is extended to K sources J destination nodes with arbitrary message demands by [46].

Recently, authors in [47, 48] proposed to use the interference alignment technique in the

wired networks. In a three source three destination node setup, they were able to show that each user can achieve a rate of one half when the min-cut is one and the network transfer functions satisfy certain conditions. 3 unicast connections also considered in [79] where authors characterize the feasibility of the connections based on the connectivity levels which is defined as the number of edge-disjoint paths between the source-destination pairs.

In this thesis, we extend the idea of using interference alignment in wired networks to more general networks. We consider networks with K source nodes and J destination nodes with arbitrary message demands. We first consider a simple network consisting of three source nodes and four destination nodes and show that each user can achieve a rate of one half. Then we give the result for the general case which states that when the min-cut between each source-destination pair is one, it is possible to achieve a sum rate that is arbitrarily close to the min-cut between the source nodes whose messages are demanded and the destination node where the sum rate is the summation of all the demanded source message rates plus the biggest interferer's rate.

Rest of the chapter is organized as follows. Sec. 4.2 introduces the system model and formulation of the problem that is studied. Sec. 4.3 presents the proposed approach and illustrates it on a simple network consisting of three sources and four destinations. Then Sec. 4.4 generalizes the result to more general networks consisting of K sources and J destinations. Finally, Sec. 4.6 summarizes and concludes the chapter.

4.2 General System Description

The network studied in this chapter is composed of K source nodes s_1, \dots, s_K , and J destination nodes d_1, \dots, d_J with arbitrary number of intermediary relay nodes in between. The network is assumed to be representable by a directed and acyclic graph $G = (V, E)$ where V is the set of nodes, and E is the set of directed edges. Each edge $e \in E$ has unit capacity and can transmit one symbol from a finite field \mathbb{F}_q per unit time. Each source message is independent of rest of the source messages. Each directed edge is an error-free channel and the transmissions from different edges do not interfere with each other. The interference that we

try to combat in this problem occurs only as a result of the application of network coding at the intermediary nodes. Here, we consider destination nodes with arbitrary message demands meaning d_i is interested in a subset of the source messages.

Linear network coding is employed at the intermediary nodes in the usual sense by choosing coefficients from \mathbb{F}_q and making a linear combination of the symbols received from the incoming edges. The number of these coefficient vectors a_i 's depends on the number of outgoing and incoming edges. Define all the coefficients to be used by $a = [a_1 \dots a_s] \in \mathbb{F}_q^s$. Let X_i denote the source s_i 's input vector. Let $t = 1, 2, \dots$ denote the channel use index, and let a^t denote the linear combination coefficients used during the channel use t .

We know from [6] that, when intermediary nodes apply network coding, we can represent the input output relation at the destination nodes using a transfer matrix M as follows:

$$Y_j(t) = \sum_{k=1}^K M_{jk}(a^{(t)})X_k(t). \quad (4.1)$$

Assume that the min-cut between s_k and r_j is c_{jk} and that $c_j = \max_k c_{jk}$, then M_{jk} is a $c_j \times c_{jk}$ matrix whose elements are polynomials that belong to the polynomial ring $\mathbb{F}_q[a]$, $X_k \in \mathbb{F}_q^{c_{jk} \times 1}$ the input vector at source node s_k and $Y_j \in \mathbb{F}_q^{c_j \times 1}$ is the received vector at the destination node d_j during the channel use t . The problem can be formulated as follows: given the min-cut values c_{jk} 's, what is the maximum achievable total throughput of all users?

In the next section, we start considering a simple network with three source nodes ($K = 3$) and four destination nodes ($J = 4$) and $c_i = 1$. Receivers 1 and 4 are interested in the message of source node s_1 and receivers 2 and 3 are interested in the messages of the source nodes s_2 and s_3 respectively. For this example we show that for a broad class of these networks it is possible to achieve a throughput of $1/2$ for each source node when the min-cut for each source-destination pair is 1. Then we generalize the result to arbitrary number of source and destination nodes and show that it is possible to achieve a sum rate that is arbitrarily close to the min-cut between the source nodes whose messages are demanded and the destination node where the sum rate is the summation of all the demanded source message rates plus the biggest interferer's rate. Before we move on to the next section we quote the Schwartz-Zippel Lemma from [47] which will be very useful in the sequel.

Lemma 7. *Let $p(x_1, x_2, \dots, x_n)$ be a non-zero polynomial in the polynomial ring $\mathbb{F}[x_1, x_2, \dots, x_n]$, where \mathbb{F} is a field. If $|\mathbb{F}|$ is greater than the degree of p in every variable x_j , there exist $r_1, r_2, \dots, r_n \in \mathbb{F}$ such that $p(r_1, r_2, \dots, r_n) \neq 0$.*

4.3 Simple Case: Three Source Four Destination Nodes

Consider a time expansion model of this network for $\tau = 2(l+1)^4$, where l is a positive integer. Taking b as the block index, $c_i = 1$ and using (4.1) we have,

$$\begin{aligned} Y_1(b) &= M_{11}(b)X_1(b) + M_{12}(b)X_2(b) + M_{13}(b)X_3(b), \\ Y_2(b) &= M_{21}(b)X_1(b) + M_{22}(b)X_2(b) + M_{23}(b)X_3(b), \\ Y_3(b) &= M_{31}(b)X_1(b) + M_{32}(b)X_2(b) + M_{33}(b)X_3(b), \\ Y_4(b) &= M_{41}(b)X_1(b) + M_{42}(b)X_2(b) + M_{43}(b)X_3(b), \end{aligned} \quad (4.2)$$

where $X_i(b), Y_i(b) \in \mathbb{F}_q^\tau$ are the time expanded version of each input and output symbol and $M_{ij}(b) \in \mathbb{F}_q^{\tau \times \tau}$'s are diagonal matrices. Take the message symbols at the sources to be $Z_1 \in \mathbb{F}_q^{(l+1)^4}$, $Z_2 \in \mathbb{F}_q^{l(l+1)^3}$ and $Z_3 \in \mathbb{F}_q^{l^4}$. Then the input symbols at the sources can be expressed using the corresponding precoding matrices V_i 's as $X_i = V_i Z_i$, $i \in \{1, 2, 3\}$ where specifically $V_1 \in \mathbb{F}_q^{\tau \times (l+1)^4}$, $V_2 \in \mathbb{F}_q^{\tau \times l(l+1)^3}$ and $V_3 \in \mathbb{F}_q^{\tau \times l^4}$. Notice that V_i 's have to be full-rank matrices since otherwise different Z_i 's could be mapped to the same X_i .

