Title
Modern Low-Complexity Capacity-Achieving Codes For Network Communication

Author
Goela, Naveen

Publication Date
2013

Peer reviewed|Thesis/dissertation

Modern Low-Complexity Capacity-Achieving Codes for Network Communication

by

Naveen Goela

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Engineering-Electrical Engineering & Computer Sciences

and the Designated Emphasis

in

Communication, Computation, and Statistics

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Michael Gastpar, Chair
Professor Kannan Ramchandran
Professor Jim Pitman

Fall 2013

Modern Low-Complexity Capacity-Achieving Codes for Network Communication

Abstract

Modern Low-Complexity Capacity-Achieving Codes
for Network Communication

by

Naveen Goela

Doctor of Philosophy in Engineering-Electrical Engineering & Computer Sciences

and the Designated Emphasis

in

Communication, Computation, and Statistics

University of California, Berkeley

Professor Michael Gastpar, Chair

Communication over unreliable, interfering networks is one of the current challenges in engineering. For point-to-point channels, Shannon established capacity results in 1948, and it took more than forty years to find coded systems approaching the capacity limit with feasible complexity. Significant research efforts have gone into extending Shannon's capacity results to networks with many partial successes. By contrast, the development of low-complexity codes for networks has received limited attention to date. The focus of this thesis is the design of *capacity-achieving network codes* realizable by modern signal processing circuits.

For classes of networks, the following codes have been invented on the foundation of algebraic structure and probability theory: *i*) Broadcast codes which achieve multi-user rates on the capacity boundary of several types of broadcast channels. The codes utilize Arıkan's polarization theory of random variables, providing insight into information-theoretic concepts such as random binning, superposition coding, and Marton's construction. Reproducible experiments over block lengths $n = 512, 1024, 2048$ corroborate the theory; *ii*) A network code which achieves the computing capacities of a countably infinite class of simple noiseless interfering networks. The code separates a network into irreducible parallel sub-networks and applies a new vector-space function alignment scheme inspired by the concept of interference alignment for channel communications. New bounds are developed to tighten the standard cut-set bound for multi-casting functions.

As an additional example of low-complexity codes, reduced-dimension linear transforms and convex optimization methods are proposed for the lossy transmission of correlated sources across noisy networks. Surprisingly, simple un-coded or one-shot strategies achieve a performance which is exactly optimal in certain networks, or close to optimal in the low signal-to-noise regime relevant for sensor networks.

To Mom, Pa, and Vikas
for their love and support.

Contents

List of Figures

List of Tables

Acknowledgments

It has been a remarkable time at Berkeley during my years in the doctoral program. I am deeply grateful for the invaluable guidance and support from distinguished mentors, colleagues, and friends.

I would like to thank Michael Gastpar for being a superb advisor, patient mentor, and steady collaborator over the years. As I have realized, it requires a great deal of patience to accept the responsibilities of an advisor and maintain the high standards of a respected professor. I am grateful for Michael's flexibility, focus, and commitment to the pursuit of innovative theories of information. I was granted the independence to pursue my own ideas while receiving fresh perspectives and intuition. I thank Michael for providing generous support in his research groups both at U.C. Berkeley and at EPFL, Switzerland.

I would like to offer special thanks to professors Jim Pitman and Venkat Anantharam for several meetings and discussions which have helped strengthen my thesis contributions. I am very grateful for their teaching in the classroom and their guidance outside the classroom at critical periods of time. I hope to gain even a fraction of their intuition and knowledge in my future studies. As far as words may express, I feel that their hard-work and dedication to teaching and research at Berkeley is exceptional.

I thank professors Murat Arcak, Jim Pitman, and Kannan Ramchandran for their thoughtful advice and feedback as thesis committee members. The direction provided both during the qualifying exam and beyond was crucial for measuring my progress. In addition, I thank Prof. Arcak for offering me the opportunity to be a recitation instructor in his class, and the chance to provide one substitute lecture on the topic of signals and systems. Through experience, I realized that I had to obtain a crystal-clear understanding to teach concepts such as Fourier analysis to younger students who conjured up a myriad of questions.

In terms of research collaborations, I would like to acknowledge many fruitful discussions and the exchange of ideas from the following collaborators in alphabetical order: Prof. Emmanuel Abbe of Princeton University; Prof. Sang-Woon Jeon of Andong National University; Dr. Satish Babu Korada, graduate of EPFL and post-doctoral scholar at Stanford University; Prof. Galen Reeves of Duke University; and Prof. Changho Suh of KAIST. Emmanuel introduced me to topics in applied mathematics, and Sang-Woon taught me about coding in multi-hop networks. Satish introduced me to the theory of polar codes, and Galen offered enthusiastic discussions about compressed sensing. Changho introduced me to converse theorems, and a deeper understanding of interference alignment.

My fellow students, colleagues, and friends have contributed immensely to my experience at Berkeley. In particular, I am indebted to Se Yong Park, Venkatesan Ekambaram, and Nebojsa Milosavljevic for countless discussions about research and life. For creating a stimulating research environment at U.C. Berkeley during group meetings, I thank all SIPC members including Krish Eswaran, Nebojsa Milosavljevic, Bobak Nazer, Galen Reeves, Anand Sarwate, and Jiening Zhan. Senior members Prof. Bobak Nazer now at Boston University and Prof. Anand Sarwate now at Rutgers University set the bar for achievement very high. I am fortunate to be an alumni of the Wireless Foundations Center at Berkeley comprised

of core professors such as Prof. Venkat Anantharam, Prof. Kannan Ramchandran, Prof. Anant Sahai, Prof. David Tse, and Prof. Martin Wainwright. I am thankful for colleagues such as Guy Bresler, Amin Gohari, Kate Harrison, Varun Jog, Sudeep Kamath, Sreeram Kannan, Po-Ling Loh, Mohammad Ali Maddah-Ali, Sahand Negahban, Nima Noorshams, Barlas Oguz, Dapo Omidiran, Sameer Pawar, Gireeja Ranade, Rashmi and Nihar Shah, I-Hsiang Wang, Kristen Woyach, and Baosen Zhang.

I thank the American Society for Engineering Education for providing an NDSEG graduate fellowship for the first three years of my doctoral program. The fellowship granted me the freedom to explore new directions early as a graduate student at Berkeley. I am thankful to EPFL in Switzerland for graciously hosting me as an exchange student for over a year and a half. Living at the edge of Lake Lausanne was a blessing. The intensity of research was balanced by the calm of the Swiss Alps. I would like to express my gratitude to the LINX group at EPFL including members Sang-Woon Jeon, Chien-Yi Wang, and Jingge Zhu. In addition, France Faille was a constant source of encouragement and motherly affection. I thank her for organizing all the group activities such as ice skating and fondue, and for helping me practice the French language.

I owe all of my education since I was a child to my parents and brother. My father taught me mathematics from a young age, and my mother would read books to me. If it were not for their sacrifices and dedicated support from the beginning, I would not have the audacity or strength to embark upon the long journey of the doctoral program.

Fall 2013, U.C. Berkeley
Naveen Goela

Chapter 1

Dissertation Overview

1.1 Information Theory, Statistics, and New Codes

The field of information theory was pioneered by Claude Shannon beginning in 1948 to understand the fundamental limits of communication systems. The probabilistic method applied to random codes proved the existence of capacity-achieving codes for point-to-point discrete, memoryless channels. However, early ideas such as random code ensembles did not solve the problem of constructing explicit codes with low encoding and decoding complexity. In recent years, several capacity-achieving explicit codes for point-to-point channels have been invented (e.g., spatially-coupled codes, Arıkan's polar codes). However, in the case of multi-user channels and network communication, questions regarding finding the exact capacity region and questions regarding finding good low-complexity codes remain open to a large extent. It is intriguing that Shannon's abstraction of information as bits is challenged in networks. Furthermore, basic tools in networks such as cut-set bounds fail to establish fundamental limits when information is "mixed" in network pathways. In this thesis, progress is made towards designing low-complexity capacity-achieving codes for classes of networks.

How is it possible to design low-complexity capacity-achieving codes? One idea is to create and exploit structure in a code. The structure serves two chief purposes: (i) Low-complexity encoding and decoding become possible using recursive methods; (ii) It is mathematically tractable to "extrapolate to infinity" in proofs to verify achievable rates. Beyond Shannon's original idea of using randomness, the element of structure appears to be crucial. Somewhat counter-intuitively, structure may coexist with randomness.[1] This thesis demonstrates the advantages of using both randomness and structure (e.g., algebraic structure) in the design of network codes.

One way of discovering structure in a world of randomness and random variables is now understood and it was first published in 2008 by E. Arıkan. This method is regarding the polarization of discrete random variables. Briefly, Arıkan's original concept is about

[1] For example, the Green-Tao theorem in mathematics elucidates a surprising structure and randomness appearing in the sequence of primes.

extracting the randomness inherent in a sequence of independent and identically distributed binary random variables. Due to applying an algebraic transformation on the sequence of variables, suitably defined conditional entropies of the transformed variables converge to zero or one as the length of the sequence increases to infinity. The convergence is proven using a new application of Martingales from probability theory. Moreover, codes built on the polarization principle achieve capacity for point-to-point noisy channels. The elegant recursive structure of polar codes, a butterfly structure similar to the pattern found in computing the Fast Fourier Transform, is the key to low-complexity encoding and decoding via a dynamic programming, "divide-and-conquer", successive cancelation algorithm.

Building upon polarization principles, this thesis develops new low-complexity codes for multi-user channels. A particular focus is on the broadcast channel, whose capacity is unknown, except for a few special classes of channels. In Chapters 2-Chapter 5 based on [42], new practical broadcast code constructions are able to approach the capacity boundary for almost all of these special classes. The new codes also apply to general classes of channels. In prior research, sub-optimal coding strategies and heuristics were employed. For example, in the case of deterministic broadcast channels, researchers tried low-density parity-check codes (LDPC), reinforced belief propagation, and constraint satisfaction algorithms. The new code constructions of this thesis provide insight on the information-theoretic arguments underlying Cover's superposition codes and Marton's ingenious broadcast construction for noisy channels.

The concept of polarization of random variables is quite broad and offers a new perspective in statistics itself. The ideas developed in this thesis bear the potential to lead to new capacity theorems that are outside the reach of classical random coding arguments. Experimental evidence and reproducible simulations are recorded for the first practical broadcast codes with optimal asymptotic properties. The theory sheds light on important questions about engineering communication systems using modern circuits.

1.2 The Abstraction of Information in Networks

In network information theory, it is an open question whether the abstraction of information as bits is correct or whether there exists a broader representation. One idea is to understand network information as a transmission of functions of original sources. In Chapter 6, a network computing problem is studied (drawing from material in [41, 87]) and related to the well-known multiple-unicast communication problem. In the network computing problem, each receiver computes the same identical function of multiple sources. In this thesis, the computation capacity is determined for a countably-infinite class of simple, interfering networks. A new network decomposition theorem and function alignment code are derived. Vector-space function alignment is inspired by the idea of interference alignment for channel communications. In addition, new linear coding arguments for multi-casting functions and new information-theoretic bounds are provided which sharpen ordinary cut-set bounds.

Chapters 7 and 8 provide analysis for the lossy transmission of distributed, correlated

sources across noisy networks [39]. In certain cases such as biological systems, it might not be feasible or valuable to code and represent information as bits. Rather, un-coded and one-shot strategies offer low delay and low-complexity solutions. Linear transforms are proposed for dimensionality-reduction of distributed sources while convex optimization methods are applied to handle power constraints. New cut-set bounds link information theory and signal processing in networks.

Part I

Polar Codes For Networks

Chapter 2

Polarization of Random Variables

2.1 Overview of Theory

The following theory by Arıkan [6] characterizes the polarization of random variables which is applicable for both channel and source coding.

Theorem 1 (Polarization of Random Variables)**.** *Let*

$$\vec{Y} = [Y_1, Y_2, \ldots, Y_n],$$
$$\vec{Z} = [Z_1, Z_2, \ldots, Z_n],$$

be two independent and identically distributed row vectors of random variables where $(Y_j, Z_j) \sim P_{YZ}$*,* $j \in [n]$*, and* $n = 2^\ell$ *for integer* $\ell \geq 1$*. Consider polarized random variables* $\vec{U} = \vec{Y}F_nB_n$ *and* $\vec{V} = \vec{Z}F_nB_n$*, where the matrix* B_n *is a bit-reversal matrix as defined by Arıkan in [6] and*

$$F_n = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{\otimes \log_2(n)}.$$

Then as $n \to \infty$*, for any* $\epsilon \in (0, 1)$*,*

$$\frac{1}{n}\Big|\big\{j \in [n] : H(U_j|U_1^{j-1}) \geq 1 - \epsilon\big\}\Big| \to H(Y),$$
$$\frac{1}{n}\Big|\big\{j \in [n] : H(V_j|V_1^{j-1}, Y_1^n) \geq 1 - \epsilon\big\}\Big| \to H(Z|Y).$$

Notation: *Let* $H(U_j|U_1^{j-1})$ *denote the conditional entropy between random variables where* U_1^{j-1} *is shorthand notation for the set of random variables* $\{U_1, U_2, \ldots, U_{j-1}\}$*. Similarly,* $H(V_j|V_1^{j-1}, Y_1^n)$ *represents the conditional entropy and* $Y_1^n = \{Y_1, Y_2, \ldots, Y_n\}$*. The notation* $\otimes$ *denotes the Kronecker matrix product.*