First we give the interference alignment requirements for the model given in (4.2). We want to choose precoding matrices such that the interference from source 2 and 3 is aligned at r_1 and r_4 :

$$\begin{aligned} \text{span}(M_{13}V_3) &\subseteq \text{span}(M_{12}V_2) \\ \text{rank}[M_{11}V_1 \quad M_{12}V_2] &= (l+1)^4 + l(l+1)^3 \\ \text{span}(M_{43}V_3) &\subseteq \text{span}(M_{42}V_2) \\ \text{rank}[M_{41}V_1 \quad M_{42}V_2] &= (l+1)^4 + l(l+1)^3. \end{aligned} \quad (4.3)$$

Similarly, we want to align the interference from source 1 and 3 at r_2 :

$$\text{span}(M_{23}V_3) \subseteq \text{span}(M_{21}V_1) \quad (4.4)$$

$$\text{rank}[M_{21}V_1 \quad M_{22}V_2] = (l+1)^4 + l(l+1)^3.$$

And finally, we want to align the interference from source 1 and 2 at r_3 :

$$\text{span}(M_{32}V_2) \subseteq \text{span}(M_{31}V_1) \quad (4.5)$$

$$\text{rank}[M_{31}V_1 \quad M_{33}V_3] = (l+1)^4 + l^4.$$

We adapt the same framework in [46] for the choices of the precoding matrices. Before we give the precoding matrices, please note that M_{ij} 's are assumed to have well-defined inverses. We will formalize this assumption more precisely using network transfer functions $m_{ij}(a)$'s in the sequel. First define,

$$\begin{aligned} T_{2,3}^{[1]} &= M_{12}^{-1}M_{13}, & T_{1,3}^{[2]} &= M_{21}^{-1}M_{23} \\ T_{1,2}^{[3]} &= M_{31}^{-1}M_{32}, & T_{2,3}^{[4]} &= M_{42}^{-1}M_{43} \end{aligned} \quad (4.6)$$

then choose precoding matrices such as:

$$V_1 = \left\{ (T_{2,3}^{[1]})^{\alpha_1} (T_{1,3}^{[2]})^{\alpha_2} (T_{1,2}^{[3]})^{\alpha_3} (T_{2,3}^{[4]})^{\alpha_4} \mathbf{1}_\tau : \alpha_i = \{0, 1, \dots, l\}, i = 1, \dots, 4 \right\} \quad (4.7)$$

$$V_2 = \left\{ (T_{2,3}^{[1]})^{\alpha_1} (T_{1,3}^{[2]})^{\alpha_2} (T_{1,2}^{[3]})^{\alpha_3} (T_{2,3}^{[4]})^{\alpha_4} \mathbf{1}_\tau : \begin{array}{l} \alpha_i = \{0, 1, \dots, l\}, i \neq 3 \\ \alpha_3 = \{0, 1, \dots, l-1\} \end{array} \right\} \quad (4.8)$$

$$V_3 = \left\{ (T_{2,3}^{[1]})^{\alpha_1} (T_{1,3}^{[2]})^{\alpha_2} (T_{1,2}^{[3]})^{\alpha_3} (T_{2,3}^{[4]})^{\alpha_4} \mathbf{1}_\tau : \alpha_i = \{0, 1, \dots, l-1\} \right\} \quad (4.9)$$

where $\mathbf{1}_\tau$ is the all-1 vector of dimension τ .

Note that this choice of the precoding matrices guarantees that the span conditions are met. To satisfy the rank requirements, note that all the V_i 's should be full-rank. Since $V_i \subseteq V_1$ where $i = \{2, 3\}$, it is enough to show that V_1 is full-rank. V_1 is full-rank if $\forall p_i \in \mathbb{F}_q, i = 1, \dots, (l+1)^4$

except the trivial choice of all zeros we have,

$$\sum_{k=1}^{(l+1)^4} p_k (T_{2,3}^{[1]})^{\alpha_{1k}} (T_{1,3}^{[2]})^{\alpha_{2k}} (T_{1,2}^{[3]})^{\alpha_{3k}} (T_{2,3}^{[4]})^{\alpha_{4k}} \mathbf{1}_\tau \neq \mathbf{0}_\tau$$

$$\alpha_{jk} = \{0, 1, \dots, l\}, j = 1, \dots, 4. \quad (4.10)$$

where $\mathbf{0}_\tau$ is the all-1 vector of dimension τ . Recall that M_{ij} 's are diagonal matrices. Let $M_{ij} = [m_{ij}(a^t)]_{(t,t)}$, $t = \{1, \dots, \tau\}$ so that $m_{ij}(a^t)$ is the t^{th} diagonal element of M_{ij} . Then (4.10) reduces to,

$$q(a^t) = \sum_{k=1}^{(l+1)^4} p_k \left(\frac{m_{1,3}(a^t)}{m_{1,2}(a^t)} \right)^{\alpha_{1k}} \left(\frac{m_{2,3}(a^t)}{m_{2,1}(a^t)} \right)^{\alpha_{2k}}$$

$$\cdot \left(\frac{m_{3,2}(a^t)}{m_{3,1}(a^t)} \right)^{\alpha_{3k}} \left(\frac{m_{4,3}(a^t)}{m_{4,2}(a^t)} \right)^{\alpha_{4k}} \neq 0$$

$$\alpha_{jk} = \{0, 1, \dots, l\}, j = 1, \dots, 4, t = \{1, \dots, \tau\}. \quad (4.11)$$

Let $\bar{a} \triangleq [a^1, \dots, a^\tau]$ and also let $q^N(a^t)$ and $q^D(a^t)$ be the numerator and denominator polynomials of $q(a^t)$ such that $q(a^t) \triangleq q^N(a^t)/q^D(a^t)$. Now define the polynomial $q(\bar{a}) \triangleq \prod_{t=1}^\tau q_D(a^t) q_N(a^t)$. Then in order for V_1 to be full-rank $q(\bar{a})$ needs to be a non-zero polynomial. We make the following assumption on the network transfer functions $m_{ij}(a)$'s:

$$(A1) \quad q(\bar{a}) \neq 0. \quad (4.12)$$

Then, the existence of an assignment \bar{a} in $\mathbb{F}_q^{\tau s}$ such that $q(\bar{a})$ is nonzero is guaranteed by the Lemma 7 for a sufficiently large field size q . Next consider the following product polynomial similar to [47]:

$$p(\bar{a}) = \prod_{\substack{i \in \{1, 2, 3\} \\ j \in \{1, 2, 3, 4\}}} \prod_{t=1}^\tau m_{ij}(a^t).$$

Then one can see that the diagonal matrices M_{ij} 's have well-defined inverses as long as $p(\bar{a})$ is non-zero. Now consider the rank conditions given above at each destination node. We need to show that the following holds:

$$\text{rank}[M_{11}V_1 \quad M_{12}V_2] = (l+1)^4 + l(l+1)^3.$$

Since M_{ij} is invertible as explained above, it is enough to show that:

$$\text{rank}[V_1 \quad M_{11}^{-1}M_{12}V_2] = (l+1)^4 + l(l+1)^3.$$

Now consider the following polynomials.

$$r_1(a^t) = \sum_{k=1}^{(l+1)^4} p_k \left(\frac{m_{1,3}}{m_{1,2}}(a^t) \right)^{\alpha_{1k}} \left(\frac{m_{2,3}}{m_{2,1}}(a^t) \right)^{\alpha_{2k}} \left(\frac{m_{3,2}}{m_{3,1}}(a^t) \right)^{\alpha_{3k}} \left(\frac{m_{4,3}}{m_{4,2}}(a^t) \right)^{\alpha_{4k}} \quad (4.13)$$

$$+ \frac{m_{11}}{m_{12}}(a^t) \sum_{k=(l+1)^4+1}^{(l+1)^4+l(l+1)^3} p_k \left(\frac{m_{1,3}}{m_{1,2}}(a^t) \right)^{\alpha_{5k}} \left(\frac{m_{2,3}}{m_{2,1}}(a^t) \right)^{\alpha_{6k}} \left(\frac{m_{3,2}}{m_{3,1}}(a^t) \right)^{\alpha_{7k}} \left(\frac{m_{4,3}}{m_{4,2}}(a^t) \right)^{\alpha_{8k}},$$

$$\alpha_{jk} = \left\{ \begin{array}{l} \{0, 1, \dots, l-1\}, \quad j = 7, \\ \{0, 1, \dots, l\}, \quad j = \{1, \dots, 6, 8\} \end{array} \right\}, \quad t = \{1, \dots, \tau\}.$$