2.1.1 Estimating Conditional Entropies By Sampling

Although Theorem 1 was a break-through in information theory, an even more important part of polarization is the dynamic programming method associated with computing probabilities and estimating entropies. As in Theorem 1, define the following row vectors

$$\vec{Y} = [Y_1, Y_2, \ldots, Y_n],$$
$$\vec{Z} = [Z_1, Z_2, \ldots, Z_n],$$

where for $j \in [n]$, the random variables $(Y_j, Z_j) \sim P_{YZ}$. In addition, the polarized variables

$$\vec{U} = [U_1, U_2, \ldots, U_n],$$
$$\vec{V} = [V_1, V_2, \ldots, V_n],$$

where $\vec{U} = \vec{Y}F_nB_n$ and $\vec{V} = \vec{Z}F_nB_n$ as in Theorem 1. We would like to compute the entropy terms $H(U_j|U_1^{j-1})$ and $H(V_j|V_1^{j-1}, Y_1^n)$ numerically to simulate the polarization phenomenon. The basic formula for the conditional entropies is

$$H(U_j|U_1^{j-1}) \triangleq -\mathbb{E}_{U_1^j} \log_2 \left[P_{U_j|U_1^{j-1}}(U_j|U_1^{j-1}) \right], \tag{2.1}$$
$$H(V_j|V_1^{j-1}, Y_1^n) \triangleq -\mathbb{E}_{V_1^j, Y_1^n} \log_2 \left[P_{V_j|V_1^{j-1}, Y_1^n}(V_j|V_1^{j-1}, Y_1^n) \right]. \tag{2.2}$$

The expectations in the formulae for the conditional entropies imply averaging over samples drawn from the joint distribution of $\vec{U}$ and $\vec{V}$. Equivalently, we can sample from the simple independent and identically distributed joint distribution of $\vec{Y}$ and $\vec{Z}$ and apply a polar transformation to the samples.

2.1.2 Dynamic Programming and Numerically Robust Recursions

The previous subsection showed that the conditional entropies may be estimated by sampling from the appropriate distributions and computing *probabilities* as in Equation (2.1) and Equation (2.2). Fortunately, the probabilities may be computed recursively. The recursions were derived originally by Arıkan as a part of the low-complexity successive cancelation decoder [6]. In those recursions, the ratios of probabilities (likelihoods) were computed. However, since probabilities are bounded, we will compute them instead of likelihoods to maintain numerical stability.

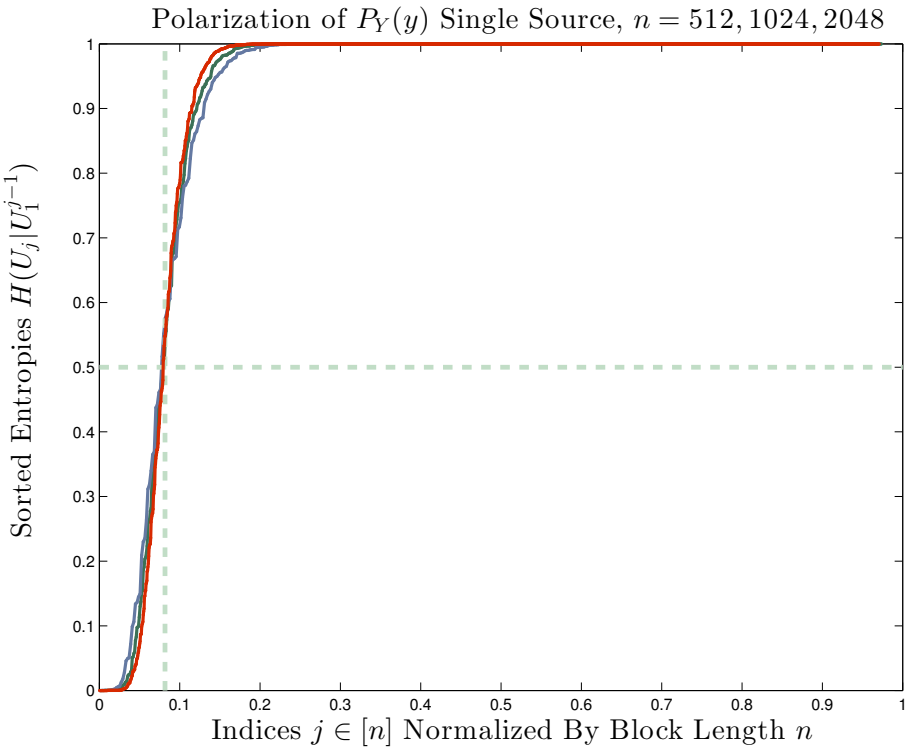


Figure 2.1: Polarization of a Bernoulli source distribution $P_Y(y)$ defined by $P_Y(0) = \frac{2}{3}$.

In the base case, the block length of the polar transform is $n = 2$.

$$\begin{aligned} P_2^{(1)} &\triangleq \mathsf{Pr}\{U_1 = 0\} \\ &= \mathsf{Pr}\{Y_1 \oplus Y_2 = 0\} \\ &= P_Y(0)P_Y(0) + P_Y(1)P_Y(1). \\ P_2^{(2)}\left[u_1\right] &\triangleq \mathsf{Pr}\{U_2 = 0 | U_1 = u_1\} \\ &= \frac{\mathsf{Pr}\{Y_2 = 0, Y_1 \oplus Y_2 = u_1\}}{\mathsf{Pr}\{Y_1 \oplus Y_2 = u_1\}} \\ &= \frac{P_Y(u_1)P_Y(0)}{P_Y(0)P_Y(u_1) + P_Y(1)P_Y(u_1 \oplus 1)}. \end{aligned}$$

Our aim is to compute the following probabilities for arbitrary $n = 2^\ell$ and integer $\ell \geq 1$.

$$P_n^{(j)}\left[u_1^{j-1}\right] \triangleq \mathsf{Pr}\{U_j = 0 | U_1^{j-1} = u_1^{j-1}\}.$$

This is possible due to a "divide and conquer" step for $n > 2$. Define the following

sub-problems

$$\Xi_1 = P_{\frac{n}{2}}^{(j)}\left[u_{o,1}^{2j-2} \oplus u_{e,1}^{2j-2}\right],$$
$$\Xi_2 = P_{\frac{n}{2}}^{(j)}\left[u_{e,1}^{2j-2}\right],$$

where the notation $u_{o,1}^{2j-2}$ and $u_{e,1}^{2j-2}$ represents the odd and even indices respectively of the sequence u_1^{2j-2}. The recursive computation of the probabilities is characterized by

$$P_n^{(2j-1)}\left[u_1^{2j-2}\right] = 1 - \Xi_1 - \Xi_2 + 2\Xi_1\Xi_2.$$

$$P_n^{(2j)}\left[u_1^{2j-1}\right] \triangleq \begin{cases} \dfrac{\Xi_1\Xi_2}{1-\Xi_1-\Xi_2+2\Xi_1\Xi_2} & \text{if } u_{2j-1}=0 \\ \dfrac{\Xi_2-\Xi_1\Xi_2}{\Xi_1+\Xi_2-2\Xi_1\Xi_2} & \text{if } u_{2j-1}=1 \end{cases}$$

It can be shown that if $u_{2j-1} = 0$, then it is not possible for $(\Xi_1, \Xi_2) = (0, 1)$ or $(\Xi_1, \Xi_2) = (1, 0)$. Similarly, if $u_{2j-1} = 1$, it is not possible for $(\Xi_1, \Xi_2) = (0, 0)$ or $(\Xi_1, \Xi_2) = (1, 1)$. Therefore the denominators in $P_n^{(2j)}\left[u_1^{2j-1}\right]$ will not be zero.

Example 1. *Consider a Bernoulli source distribution $P_Y(y)$ given as follows: $P_Y(0) = \frac{2}{3}$. Let $\vec{Y} = [Y_1, Y_2, \ldots, Y_n]$ be independent and identically distributed random variables where $Y_j \sim P_Y$, $j \in [n]$, and $n = 2^\ell$ for integer $\ell \geq 1$. Consider polarized random variables $\vec{U} = \vec{Y}F_nB_n$. Figure 2.1 plots the sorted values in the set $\{H(U_j|U_1^{j-1})\}_{j\in[n]}$. Due to Theorem 1, the fraction of indices that are close to 1 approaches $H(Y) = h_b(\frac{2}{3})$. The polarization phenomenon is depicted for finite block lengths $n = 512, 1024, 2048$.*

2.1.3 Dynamic Programming and Numerically Robust Recursions: Extension

To extend the analysis of the previous subsection, consider further conditioning in the probabilities. Again, the base case begins with $n = 2$.

$$\begin{aligned} P_2^{(1)}\left[y_1^2\right] &\triangleq \mathsf{Pr}\{V_1 = 0 | Y_1^2 = y_1^2\} \\ &= \frac{\mathsf{Pr}\{Z_1 \oplus Z_2 = 0, Y_1^2 = y_1^2\}}{\mathsf{Pr}\{Y_1^2 = y_1^2\}} \\ &= \frac{P_{YZ}(y_1,0)P_{YZ}(y_2,0) + P_{YZ}(y_1,1)P_{YZ}(y_2,1)}{P_Y(y_1)P_Y(y_2)}. \\ P_2^{(2)}\left[v^1, y^{1:2}\right] &\triangleq \mathsf{Pr}\{V_2 = 0 | V_1 = v_1, Y_1^2 = y_1^2\} \\ &= \frac{\mathsf{Pr}\{Z_2 = 0, Z_1 \oplus Z_2 = v_1, Y_1^2 = y_1^2\}}{\mathsf{Pr}\{Z_1 \oplus Z_2 = v_1, Y_1^2 = y_1^2\}} \\ &= \frac{P_{YZ}(y_1,v_1)P_{YZ}(y_2,0)}{P_{YZ}(y_1,0)P_{YZ}(y_2,v_1) + P_{YZ}(y_1,1)P_{YZ}(y_2,v_1\oplus 1)}. \end{aligned}$$

The aim is to compute the following probabilities for arbitrary $n = 2^\ell$ and integer $\ell \geq 1$.

$$P_n^{(j)}\left[v_1^{j-1}, y_1^n\right] \triangleq \mathsf{Pr}\{V_j = 0 | V_1^{j-1} = v_1^{j-1}, Y_1^n = y_1^n\}.$$

This is possible due to a "divide and conquer" step for $n > 2$. Define the following sub-problems

$$\Lambda_1 = P_{\frac{n}{2}}^{(j)}\left[v_{o,1}^{2j-2} \oplus v_{e,1}^{2j-2}, y^{1:\frac{n}{2}}\right],$$
$$\Lambda_2 = P_{\frac{n}{2}}^{(j)}\left[v_{e,1}^{2j-2}, y^{\frac{n}{2}+1:n}\right],$$

where the notation $v_{o,1}^{2j-2}$ and $v_{e,1}^{2j-2}$ represents the odd and even indices respectively of the sequence v_1^{2j-2}. The recursive computation of the probabilities is characterized by

$$P_n^{(2j-1)}\left[v_1^{2j-2}, y_1^n\right] = 1 - \Lambda_1 - \Lambda_2 + 2\Lambda_1\Lambda_2.$$

$$P_n^{(2j)}\left[v_1^{2j-1}, y_1^n\right] \triangleq \begin{cases} \dfrac{\Lambda_1\Lambda_2}{1 - \Lambda_1 - \Lambda_2 + 2\Lambda_1\Lambda_2} & \text{if } v_{2j-1} = 0 \\ \dfrac{\Lambda_2 - \Lambda_1\Lambda_2}{\Lambda_1 + \Lambda_2 - 2\Lambda_1\Lambda_2} & \text{if } v_{2j-1} = 1 \end{cases}$$

It can be shown that if $v_{2j-1} = 0$, then it is not possible for $(\Lambda_1, \Lambda_2) = (0, 1)$ or $(\Lambda_1, \Lambda_2) = (1, 0)$. Similarly, if $v_{2j-1} = 1$, it is not possible for $(\Lambda_1, \Lambda_2) = (0, 0)$ or $(\Lambda_1, \Lambda_2) = (1, 1)$. Therefore the denominators in $P_n^{(2j)}\left[v_1^{2j-1}, y_1^n\right]$ will not be zero.

Example 2. *Consider a joint distribution $P_{YZ}(y, z)$ given as follows: $P_{YZ}(0,0) = P_{YZ}(0,1) = P_{YZ}(1,1) = \frac{1}{3}$. Let $\vec{Y} = [Y_1, Y_2, \ldots, Y_n]$ and $\vec{Z} = [Z_1, Z_2, \ldots, Z_n]$ be two independent and identically distributed row vectors of random variables where $(Y_j, Z_j) \sim P_{YZ}$, $j \in [n]$, and $n = 2^\ell$ for integer $\ell \geq 1$. Consider polarized random variables $\vec{U} = \vec{Y}F_nB_n$ and $\vec{V} = \vec{Z}F_nB_n$. Figure 2.2 plots the sorted values in the set $\{H(V_j|V_1^{j-1}, Y_1^n)\}_{j\in[n]}$. Due to Theorem 1, the fraction of indices that are close to 1 approaches $H(Z|Y) = \frac{2}{3}$. The polarization phenomenon is depicted for finite block lengths $n = 512, 1024, 2048$.*

2.2 Polar Codes for Multi-User Networks

2.2.1 Deterministic Broadcast Channels

The deterministic broadcast channel has received considerable attention in the literature (e.g. due to related extensions such as secure broadcast, broadcasting with side information, and index coding [12, 79]). Several *practical* codes have been designed. For example, the authors of [93] propose sparse linear coset codes to emulate random binning and survey propagation to enforce broadcast channel constraints. In [20], the authors propose enumerative source