$$r_2(a^t) = \sum_{k=1}^{(l+1)^4} p_k \left(\frac{m_{1,3}}{m_{1,2}}(a^t) \right)^{\alpha_{1k}} \left(\frac{m_{2,3}}{m_{2,1}}(a^t) \right)^{\alpha_{2k}} \left(\frac{m_{3,2}}{m_{3,1}}(a^t) \right)^{\alpha_{3k}} \left(\frac{m_{4,3}}{m_{4,2}}(a^t) \right)^{\alpha_{4k}} \quad (4.14)$$

$$+ \frac{m_{22}}{m_{21}}(a^t) \sum_{k=(l+1)^4+1}^{(l+1)^4+l(l+1)^3} p_k \left(\frac{m_{1,3}}{m_{1,2}}(a^t) \right)^{\alpha_{5k}} \left(\frac{m_{2,3}}{m_{2,1}}(a^t) \right)^{\alpha_{6k}} \left(\frac{m_{3,2}}{m_{3,1}}(a^t) \right)^{\alpha_{7k}} \left(\frac{m_{4,3}}{m_{4,2}}(a^t) \right)^{\alpha_{8k}},$$

$$\alpha_{jk} = \left\{ \begin{array}{l} \{0, 1, \dots, l-1\}, \quad j = 7, \\ \{0, 1, \dots, l\}, \quad j = \{1, \dots, 6, 8\} \end{array} \right\}, \quad t = \{1, \dots, \tau\}.$$

$$r_3(a^t) = \sum_{k=1}^{(l+1)^4} p_k \left(\frac{m_{1,3}}{m_{1,2}}(a^t) \right)^{\alpha_{1k}} \left(\frac{m_{2,3}}{m_{2,1}}(a^t) \right)^{\alpha_{2k}} \left(\frac{m_{3,2}}{m_{3,1}}(a^t) \right)^{\alpha_{3k}} \left(\frac{m_{4,3}}{m_{4,2}}(a^t) \right)^{\alpha_{4k}} \quad (4.15)$$

$$+ \frac{m_{32}}{m_{31}}(a^t) \sum_{k=(l+1)^4+1}^{(l+1)^4+l^4} p_k \left(\frac{m_{1,3}}{m_{1,2}}(a^t) \right)^{\alpha_{5k}} \left(\frac{m_{2,3}}{m_{2,1}}(a^t) \right)^{\alpha_{6k}} \left(\frac{m_{3,2}}{m_{3,1}}(a^t) \right)^{\alpha_{7k}} \left(\frac{m_{4,3}}{m_{4,2}}(a^t) \right)^{\alpha_{8k}},$$

$$\alpha_{jk} = \left[\begin{array}{l} \{0, 1, \dots, l-1\}, \quad j = \{5, \dots, 8\}, \\ \{0, 1, \dots, l\}, \quad j = \{1, \dots, 4\} \end{array} \right], \quad t = \{1, \dots, \tau\}.$$

$$r_4(a^t) = \sum_{k=1}^{(l+1)^4} p_k \left(\frac{m_{1,3}}{m_{1,2}}(a^t) \right)^{\alpha_{1k}} \left(\frac{m_{2,3}}{m_{2,1}}(a^t) \right)^{\alpha_{2k}} \left(\frac{m_{3,2}}{m_{3,1}}(a^t) \right)^{\alpha_{3k}} \left(\frac{m_{4,3}}{m_{4,2}}(a^t) \right)^{\alpha_{4k}} \quad (4.16)$$

$$+ \frac{m_{41}}{m_{42}}(a^t) \sum_{k=(l+1)^4+1}^{(l+1)^4+l(l+1)^3} p_k \left(\frac{m_{1,3}}{m_{1,2}}(a^t) \right)^{\alpha_{5k}} \left(\frac{m_{2,3}}{m_{2,1}}(a^t) \right)^{\alpha_{6k}} \left(\frac{m_{3,2}}{m_{3,1}}(a^t) \right)^{\alpha_{7k}} \left(\frac{m_{4,3}}{m_{4,2}}(a^t) \right)^{\alpha_{8k}},$$

$$\alpha_{jk} = \left\{ \begin{array}{l} \{0, 1, \dots, l-1\}, \quad j = 7, \\ \{0, 1, \dots, l\}, \quad j = \{1, \dots, 6, 8\} \end{array} \right\}, \quad t = \{1, \dots, \tau\}.$$

Define $r_j(\bar{a}) \triangleq \prod_{t=1}^{\tau} r_j^D(a^t) r_j^N(a^t)$ where we have the denominator and the numerators polynomials defined as $r_j(a^t) \triangleq r_j^N(a^t)/r_j^D(a^t)$ and $r_j(a^t)$ is given as above. We make the following assumption on the network transfer functions $m_{ij}(a)$'s:

$$(A2) \quad r_j(\bar{a}) \neq 0, \quad \forall j = \{1, \dots, 4\}. \quad (4.17)$$

Now consider a polynomial $f(\bar{a})$ which is the multiplication of the polynomials defined earlier such that,

$$f(\bar{a}) = p(\bar{a})q(\bar{a})r_1(\bar{a})r_2(\bar{a})r_3(\bar{a})r_4(\bar{a}).$$

We know that by assumptions (A1) – (A2) and with the assumption that $m_{ij}(a)$'s are non-trivial polynomials, $f(\bar{a})$ also becomes a non-trivial polynomial. Therefore, using Lemma 7 we can conclude that for large enough field size q , there exist $\bar{a}_0 \in \mathbb{F}_q^{\tau s}$ such that $f(\bar{a}_0) \neq 0$. Since by using such an \bar{a}_0 all the rank and span conditions are satisfied, it is possible to achieve a throughput of $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$:

$$\begin{aligned} \lim_{l \rightarrow \infty} \frac{|V_1|}{\tau} &= \lim_{l \rightarrow \infty} \frac{(l+1)^4}{2(l+1)^4} = \frac{1}{2}, \\ \lim_{l \rightarrow \infty} \frac{|V_2|}{\tau} &= \lim_{l \rightarrow \infty} \frac{l(l+1)^3}{2(l+1)^4} = \frac{1}{2}, \\ \lim_{l \rightarrow \infty} \frac{|V_3|}{\tau} &= \lim_{l \rightarrow \infty} \frac{l^4}{2(l+1)^4} = \frac{1}{2}. \end{aligned}$$

Now we can state the result formally.

Theorem 4. *In a three-source four-destination multiple unicast network representable by a directed, acyclic graph G , if the min-cut for each source-destination pair is 1 and if the network transfer functions $m_{ij}(a)$, $i \in \{1, 2, 3\}$, $j \in \{1, 2, 3, 4\}$ consists of non-trivial polynomials satisfying the assumption (A1) $q(\bar{a}) \triangleq \prod_{t=1}^{\tau} q_D(a^t) q_N(a^t) \neq 0$ where $q(a^t) \triangleq q_N(a^t)/q_D(a^t)$ and*

$$q(a^t) = \sum_{k=1}^{(l+1)^4} p_k \left(\frac{m_{1,3}(a^t)}{m_{1,2}(a^t)} \right)^{\alpha_{1k}} \left(\frac{m_{2,3}(a^t)}{m_{2,1}(a^t)} \right)^{\alpha_{2k}} \left(\frac{m_{3,2}(a^t)}{m_{3,1}(a^t)} \right)^{\alpha_{3k}} \left(\frac{m_{4,3}(a^t)}{m_{4,2}(a^t)} \right)^{\alpha_{4k}} \neq 0$$

$$\alpha_{jk} = \{0, 1, \dots, l\}, \quad j = 1, \dots, 4, \quad t = \{1, \dots, \tau\}.$$

and also satisfying the assumption (A2) $r_j(\bar{a}) \triangleq \prod_{t=1}^T r_j^D(a^t) r_j^N(a^t) \neq 0$, $\forall j = \{1, \dots, 4\}$, where $r_j(a^t) \triangleq r_j^N(a^t)/r_j^D(a^t)$ and $r_j(a^t)$ is given as in (4.13)-(4.16), then each source can achieve a rate arbitrarily close to $1/2$.