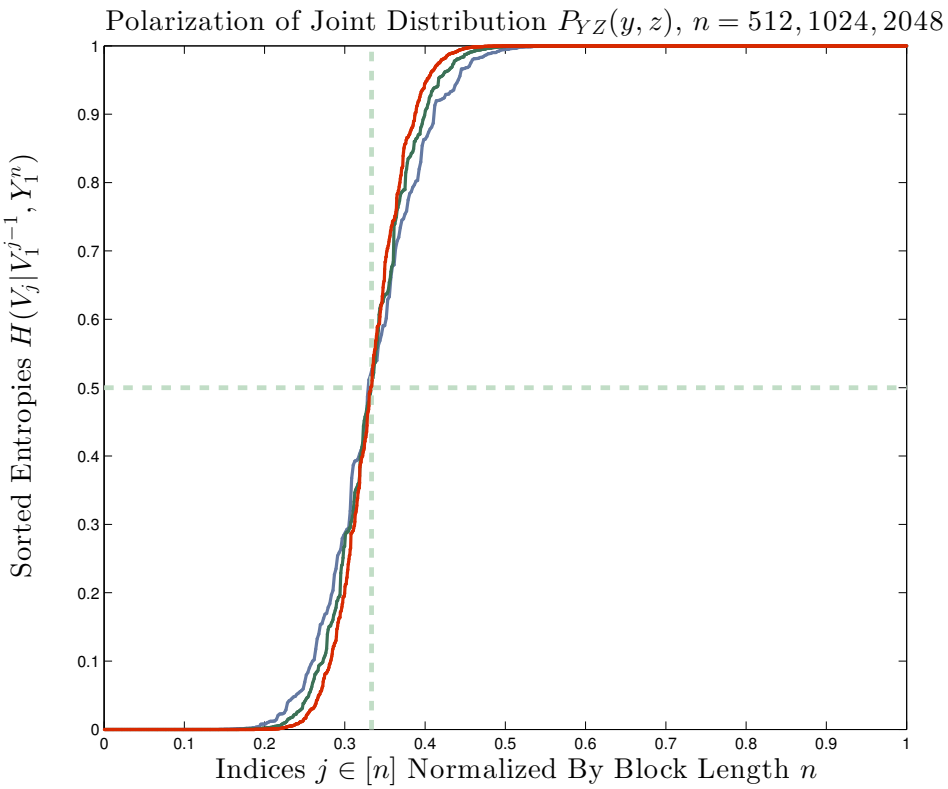


Figure 2.2: Polarization of a joint distribution of binary random variables $P_{YZ}(y,z)$ defined by $P_{YZ}(0,0) = P_{YZ}(0,1) = P_{YZ}(1,1) = \frac{1}{3}$.

coding and Luby-Transform codes for deterministic DM-BCs specialized to interference-management scenarios. Additional research includes reinforced belief propagation with non-linear coding [16]. To our knowledge, polarization-based codes provide provable guarantees for achieving rates on the capacity-boundary in the general case.

2.2.2 Polar Codes for Multi-User Settings

Subsequent to the derivation of channel polarization in [6] and the refined rate of polarization in [9], polarization methods have been extended to analyze multi-user information theory problems. In [2], a joint polarization method is proposed for m-user MACs with connections to matroid theory. Polar codes were extended for several other multi-user settings: arbitrarily-permuted parallel channels [48], degraded relay channels [51], cooperative relaying [14], and wiretap channels [4, 61, 57]. In addition, several binary multi-user communication scenarios including the Gelfand-Pinsker problem, and Wyner-Ziv problem were analyzed in [55, Chapter 4]. Polar codes for lossless and lossy source compression were investigated respectively in [7] and [54]. In [7], source polarization was extended to the Slepian-Wolf problem involving distributed sources. The approach is based on an "onion-

peeling" encoding of sources, whereas a joint encoding is proposed in [1]. In [8], a unified approach is provided for the Slepian-Wolf problem based on generalized monotone chain rules of entropy. To our knowledge, the design of polarization-based broadcast codes is relatively new.

2.2.3 Binary vs. q-ary Polarization

The broadcast codes constructed in this thesis for DM-BCs are based on polarization for binary random variables. However, in extending to arbitrary alphabet sizes, a large body of prior work exists and has focused on generalized constructions and kernels [56], and generalized polarization for q-ary random variables and q-ary channels [24, 64, 81, 71]. The reader is also referred to the monograph in [82] containing a clear overview of polarization methods.

2.3 Polar Codes For Broadcast Channels

Introduced by T. M. Cover in 1972, the broadcast problem consists of a single source transmitting m independent private messages to m receivers through a single discrete, memoryless, broadcast channel (DM-BC) [22]. The private-message capacity region is known if the channel structure is *deterministic*, *degraded*, *less-noisy*, or *more-capable* [33]. For general classes of DM-BCs, there exist inner bounds such as Marton's inner bound [63] and outer bounds such as the Nair-El-Gamal outer bound [66]. One difficult aspect of the broadcast problem is to design an encoder which maps m independent messages to a single codeword of symbols which are transmitted simultaneously to all receivers. Several codes relying on *random binning*, *superposition*, and *Marton's strategy* have been analyzed in the literature (see e.g., the overview in [23]).

2.3.1 Overview of Contributions

The first part of this thesis focuses on low-complexity codes for broadcast channels based on polarization methods. Polar codes were invented originally by Arıkan and were shown to achieve the capacity of binary-input, symmetric, point-to-point channels with $\mathcal{O}(n \log n)$ encoding and decoding complexity where n is the code length [6]. We obtain the following results.

- Polar codes for deterministic, linear and non-linear, binary-output, m-user DM-BCs (cf. [40]). The capacity-achieving broadcast codes implement low-complexity *random binning*, and are related to polar codes for other multi-user scenarios such as Slepian-Wolf distributed source coding [7, 8], and multiple-access channel (MAC) coding [2]. For deterministic DM-BCs, the polar transform is applied to channel *output* variables. Polarization is useful for shaping uniformly random message bits from m independent messages into non-equiprobable codeword symbols in the presence of hard broadcast

constraints. As discussed in Section 2.2.1 and referenced in [93, 20, 16], it is difficult to design low-complexity parity-check (LDPC) codes or belief propagation algorithms for the deterministic DM-BC due to multi-user broadcast constraints.

- Polar codes for general two-user DM-BCs based on *Cover's superposition coding* strategy. In the multi-user setting, constraints on the auxiliary and channel-input distributions are placed to ensure alignment of polarization indices. The achievable rates lie on the boundary of the capacity region for certain classes of DM-BCs such as binary-input stochastically degraded channels.

- Polar codes for general two-user DM-BCs based on *Marton's coding* strategy. In the multi-user setting, due to the structure of polarization, constraints on the auxiliary and channel-input distributions are identified to ensure alignment of polarization indices. The achievable rates lie on the boundary of the capacity region for certain classes of DM-BCs such as binary-input semi-deterministic channels.

- For the above broadcast polar codes, the asymptotic decay of the average error probability under successive cancelation decoding at the broadcast receivers is established to be $\mathcal{O}(2^{-n^{\beta}})$ where $0 < \beta < \frac{1}{2}$. The error probability is analyzed by averaging over polar code ensembles. In addition, properties such as the chain rule of the Kullback-Leibler divergence between discrete probability measures are exploited.

- Reproducible experiments are provided for finite block lengths up to $n = 1024$. The results of the experiments corroborate the theory.

For different broadcast coding strategies, a systems-level block diagram of the communication channel and polar transforms is provided.

2.3.2 Notation

An index set $\{1, 2, \ldots, m\}$ is abbreviated as $[m]$. An $m \times n$ matrix array of random variables is comprised of variables $Y_i(j)$ where $i \in [m]$ represents the row and $j \in [n]$ the column. The notation $Y_i^{k:\ell} \triangleq \{Y_i(k), Y_i(k+1), \ldots, Y_i(\ell)\}$ for $k \leq \ell$. When clear by context, the term Y_i^n represents $Y_i^{1:n}$. In addition, the notation for the random variable $Y_i(j)$ is used interchangeably with Y_i^j. The notation $f(n) = \mathcal{O}(g(n))$ means that there exists a constant κ such that $f(n) \leq \kappa g(n)$ for sufficiently large n. For a set $\mathcal{S}$, $\mathrm{clo}(\mathcal{S})$ represents set closure, and $\mathrm{co}(\mathcal{S})$ the convex hull operation over set $\mathcal{S}$. Let $h_b(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ denote the binary entropy function. Let $a * b \triangleq (1-a)b + a(1-b)$.

Chapter 3

Deterministic Broadcast Channels

3.1 Channel Capacity

Definition 1 (Discrete, Memoryless Broadcast Channel)**.** *The discrete memoryless broadcast channel (DM-BC) with m broadcast receivers consists of a discrete input alphabet $\mathcal{X}$, discrete output alphabets $\mathcal{Y}_i$ for $i \in [m]$, and a conditional distribution $P_{Y_1,Y_2,\ldots,Y_m|X}(y_1, y_2, \ldots, y_m|x)$ where $x \in \mathcal{X}$ and $y_i \in \mathcal{Y}_i$.*

Definition 2 (Private Messages)**.** *For a DM-BC with m broadcast receivers, there exist m private messages $\{W_i\}_{i\in[m]}$ such that each message W_i is composed of nR_i bits and $(W_1, W_2, \ldots, W_m)$ is uniformly distributed over $[2^{nR_1}] \times [2^{nR_2}] \times \cdots \times [2^{nR_m}]$.*

Definition 3 (Channel Encoding and Decoding)**.** *For the DM-BC with independent messages, let the vector of rates $\vec{R} \triangleq \begin{bmatrix} R_1 & R_2 & \ldots & R_m \end{bmatrix}^T$. An $(\vec{R}, n)$ code for the DM-BC consists of one encoder*

$$x^n : [2^{nR_1}] \times [2^{nR_2}] \times \cdots \times [2^{nR_m}] \to \mathcal{X}^n,$$

and m decoders specified by $\hat{W}_i : \mathcal{Y}_i^n \to [2^{nR_i}]$ for $i \in [m]$. Based on received observations $\{Y_i(j)\}_{j\in[n]}$, each decoder outputs a decoded message $\hat{W}_i$.

Definition 4 (Average Probability of Error)**.** *The average probability of error $P_e^{(n)}$ for a DM-BC code is defined to be the probability that the decoded message at all receivers is not equal to the transmitted message,*

$$P_e^{(n)} = \mathbb{P}\left\{\bigvee_{i=1}^{m} \hat{W}_i\left(\{Y_i(j)\}_{j\in[n]}\right) \neq W_i\right\}.$$

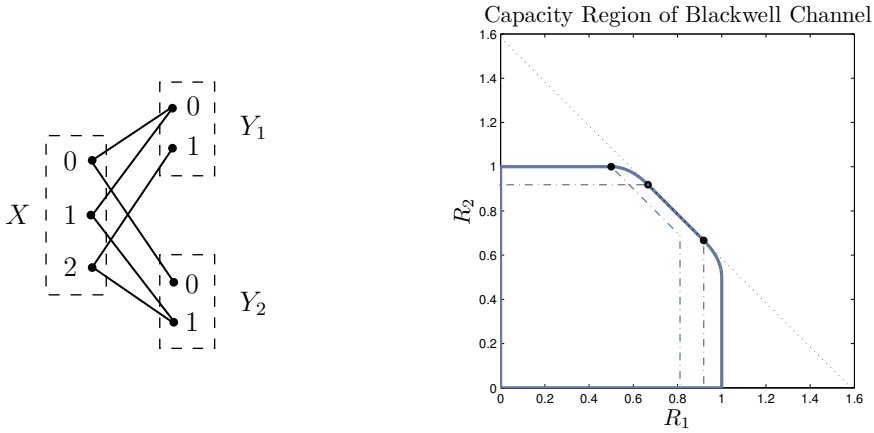


Figure 3.1: Blackwell's broadcast channel and private-message capacity region.

Definition 5 (Private-Message Capacity Region)**.** *If there exists a sequence of* $(\vec{R}, n)$ *codes with* $P_e^{(n)} \to 0$*, then the rates* $\vec{R} \in \mathbb{R}_+^m$ *are achievable. The private-message capacity region is the closure of the set of achievable rates.*

Definition 6 (Deterministic DM-BC)**.** *Define* m *deterministic functions* $f_i(x) : \mathcal{X} \to \mathcal{Y}_i$ *for* $i \in [m]$*. The deterministic DM-BC with* m *receivers is defined by the following conditional distribution*

$$P_{Y_1,Y_2,\ldots,Y_m|X}(y_1, y_2, \ldots, y_m|x) = \prod_{i=1}^{m} \mathbb{1}_{[y_i = f_i(x)]}. \tag{3.1}$$

3.1.1 Capacity Region

Proposition 1 (Marton [62], Pinsker [72])**.** *The capacity region of the deterministic DM-BC includes those rate-tuples* $\vec{R} \in \mathbb{R}_+^m$ *in the region*

$$\mathfrak{C}_{DET\text{–}BC} \triangleq \operatorname{co}\Big(\operatorname{clo}\Big(\bigcup_{X,\{Y_i\}_{i\in[m]}} \mathfrak{R}\big(X, \{Y_i\}_{i\in[m]}\big)\Big)\Big), \tag{3.2}$$

where the polyhedral region $\mathfrak{R}(X, \{Y_i\}_{i\in[m]})$ *is given by*

$$\mathfrak{R} \triangleq \Big\{\vec{R} \;\Big|\; \sum_{i\in\mathcal{S}} R_i < H(\{Y_i\}_{i\in\mathcal{S}}),\ \forall \mathcal{S} \subseteq [m]\Big\}. \tag{3.3}$$

The union in Eqn. (3.2) is over all random variables $X, Y_1, Y_2, \ldots, Y_m$ *with joint distribution induced by* $P_X(x)$ *and* $Y_i = f_i(X)$*.*