4.4 General Case: K Source J Destination Nodes

In this section, we generalize the results to the networks consisting of K source nodes and J destination nodes with general message demands. Let \mathcal{M}_j denote the set of sources whose messages are demanded at the destination node j . Also let $C_{S_i, j}$ denote the min-cut value between the source nodes in the set $S_i \subseteq \{s_1, \dots, s_K\}$ and the destination node d_j . Max-flow min-cut theorem gives us an upper bound on the achievable total rate between the sources in S_i and the destination node d_j :

$$\sum_{i \in S_i} r_i \leq C_{S_i, j}, \quad \forall 1 \leq j \leq J. \quad (4.18)$$

where r_i is the rate at the source node s_i . From now on, we assume that $\max_j C_{S_i, j} \triangleq \bar{C} \leq 1$.

We introduce some notation from [46]. Define $T_{m,n}^{[j]} \triangleq M_{j_m}^{-1} M_{j_n}$ as the matrix corresponding to the alignment constraint

$$\text{span}(M_{j_n} V_n) \subseteq \text{span}(M_{j_m} V_m)$$

that enforces the interference from message n to be aligned to the interference of message m at receiver j . Without loss of generality, we assume the following order on the source rates:

$$r_K \leq r_{K-1} \leq \dots \leq r_2 \leq r_1 \quad (4.19)$$

Based on (4.19), for any $T_{m,n}^{[j]}$ matrix, we always have $n > m$. Also let $\delta_j = \min\{k | k \in \mathcal{M}_j^c\}$ and define the following set

$$\mathcal{C} := \left\{ (m, n, j) \left| \begin{array}{l} j \in \{1, \dots, J\}, \\ m, n \in \mathcal{M}_j^c, \\ m = \delta_j, n > m \end{array} \right. \right\}.$$

which basically defines \mathcal{C} as a set of vectors denoting all the alignment constraints. Notice that $\Gamma \triangleq |\mathcal{C}|$ is the total number of matrices $T_{m,n}^{[j]}$ matrices. Let Γ_k be the cardinality of the following set

$$\mathcal{C}_k = \{(m, n, j) | (m, n, j) \in \mathcal{C}, n \leq k\}, k = 1, \dots, K \quad (4.20)$$

which defines the number of (m, n, j) indices for which the matrix $T_{m,n}^{[j]}$ has its exponents from the set $\{0, \dots, l-1\}$, while for the other $\Gamma - \Gamma_k$ indices the matrix $T_{m,n}^{[j]}$ can be raised to the power of l . Consider a time expansion of $\tau = \kappa(l+1)^\Gamma$ for this network.

Now, define the achievable rate region $\mathcal{D}(r)$ as in (4.21).

$$\mathcal{D}(r) = \left\{ r \in \mathbb{R}^K, \left| \sum_{i \in \mathcal{M}_j} r_i + \max_{k \in \mathcal{M}_j^c} r_k \leq C_{\mathcal{M}_j, j}, \forall j \in \{1, \dots, J\} \right. \right\} \quad (4.21)$$

Any irrational number can be approximated by a rational number arbitrarily closely. Then notice that if \tilde{V}_i 's are chosen as given below,

$$\tilde{V}_k = \left\{ \prod_{(m,n,j) \in \mathcal{C}} \left(T_{m,n}^{[j]} \right)^{\alpha_{m,n,j}} w_i \left| 1 \leq i \leq \bar{r}_k, \alpha_{m,n,j} \in \begin{cases} \{0, 1, \dots, l\}, & \text{if } n > k \\ \{0, 1, \dots, l-1\}, & \text{otherwise} \end{cases} \right. \right\}, \quad 1 \leq k \leq K. \quad (4.22)$$

the alignment conditions are satisfied [46]. For Z_i to be recoverable from X_i , we need \tilde{V}_i to be full-rank. Because of (4.19), it is enough to show that \tilde{V}_1 is full-rank. Consider the following rational function,

$$Q(a^t) = \sum_{k=1}^{\bar{r}_k l^{\Gamma_k} (l+1)^{\Gamma - \Gamma_k}} p_k \prod_{(m,n,j) \in \mathcal{C}} \left(\frac{m_{jn}(a^t)}{m_{jm}(a^t)} \right)^{\alpha_{m,n,j}} [w_i]_t. \quad (4.23)$$

Define $Q(\bar{a}) = \prod_{t=1}^{\tau} Q^D(a^t) Q^N(a^t)$ where $Q(a^t) \triangleq Q^N(a^t) / Q^D(a^t)$. Then we have \tilde{V}_1 full-rank if $Q(\bar{a}) \neq 0$.

$$(A3) \quad Q(\bar{a}) \neq 0. \quad (4.24)$$

Similar to the proof of Theorem 4, we need M_{ij} 's to have well-defined inverses for which we

define the following polynomial.

$$P(\bar{a}) = \prod_{i \in \{1, \dots, K\}} \prod_{t=1}^{\tau} m_{ij}(a^t).$$

$$j \in \{1, \dots, J\}$$

What remains is to show that the rank conditions are satisfied which will guarantee that the intended message space and the interference spaces are independent. For example, we need to have the following matrix

$$\Lambda_j = \left[M_{jm_{1,j}} \tilde{V}_{m_{1,j}} | M_{jm_{2,j}} \tilde{V}_{m_{2,j}} | \dots | M_{jm_{\beta_j,j}} \tilde{V}_{m_{\beta_j,j}} | M_{j\delta_j} \tilde{V}_{\delta_j} \right] \quad (4.25)$$

to be full rank at destination node d_j .

Notice that for any point within $\mathcal{D}(r)$

$$\sum_{m \in \mathcal{M}_j} \bar{r}_m + \bar{r}_{\delta_j} \leq \kappa \quad (4.26)$$

always holds (recall $\bar{C} \leq 1$) which makes the matrix Λ_j either tall or square. For any row r of its upper square sub-matrix, its elements can be expressed in the following general form:

$$M_{jk}(r) \prod_{(m,n,j) \in \mathcal{C}} \left(M_{jm}^{-1}(r) M_{jn}(r) \right)^{\alpha_{m,n,j}} [w_i]_r.$$

Therefore, for (4.25) to be full-rank, we need m_{ij} 's such that $R_j^r(a) \neq 0$ for any row r of its upper square sub-matrix, where $R_j^r(\bar{a})$ is,

$$R_j(a^r) = \sum_{t_k=1}^{\sum_{k \in \mathcal{M}_j \cup \{\delta_j\}} \bar{r}_k l^{\Gamma_k} (l+1)^{\Gamma - \Gamma_k}} p_{t_k} m_{jk}(a^r) \prod_{(m,n,j) \in \mathcal{C}} \left(\frac{m_{jn}(a^r)}{m_{jm}(a^r)} \right)^{\alpha_{m,n,j}} [w_i]_r. \quad (4.27)$$