Example 3 (Blackwell Channel)**.** *In Figure 3.1, the Blackwell channel is depicted with* $\mathcal{X} = \{0, 1, 2\}$ *and* $\mathcal{Y}_i = \{0, 1\}$*. The channel is defined as* $Y_1 = f_1(X)$ *and* $Y_2 = f_2(X)$ *where the* non-linear *functions* $f_1(x) = \max(x - 1, 0)$ *and* $f_2(x) = \min(x, 1)$*. For any fixed distribution* $P_X(x)$*, it is seen that* $P_{Y_1Y_2}(y_1, y_2)$ *has* zero mass *for the pair* $(1, 0)$*. Let* $\alpha \in [\frac{1}{2}, \frac{2}{3}]$*. Due to the symmetry of this channel, the capacity region is the union of two regions,*

$$\{(R_1, R_2) : \ R_1 \leq h_b(\alpha), R_2 \leq h_b(\frac{\alpha}{2}), R_1 + R_2 \leq h_b(\alpha) + \alpha\},$$
$$\{(R_1, R_2) : \ R_1 \leq h_b(\frac{\alpha}{2}), R_2 \leq h_b(\alpha), R_1 + R_2 \leq h_b(\alpha) + \alpha\},$$

where the first region is achieved with input distribution $P_X(0) = P_X(1) = \frac{\alpha}{2}$*, and the second region is achieved with* $P_X(1) = P_X(2) = \frac{\alpha}{2}$ *[33, Lec. 9]. The sum rate is maximized for a uniform input distribution which yields a pentagonal achievable rate region:* $R_1 \leq h_b(\frac{1}{3})$*,* $R_2 \leq h_b(\frac{1}{3})$*,* $R_1 + R_2 \leq \log_2 3$*. For different input distributions* $P_X(x)$*, the achievable rate points are contained within corresponding polyhedrons in* $\mathbb{R}_+^m$ *where* $m = 2$ *for this example. Figure 3.1 illustrates the capacity region.*

3.2 Polar Coding Theorem

Theorem 2 (Polar Code for Deterministic DM-BC)**.** *Consider an* m*-user deterministic DM-BC with arbitrary discrete input alphabet* $\mathcal{X}$*, and binary output alphabets* $\mathcal{Y}_i \in \{0, 1\}$*. Fix input distribution* $P_X(x)$ *where* $x \in \mathcal{X}$ *and constant* $0 < \beta < \frac{1}{2}$*. Let* $\pi : [m] \to [m]$ *be a permutation on the index set of receivers. Let the vector*

$$\vec{R} \triangleq \left[\begin{array}{cccc} R_{\pi(1)} & R_{\pi(2)} & \ldots & R_{\pi(m)} \end{array} \right]^T.$$

There exists a sequence of polar broadcast codes over n *channel uses which achieves rates* $\vec{R}$ *where the rate for receiver* $\pi(i) \in [m]$ *is bounded as*

$$0 \leq R_{\pi(i)} < H\left(Y_{\pi(i)} | \{Y_{\pi(k)}\}_{k=1:i-1}\right).$$

The average error probability of this code sequence decays as $P_e^{(n)} = \mathcal{O}(2^{-n^\beta})$*. The complexity of encoding and decoding is* $\mathcal{O}(n \log n)$*.*

Remark 1. *To prove the existence of* low-complexity *broadcast codes, a successive randomized protocol is introduced in Section 3.4.1 which utilizes* $o(n)$ *bits of randomness at the encoder. A deterministic encoding protocol is also presented.*

Remark 2. *The achievable rates for a fixed input distribution* $P_X(x)$ *are the vertex points of the polyhedral rate region defined in (3.3). To achieve non-vertex points, the following*

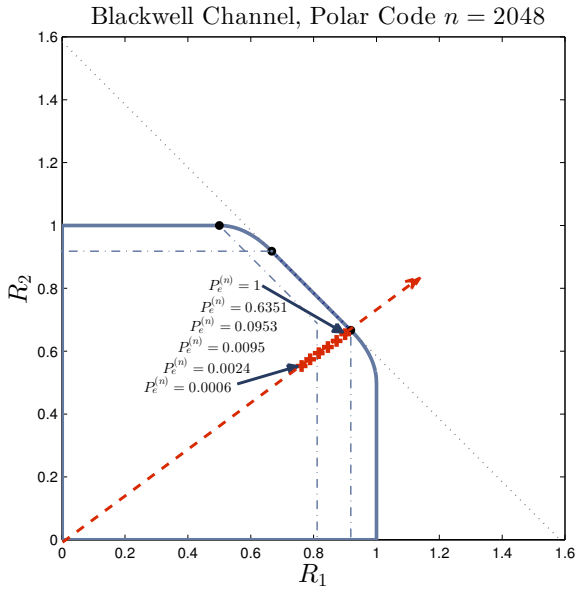


Figure 3.2: A polar code for the Blackwell channel approaching the capacity boundary point of $(R_1, R_2) = (h_b(\frac{2}{3}), \frac{2}{3})$.

coding strategies could be applied: time-sharing; rate-splitting for the deterministic DM-BC [19]; polarization by Arıkan utilizing generalized chain rules of entropy [8]. For certain input distributions $P_X(x)$, as illustrated in Figure 3.1 for the Blackwell channel, a subset of the achievable vertex points lie on the capacity boundary.

Remark 3. *Polarization of channels and sources extends to q-ary alphabets (see e.g. [24]). Similarly, it is entirely possible to extend Theorem 2 to include DM-BCs with q-ary output alphabets.*

3.2.1 Experimental Results For The Blackwell Channel

As an experiment for the Blackwell channel described in Example 3, the target rate pair on the capacity boundary is selected to be $(R_1, R_2) = (h_b(\frac{2}{3}), \frac{2}{3})$. Note that $R_1 + R_2 = \log_2 3$ which is the maximum sum rate possible for any input distribution. To achieve the target rate pair, the input distribution $P_X(x)$ is uniform. The output distribution is then $P_{Y_1Y_2}(0,0) = P_{Y_1Y_2}(0,1) = P_{Y_1Y_2}(1,1) = \frac{1}{3}$. For the output distribution, $H(Y_1) = h_b(\frac{2}{3})$ and $H(Y_2|Y_1) = \frac{2}{3}$. According to Theorem 2, these distributions permit polar codes approaching

Table 3.1: $P_e^{(n)}$ For Different Rate Pairs Achieved For The Blackwell Channel

(R_1, R_2)	n 512	n 1024	n 2048	n 4096
$(0.73, 0.53)$	0.106	0.0518	0.0195	0.0051
$(0.76, 0.55)$	0.201	0.1356	0.0631	0.0194
$(0.79, 0.57)$	0.3799	0.3177	0.2246	0.1188
$(0.82, 0.59)$	0.5657	0.5606	0.5079	0.4070
$(0.85, 0.61)$	0.7849	0.8181	0.8286	0.8133
$(0.87, 0.63)$	0.9454	0.9757	0.9866	0.9936
$(0.90, 0.65)$	0.9986	1.0000	1.0000	1.0000

the target boundary rate pair. Figure 3.2 shows the average probability of error $P_e^{(n)}$ for block length $n = 2048$ with selected rate pairs approaching the capacity boundary. The broadcast code employs a deterministic rule as opposed to a randomized rule at the encoder as described in Section 3.4.1. Table 3.1 provides results of experiments for different block lengths for a randomized rule at the encoder. While the randomized rule is important for the proof, the deterministic rule provides better error results in practice. All data points for error probabilities were generated using 10^4 codeword transmissions.