For any rational rate vector $r = (r_1, \dots, r_K)$ within $\mathcal{D}(r)$ that satisfies (4.19), we can choose a $\kappa \in \mathbb{Z}^+$, such that

$$\kappa r = (\bar{r}_1, \bar{r}_2, \dots, \bar{r}_K) \in \mathbb{Z}_+^K.$$

We define $R(\bar{a}) \triangleq \prod_{r,j} R_j^D(a^r) R_j^N(a^r)$ where $R_j^D(a^r)$ and $R_j^N(a^r)$ is defined as $R_j(a^r) \triangleq R_j^N(a^r) / R_j^D(a^r)$. We make the following assumption on the network transfer functions $m_{ij}(a)$'s:

$$(A4) \quad R(\bar{a}) \neq 0. \quad (4.28)$$

Define the grand polynomial $F(\bar{a})$,

$$F(\bar{a}) = P(\bar{a})Q(\bar{a})R(\bar{a}).$$

Now we know that by assumptions (A3)–(A4) and with the assumption that $m_{ij}(a)$'s are non-trivial polynomials, $F(\bar{a})$ also becomes a non-trivial polynomial. Therefore, using Lemma 7 we can conclude that for large enough field size q , there exist $\bar{a}_0 \in \mathbb{F}_q^{\tau s}$ such that $F(\bar{a}_0) \neq 0$. Since by using such an \bar{a}_0 all the rank and span conditions are satisfied, it is possible to achieve a throughput of

$$\lim_{l \rightarrow \infty} \frac{|V_k|}{\tau} = \lim_{l \rightarrow \infty} \frac{\bar{r}_k l^{\Gamma_k} (l+1)^{\Gamma - \Gamma_k}}{\kappa (l+1)^\Gamma} = \frac{\bar{r}_k}{\kappa} = r_k.$$

We summarize the result in the following theorem.

Theorem 5. *In a K -source J -destination multiple unicast network representable by a directed, acyclic graph G , if the min-cut for each source-destination pair is 1 and if the network transfer functions $m_{ij}(a)$, $i \in \{1, \dots, K\}$, $j \in \{1, \dots, J\}$ consists of non-trivial polynomials such that ($\forall p_k, p_{t_k} \in \mathbb{F}_q$ except the trivial choices of all zeros) polynomials $Q(\bar{a})$ and $R(\bar{a})$ defined below is nonzero:*

$$Q(\bar{a}) = \prod_{t=1}^{\tau} \prod_{(m,n,j) \in \mathcal{C}} m_{jm}(a^t)^{\alpha_{m,n,j}} \left\{ \sum_{k=1}^{\bar{r}_k l^{\Gamma_k} (l+1)^{\Gamma - \Gamma_k}} p_k \prod_{(m,n,j) \in \mathcal{C}} (m_{jn}(a^t))^{\alpha_{m,n,j}} [w_i]_t \right\} \neq 0$$

$$R(\bar{a}) = \prod_{r = \{1, \dots, \tau\}} \prod_{(m,n,j) \in \mathcal{C}} (m_{jm}(a^r))^{\alpha_{m,n,j}} .$$

$$j = \{1, \dots, J\}$$

$$\left\{ \sum_{t_k=1}^{\sum_{k \in \mathcal{M}_j \cup \{\delta_j\}} \bar{r}_k l^{\Gamma_k} (l+1)^{\Gamma - \Gamma_k}} p_{t_k} m_{jk}(a^r) \prod_{(m,n,j) \in \mathcal{C}} (m_{jn}(a^r))^{\alpha_{m,n,j}} [w_i]_r \right\} \neq 0.$$

Then it is possible to achieve the rates that are in $\mathcal{D}(r)$ arbitrarily closely:

$$\mathcal{D}(r) = \left\{ r \in \mathbb{R}^K, \left| \sum_{i \in \mathcal{M}_j} r_i + \max_{k \in \mathcal{M}_j^c} r_k \leq C_{\mathcal{M}_j, j}, \quad \forall j \in \{1, \dots, J\} \right. \right\}.$$

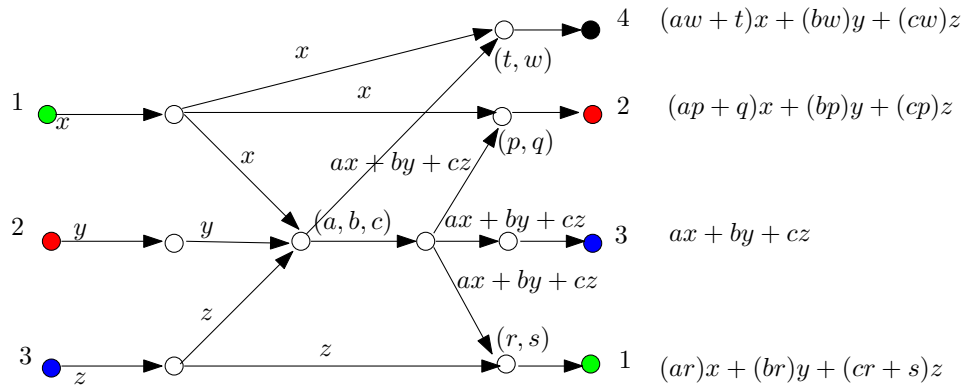


Figure 4.1 An example network for which the proposed interference alignment can not be applied since the assumption (A2) is violated.

4.5 Discussion

In this section, we would like to give an example network to demonstrate how the assumptions can be used to verify if the network would support the proposed interference alignment scheme or not. The example is adapted from one of example networks given in [48] and modified for three source four destination case. In the function $r_1(a^t)$, take $\alpha_{3k} = 1, p_3 = 1, p_5 = 1$ and take all the other $\alpha_{ij} = 0, p_i = 0$. Then we need to have:

$$m_{11} \neq \frac{m_{12}m_{31}}{m_{32}}$$

But, when we plug-in the values we obtain:

$$ar = \frac{(br)(a)}{b}.$$

And one can see that no matter what element we pick from the finite field, we will have an equality, hence the inequality in the assumption can not be satisfied.

Here we would like to point out that the assumption on the network transfer functions $m_{ij}(a)$'s to be non-trivial polynomials can be relaxed using a similar approach as in [47]. Instead of the trivial $m_{ij}(a)$ polynomials, it was proposed to use new variables which would act as "virtual" interference. Here same idea can be applied by changing the assumptions (A1) – (A4) accordingly.

It can be observed that the number of assumptions increases rapidly as the network grows larger. However, we would like to point out that the assumptions made here are verifiable

given enough time and computation power. Trying to reduce the number of assumptions made and trying to relate these assumptions with graph theoretical properties such as the min-cut value is an important direction for future work.

4.6 Conclusions

In this chapter, we first considered a simple network consisting of three source nodes and four destination nodes and showed that each user can achieve a rate of one half. Then we extended the result for a more general network consisting of K source nodes and J destination nodes. We show that when the min-cut between a source-destination pair is one, it is possible to achieve a sum rate that is arbitrarily close to the min-cut between the source nodes whose messages are demanded and the destination node where the sum rate is the summation of all the demanded source message rates plus the biggest interferer's rate. As a future work, it would be interesting to search for examples of networks for which interference alignment works as a better technique compared to routing and network coding. Another possible research direction would be to study the effect of delay similar to the approach in [6].

CHAPTER 5. CONCLUSION AND FUTURE WORK

In this thesis, we studied application of network coding to the multi-source networks for both wired and wireless settings. We had different design goals because of the differences in the nature of these two settings. For example in the wireless setup, one of the major problems is the multipath fading. And the best way to deal with fading is to introduce diversity. Therefore in the wireless setup our goal was to introduce diversity by applying a combination of techniques from cooperative communication and network coding.

To be more specific, for the wireless setup we proposed a network coded cooperation scheme for N source-destination pairs assisted with M relays under two different traffic network models: multicast and unicast. The proposed schemes allow the relays to apply network coding on the data it has received from its neighbors. We allow the relays to linearly combine the packets with coefficients either deterministically pre-designed or drawn from a finite field randomly. We established the diversity-multiplexing tradeoff performance of the proposed schemes for any network coding matrix, and showed its advantage over the existing schemes when the coding matrix is optimized. Specifically, it is capable of achieving the maximum diversity order $M + 1$ at the expense of a slightly reduced multiplexing rate. We derived the necessary and sufficient conditions to achieve the maximum diversity order. We showed that when the parity-check matrix for a $(N + M, M, N + 1)$ systematic MDS code is used as the network coding matrix, the maximum diversity is achieved. We presented two ways to generate the network coding matrix: using either the Cauchy matrices or the Vandermonde matrices. Both constructions guarantee maximum diversity order. When a relay selection is possible, we show that a multiplicative effect on the diversity order is possible when enough rounds of relay selection is performed.

In the wired setup, we had different design goals. We considered wired networks consisting

of multiple source and destination nodes and multiple relays. The best known bound for this setup is the cut-set bound. Hence our design goal was to get as close as possible to the cut-set bound. As pointed out before, network coding offers high throughput for single-source multicasting. However, if one would like to apply network coding to multiple-source networks to achieve higher throughput, network coding introduces interference to the system rendering the decodability of the source messages at the destination nodes. Therefore in the wired setup, our goal was to try to benefit from network coding's capability of providing high throughput, but also at the same time combat with the interference that comes along with the linear combination of the signals. Towards achieving this goal, we borrowed interference alignment techniques which was originally proposed for wireless networks. We first considered a simple network consisting of three source nodes and four destination nodes and showed that each user can achieve a rate of one half under certain assumptions on the network transfer functions. Then we extended the result for a more general network consisting of K source nodes and J destination nodes. The interference alignment tools enabled us to align all the interference at a particular receiver to its biggest interferer's space. As a result we were able to show that when the min-cut between each source-destination pair is one, it is possible to achieve a sum rate that is arbitrarily close to the min-cut between the source nodes whose messages are demanded and the destination node where the sum rate is the summation of all the demanded source message rates plus the biggest interferer's rate.

For both wired and wireless networks, our approach can be extended in several directions. For wireless networks, instead single-hop as we considered in this thesis, the model can be extended to allow multi-hop between the relays. Another interesting direction would be to apply network coding in the physical layer unlike our approach in this thesis which was to apply it at the network layer. Application of network coding at the physical layer brings its own challenges like CFO and the synchronization problem.

For wired networks, multiple future research directions exist as well. One of the possibilities for the future work could be to discover examples of networks for which interference alignment works as a better technique compared to routing and other existing methods like butterfly

packing, etc. Another direction might be to try to minimize the number of assumptions that have been made. Trying to relate these assumptions to graph theoretical properties such as the min-cut value is another important future research direction. In our study for the wired networks, one of the important assumptions that we made was to assume that the min-cut for all source-destination pairs to be one. The general case for arbitrary min-cut values is certainly an important open problem. It might also be interesting to study the proposed approach for networks with delays similar to the approach in [6].

APPENDIX A. Proof of Lemma 3

Here we define the following relevant events. $\bar{E}_i \triangleq \{e_i \notin \text{span}(A_i)\}$, $\bar{E}_i^{up} \triangleq \{A_i \text{ has at most } \Lambda_i(A) - 1 \text{ rows}\}$. Notice that, $\bar{E}_i \subset \bar{E}_i^{up}$ by the first condition in the definition of Λ_i -rank. By the second condition in the definition of Λ_i -rank, there exist a collection of $\Lambda_i(A) - 1$ rows of A_i that does not span e_i . Let \bar{A}_i denote a $(\Lambda_i(A) - 1) \times N$ submatrix of A_i that consists of such rows. Keeping the definition of F_m define $\bar{E}_i^{low} \triangleq \{F_0 \cap \{A_i = \bar{A}_i\}\}$. It follows that $\bar{E}_i^{low} \subset \bar{E}_i$. Since $\bar{E}_i^{low} \subset \bar{E}_i \subset \bar{E}_i^{up}$, using (3.6) and (3.7) we have:

$$\begin{aligned} P(\bar{E}_i) &\leq P(\bar{E}_i^{up}) \\ &= P_0 \sum_{m=0}^M P(F_m) \cdot \sum_{l=0}^{\Lambda_i(A)-1} P(E(N-1+M-m, l)), \end{aligned} \quad (\text{A.1})$$

and

$$P(\bar{E}_i) \geq P(\bar{E}_i^{low}) = P(F_0) P_0^{N+M-(\Lambda_i(A)-1)} (1 - P_0)^{\Lambda_i(A)-1}$$

where the first P_0 in (A.1) accounts for the outage of the direct link between s_i and d_i . The limits in the second summation in (A.1) is due to the fact that the destination d_i may not be able to recover all Θ_i 's, if only $\Lambda_i(A) - 1$ or less number of transmissions are successful. The rest of the proof can be completed by showing that the diversity orders of both the upper and the lower bound are equal to (3.14) as in the proof of the multicast scenario. \square

APPENDIX B. Proof of Theorem 3

Let $r = \arg \max h_i$ where h_i is as in (3.19). The cdf for $|h_{jr}|^2$ (or $|h_{rj}|^2$) where j can be a source (or a destination) node was derived in [40] as:

$$F(\tau) = \int_0^\tau \sum_{m=1}^M \left\{ \beta_{kr_m} e^{-\beta_m \phi} \prod_{j \neq m}^M (1 - e^{-\beta_j}) \right\} d\phi + \int_0^\tau \sum_{m=1}^M \int_0^\phi (\beta_m - \beta_{mk}) e^{-(\beta_m - \beta_{mk})\theta} \prod_{j \neq m}^M (1 - e^{-\beta_j \theta}) d\theta \beta_{mk} e^{-\beta_{mk} \phi} d\phi \quad (\text{B.1})$$

where $\beta_{m,k}$'s are the parameters of the exponential random variables associated with the corresponding channels between node m and node k , and $\beta_m = \sum_{k=1}^N [\beta_{m,k} + \beta_{k,m}]$, $m = \{1, \dots, M\}$. Taking $\beta_{m,k} = \beta$ and using exponential expansion, a high-SNR approximation for (B.1) can be shown to be equal to: $F(\tau) \cong (2N\beta)^{M-1} \beta \tau^M$. Now, the probability that any relay can successfully decode all N packets in the first stage is $P(S) = \prod_{k=1}^N P(|h_{kr}|^2 > \tau) = \prod_{k=1}^N (1 - F(\tau)) = (1 - F(\tau))^N$. Similar to the definition of F_m , let F_k denote the event that k out of K relays fail to receive all the packets: $P(F_k) = \binom{K}{k} P(S)^{K-k} (1 - P(S))^k$. Using similar techniques as in the proof of Theorem 1, it can be shown that $Pr(E_k) \cong K_1 \tau^{Mk}$ where $K_1 = \binom{K}{k} (2N)^{(M-1)k} \beta^{Mk} N^k$.

Also let $E_{s,t}(k)$ denote the event that s channels out of N source channels and t channels out of $K - k$ relay channels were operational. Then we have

$$P(E_{s,t}(k)) = \binom{N}{s} P_0^{N-s} (1 - P_0)^s \binom{K-k}{t} \cdot F(\tau)^{K-k-t} (1 - F(\tau))^t.$$

Notice that, since $\Gamma_N(A) = N$ we have $E_i = E_i^{up}$. Therefore, we have

$$P(E_i) = \sum_{k=0}^K P(E_k) \cdot \sum_{\{s,t|s+t=0\}}^{N-1} P(E_{s,t}(k)). \quad (\text{B.2})$$

It can be shown that $P(E_{s,t}(k)) \cong K_2 \tau^{(N-s)^+ + (K-k-t)^+ M}$, where $(x)^+ = \max(x, 0)$ and $K_2 = \binom{N}{s} \binom{K-k}{t} \beta^{N-s+(K-k-t)M} (2N)^{(M-1)(K-k-t)}$ and hence $P(E_i) \cong K_1 K_2 \tau^{Mk+(N-s)^+ + (K-k-t)^+ M}$.

We need to find out

$$\min_{\{s,t|s+t=\{0,\dots,N-1\}\}} ((N-s)^+ + (K-t)^+ M). \quad (\text{B.3})$$

We need to consider two different cases: $K < N-1$ and $K \geq N-1$. For the first case, choosing $t = K$ and $s = N-1-t = N-1-K$ achieves the minimum: $(N-s)^+ + (K-t)^+ M = (N - (N-1-K)) + (K-K)M = K+1$. And for the second case choosing $t = N-1$ and $s = 0$ achieves the minimum: $(N-s)^+ + (K-t)^+ M = N + (K - (N-1))M$. Now, rest of the proof can be completed using similar techniques as in the proof of Theorem 1. \square

BIBLIOGRAPHY

- [1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, “Network information flow,” *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1204–1216, Apr. 2000.
- [2] L. Zheng and D. N. C. Tse, “Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels,” *IEEE Trans. Inform. Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.
- [3] V. Cadambe and S. Jafar, “Interference alignment and degrees of freedom of the K-user interference channel,” *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.
- [4] R. K. Ahuja, T. L. Maganti, and J. B. Orlin, *Network Flows: Theory, Algorithms and Applications*. Prentice-Hall, 1993.
- [5] S.-Y. R. Li, R. W. Yeung, and N. Cai, “Linear network coding,” *IEEE Trans. Inform. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.
- [6] R. Koetter and M. Médard, “An algebraic approach to network coding,” *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782–795, Oct. 2003.
- [7] T. Ho, R. Koetter, M. Médard, D. R. Karger, and M. Effros, “The benefits of coding over routing in a randomized setting,” *Information Theory, 2003. Proceedings. IEEE International Symposium on*, Jun. 2003.
- [8] M. Feder, D. Ron, and A. Tavor, “Bounds on linear codes for network multicast,” *Electronic Colloquium on Computational Complexity*, 2003.

- [9] R. Dougherty, C. Freiling, and K. Zeger, “Insufficiency of linear coding in network information flow,” *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*, Sept. 2005.
- [10] —, “Linearity and solvability in multicast networks,” *IEEE Trans. Inform. Theory*, vol. 50, oct. 2004.
- [11] Z. Li and B. Li, “Network coding: The case of multiple unicast sessions,” *In Proceedings of the 42nd Allerton Annual Conference on Communication, Control and Computing*, 2004.
- [12] M. Médard, M. Effros, T. Ho, and D. R. Karger., “On coding for non-multicast networks.” *In Proceedings of 41st Annual Allerton Conference on Communication, Control, and Computing*, 2003.
- [13] A. R. Lehman and E. Lehman, “Complexity classification of network information flow problems.” *In Proceedings of 41st Annual Allerton Conference on Communication, Control, and Computing*, 2003.
- [14] S. Riis, “Linear versus nonlinear boolean functions in network flow,” *Proceedings of 38th Annual Conference on Information Sciences and Systems*, 2003.
- [15] R. Dougherty, C. Freiling, and K. Zeger, “Linear network codes and systems of polynomial equations,” *IEEE Trans. Inform. Theory*, 2008.
- [16] D. S. Lun, M. Médard, and R. Koetter, “Efficient operation of wireless packet networks using network coding,” *Proc. International Workshop on Convergent Technologies (IWCT)*, 2005.
- [17] S. Katti, H. Rahul, D. Katabi, M. Médard, and J. Crowcroft, “XOR’s in the air: Practical wireless network coding,” *Proc. ACM SIGCOMM*, 2006.
- [18] N. Cai and R. W. Yeung, “Network coding and error correction,” *Proc. 2002 IEEE Information Theory Workshop*, 2002.

- [19] C. Gkantsidis and P. Rodriguez, “Network coding for large scale content distribution,” *Proc. IEEE INFOCOM*, 2005.
- [20] D. Leong, A. Dimakis, and T. Ho, “Distributed storage allocation for high reliability,” *Communications (ICC), 2010 IEEE International Conference on*, May 2010.
- [21] S. Zhang, S. Liew, and P. Lam, “Physical layer network coding,” *The Annual Intl. Conf. on Mobile Comp. and Networking*, Sept. 2006.
- [22] S. Katti, I. Maric, A. Goldsmith, D. Katabi, and M. Médard, “Joint relaying and network coding in wireless networks,” *Proc. IEEE ISIT*, Jun. 2007.
- [23] B. Nazer and M. Gastpar, “Computation over multiple-access channels,” *Information Theory, IEEE Transactions on*, Oct. 2007.
- [24] H. Topakkaya and Z. Wang, “Wireless network code design and performance analysis using diversity-multiplexing tradeoff,” *IEEE Transactions on Communications*, vol. 59, no. 2, pp. 488–496, Feb. 2011.
- [25] J. N. Laneman, D. N. C. Tse, and G. W. W. J. N. Laneman, “Cooperative diversity in wireless networks: Efficient protocols and outage behavior,” *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 2415–2425, Dec. 2004.
- [26] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, “A simple cooperative diversity method based on network path selection,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 659–672, Mar. 2006.
- [27] T. M. Cover and A. E. Gamal, “Capacity theorems for the relay channel,” *IEEE Trans. Inform. Theory*, Sep. 1979.
- [28] G. Kramer, M. Gastpar, and P. Gupta, “Cooperative strategies and capacity theorems for relay networks,” *IEEE Trans. Inform. Theory*, Sep. 2005.
- [29] A. Nosratinia, T. E. Hunter, and A. Hedayat, “Cooperative communication in wireless networks,” *IEEE Comm. Magazine*, Oct. 2004.

- [30] T. E. Hunter and A. Nosratinia, "Diversity through coded cooperation," *IEEE Trans. Wireless Commun.*, Feb. 2006.
- [31] T. E. Hunter, S. Sanayei, and A. Nosratinia, "Outage analysis of coded cooperation," *IEEE Trans. Inform. Theory*, Feb. 2006.
- [32] E. C. van der Meulen, "Three-terminal communication channels," *Advances in Applied Probability*, 1971.
- [33] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity-Part I: System description," *Communications, IEEE Transactions on*, vol. 51, no. 11, nov. 2003.
- [34] —, "User cooperation diversity-Part II: Implementation aspects and performance analysis," *Communications, IEEE Transactions on*, vol. 51, no. 11, nov. 2003.
- [35] J. N. Laneman and G. W. Wornell, "Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2415–2425, Oct. 2003.
- [36] G. Kramer, I. Maric, and R. Yates, "Cooperative communications," *Foundations and Trends in Networking*, vol. 1, no. 3, 2006.
- [37] Y. Yang, H. Hu, and J. Xu, "Relay technologies for WiMAX and LTE advanced mobile systems," *IEEE Commun. Magazine*, 2009.
- [38] E. Beres and R. Adve, "Selection cooperation in multi-source cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 118–127, Jan. 2008.
- [39] G. Alexandropoulos, A. Papadogiannis, and K. Berberidis, "Performance analysis of cooperative networks with relay selection over Nakagami-m fading channels," *IEEE Trans. Signal Processing*, vol. 17, no. 5, pp. 441–444, May 2010.
- [40] C. Peng, Q. Zhang, M. Zhao, Y. Yao, and W. Jia, "On the performance analysis of network-coded cooperation in wireless networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 8, pp. 3090–3097, Aug. 2008.

- [41] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs Technical Journal*, 1996.
- [42] M. Maddah-Ali, A. Motahari, and A. Khandani, "Signaling over MIMO multi-base systems: Combination of multi-access and broadcast schemes," *IEEE International Symposium on Information Theory*, pp. 2104–2108, July 2006.
- [43] B. Nazer, S. Jafar, M. Gastpar, and S. Vishwanath, "Ergodic interference alignment," *IEEE International Symposium on Information Theory*, July 2009.
- [44] S. Sridharan, A. Jafarian, S. Vishwanath, S. Jafar, and S. Shamai, "A layered lattice coding scheme for a class of three user gaussian interference channels," *46th Annual Allerton Conference on Communication, Control, and Computing*, Sept. 2008.
- [45] A. Motahari, A. Khandani, and S. Gharan, "On the degrees of freedom of the 3-user gaussian interference channel: The symmetric case," *IEEE International Symposium on Information Theory*, July 2009.
- [46] L. Ke, A. Ramamoorthy, Z. Wang, and H. Yin, "Degrees of freedom region for an interference network with general message demands," *IEEE International Symposium on Information Theory Proceedings (ISIT)*, Aug. 2011.
- [47] A. Das, S. Vishwanath, S. Jafar, and A. Markopoulou, "Network coding for multiple unicasts: An interference alignment approach," *IEEE International Symposium on Information Theory Proceedings (ISIT)*, pp. 1878–1882, Jun. 2010.
- [48] A. Ramakrishnan, A. Das, H. Maleki, A. Markopoulou, S. Jafar, and S. Vishwanath, "Network coding for three unicast sessions: Interference alignment approaches," *48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 1054–1061, 2010.
- [49] N. F. Mir, *Computer and Communication Networks*. Prentice Hall, 2006.

- [50] S. Hanly and D. Tse, “Multiaccess fading channels-Part II. delay-limited capacities,” *IEEE Trans. Inform. Theory*, vol. 44, no. 7, pp. 2816–2831, Nov. 1998.
- [51] R. Berry and R. Gallager, “Communication over fading channels with delay constraints,” *IEEE Trans. Inform. Theory*, vol. 48, no. 5, pp. 1135–1149, May 2002.
- [52] A. El. Gamal, J. Mammen, B. Prabhakar, and D. Shah, “Throughput-delay trade-off in wireless networks,” *Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 1, p. 475, Mar. 2004.
- [53] A. Bader and E. Ekici, “Throughput and delay optimization in interference-limited multihop networks,” *Proceedings ACM international symposium on Mobile ad hoc networking and computing*, 2006.
- [54] P. Gupta and P. R. Kumar, “The capacity of wireless networks,” *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 388–404, Feb. 2000.
- [55] A. Eryilmaz, A. Ozdaglar, and M. Médard, “On delay performance gains from network coding,” *Annual Conference on Information Sciences and Systems*, pp. 864–870, Mar. 2006.
- [56] Y. Sagduyu, G. Dongning, and R. Berry, “On the delay and throughput of digital and analog network coding for wireless broadcast,” *Annual Conference on Information Sciences and Systems*, pp. 534–539, Mar. 2008.
- [57] Y. Shi and M. Sheng, “Study of a scheduling algorithm based on simple network coding with high throughput and low delay,” *International Conference on Advanced Information Networking and Applications Workshops*, pp. 520–525, Mar. 2008.
- [58] H. Topakkaya and Z. Wang, “Effects of delay and links between relays on the min-cut capacity in a wireless relay network,” *46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 319–323, Sept. 2008.

- [59] S. Zhang and S.-C. Liew, "Channel coding and decoding in a relay system operated with physical-layer network coding," *IEEE Journal on Selected Areas in Communications*, pp. 788–796, Jun. 2009.
- [60] R. Louie, Y. Li, and B. Vucetic, "Practical physical layer network coding for two-way relay channels: performance analysis and comparison," *IEEE Trans. Wireless Commun.*, pp. 764–777, Feb. 2010.
- [61] M. Yu, J. Li, and R. S. Blum, "User cooperation through network coding," *Proc. of IEEE Intl. Conf. on Communications*, pp. 4064–4069, Jun. 2007.
- [62] Z. Han, X. Zhang, and H. Poor, "Cooperative transmission protocols with high spectral efficiency and high diversity order using multiuser detection and network coding," *Proc. of IEEE Intl. Conf. on Communications*, pp. 4232–4236, Jun. 2007.
- [63] T. Wang and G. Giannakis, "Complex field network coding for multiuser cooperative communications," *IEEE Journal on Selected Areas in Communications*, pp. 561–571, Apr. 2008.
- [64] M. Xiao and M. Skoglund, "Design of network codes for multiple-user multiple-relay wireless networks," *Proc. IEEE Intl. Symp. on Info. Theory*, pp. 2562–2566, July 2009.
- [65] D. Woldegebreal and H. Karl, "Multiple-access relay channel with network coding and non-ideal source-relay channels," *ISWCS*, pp. 732–736, Oct. 2007.
- [66] X. Bao and J. Li, "Adaptive network coded cooperation (ANCC) for wireless relay networks: matching code-on-graph with network-on-graph," *IEEE Trans. Wireless Commun.*, vol. 7, no. 2, pp. 574–583, Feb. 2008.
- [67] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*. Cambridge University Press, 1986.

- [68] G. Drolet, "A new representation of elements of finite fields $GF(2^m)$ yielding small complexity arithmetic circuits," *IEEE Transactions on Computers*, vol. 47, no. 9, pp. 938–946, Sept. 1998.
- [69] N. Sidiropoulos, G. Giannakis, and R. Bro, "Blind PARAFAC receivers for DS-CDMA systems," *IEEE Trans. Signal Processing*, vol. 48, no. 3, pp. 810–823, Mar. 2000.
- [70] Z. Wang and G. B. Giannakis, "Complex-field coding for OFDM over fading wireless channels," *IEEE Trans. Inform. Theory*, vol. 49, no. 3, pp. 707–720, Mar. 2003.
- [71] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.
- [72] R. C. Singleton, "Maximum distance Q-Nary codes," *IEEE Trans. Inform. Theory*, vol. 10, pp. 116–118, 1964.
- [73] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *SIAM Journal of Applied Math.*, vol. 8, pp. 300–304, 1960.
- [74] S. Wicker and V. Bhargava, *Reed-Solomon Codes and Their Applications*. Wiley-IEEE Press, 1999.
- [75] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, S. Jun, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inform. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.
- [76] T. S. Rappaport, *Wireless Communications: Principles and Practice*. NJ: Prentice Hall, 1996.
- [77] S. Jafar and S. Shamai, "Degrees of freedom region of the MIMO X channel," *IEEE Trans. Inform. Theory*, vol. 54, pp. 151–170, Jan. 2008.
- [78] V. Cadambe and S. Jafar, "Interference alignment and the degrees of freedom of wireless X networks," *IEEE Trans. Inform. Theory*, vol. 55, no. 9, pp. 3893–3908, Sept. 2009.

- [79] S. Huang and A. Ramamoorthy, "A note on the multiple unicast capacity of directed acyclic networks," *Proc. of IEEE Intl. Conf. on Communications*, Jun. 2011.