Remark 4 (Zero Error vs. Average Error)**.** *A zero-error coding scheme is trivial for rate pairs (R_1, R_2) within the triangle: $(0, 0), (0, 1), (1, 0)$. Beyond the triangular region, it is possible to achieve zero-error throughout the whole capacity region by purging the polar code-book of any codewords causing error at the encoder. However, unless there exists an efficient method to enumerate the code-book, the purging process is not feasible with low-complexity since there exist an exponential number of codewords.*

3.3 Overview of Polarization Method

For the proof of Theorem 2, we utilize binary polarization theorems. By contrast to polarization for point-to-point channels, in the case of deterministic DM-BCs, the polar transform is applied to the *output* random variables of the channel.

3.3.1 Polar Transform

Consider an input distribution $P_X(x)$ to the deterministic DM-BC. Over n channel uses, the input random variables to the channel are given by

$$X^{1:n} = \{X^1, X^2, \ldots, X^n\},$$

where $X^j \sim P_X$ are independent and identically distributed (*i.i.d.*) random variables. The channel output variables are given by $Y_i(j) = f_i(X(j))$ where $f_i(\cdot)$ are the deterministic functions to each broadcast receiver. Denote the random matrix of channel output variables by

$$\mathbf{Y} \triangleq \begin{bmatrix} Y_1^1 & Y_1^2 & Y_1^3 & \dots & Y_1^n \\ Y_2^1 & Y_2^2 & Y_2^3 & \dots & Y_2^n \\ \vdots & \vdots & \vdots & \dots & \vdots \\ Y_m^1 & Y_m^2 & Y_m^3 & \dots & Y_m^n \end{bmatrix}, \tag{3.4}$$

where $\mathbf{Y} \in \mathbb{F}_2^{m \times n}$. For $n = 2^\ell$ and $\ell \geq 1$, the polar transform is defined as the following invertible linear transformation,

$$\mathbf{U} = \mathbf{Y}\mathbf{G}_n \tag{3.5}$$
$$\text{where } \mathbf{G}_n \triangleq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{\bigotimes \log_2 n} \mathbf{B}_n.$$

The matrix $\mathbf{G}_n \in \mathbb{F}_2^{n \times n}$ is formed by multiplying a matrix of successive Kronecker matrix-products (denoted by $\bigotimes$) with a bit-reversal matrix $\mathbf{B}_n$ introduced by Arıkan [7]. The polarized random matrix $\mathbf{U} \in \mathbb{F}_2^{m \times n}$ is indexed as

$$\mathbf{U} \triangleq \begin{bmatrix} U_1^1 & U_1^2 & U_1^3 & \dots & U_1^n \\ U_2^1 & U_2^2 & U_2^3 & \dots & U_2^n \\ \vdots & \vdots & \vdots & \dots & \vdots \\ U_m^1 & U_m^2 & U_m^3 & \dots & U_m^n \end{bmatrix}. \tag{3.6}$$

3.3.2 Joint Distribution of Polarized Variables

Consider the channel output distribution $P_{Y_1 Y_2 \cdots Y_m}$ of the deterministic DM-BC induced by input distribution $P_X(x)$. The j-th *column* of the random matrix $\mathbf{Y}$ is distributed as $(Y_1^j, Y_2^j, \cdots, Y_m^j) \sim P_{Y_1 Y_2 \cdots Y_m}$. Due to the memoryless property of the channel, the joint distribution of all output variables is

$$P_{Y_1^n Y_2^n \cdots Y_m^n}\Big(y_1^n, y_2^n, \cdots, y_m^n\Big) = \prod_{j=1}^{n} P_{Y_1 Y_2 \cdots Y_m}\Big(y_1^j, y_2^j, \dots, y_m^j\Big). \tag{3.7}$$

The joint distribution of the matrix variables in $\mathbf{Y}$ is characterized easily due to the *i.i.d.* structure. The polarized random matrix $\mathbf{U}$ does *not* have an *i.i.d.* structure. However, one way to define the joint distribution of the variables in $\mathbf{U}$ is via the polar transform equation (3.5). An alternate representation is via a decomposition into conditional distributions

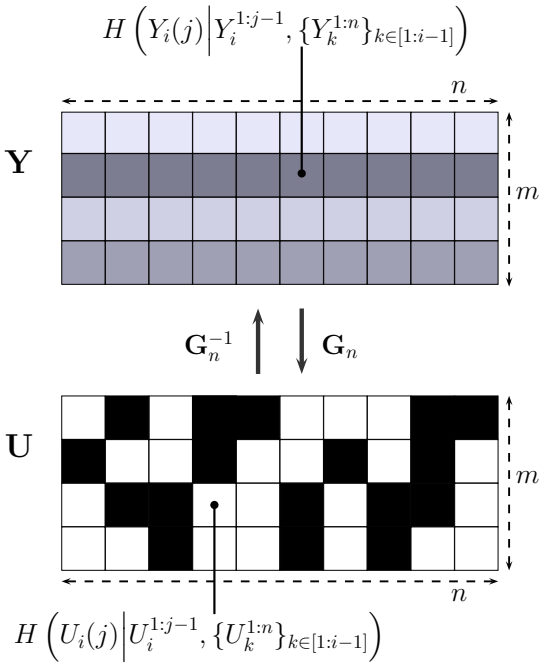


Figure 3.3: The polar transform applied to a random matrix $\mathbf{Y}$ with independent and identically distributed columns.

as follows[1].

$$P_{U_1^n U_2^n \cdots U_m^n}\left(u_1^n, u_2^n, \cdots u_m^n\right) = \prod_{i=1}^{m}\prod_{j=1}^{n} P\left(u_i(j)\middle|u_i^{1:j-1},\{u_k^{1:n}\}_{k\in[1:i-1]}\right). \tag{3.8}$$

As derived by Arıkan in [7] and summarized in Section 3.3.5, the conditional probabilities in (3.8) and associated likelihoods may be computed using a dynamic programming method which "divides-and-conquers" the computations efficiently.

3.3.3 Polarization of Conditional Entropies

Proposition 2 (Polarization [7])**.** *Consider the pair of random matrices* $(\mathbf{Y},\mathbf{U})$ *related through the polar transformation in* (3.5)*. For* $i \in [m]$ *and any* $\epsilon \in (0,1)$*, define the set of indices*

$$\mathcal{A}_i^{(n)} \triangleq \left\{j \in [n] : H\left(U_i(j)\middle|U_i^{1:j-1},\{Y_k^{1:n}\}_{k\in[1:i-1]}\right) \geq 1-\epsilon\right\}. \tag{3.9}$$

Then in the limit as $n \to \infty$*,*

$$\frac{1}{n}\left|\mathcal{A}_i^{(n)}\right| \to H(Y_i|Y_1Y_2\cdots Y_{i-1}). \tag{3.10}$$

[1]The abbreviated notation of the form $P(a|b)$ which appears in (3.8) indicates $P_{A|B}(a|b)$, i.e. the conditional probability $\mathbb{P}\{A=a|B=b\}$ where A and B are random variables.

For sufficiently large n, Theorem 2 establishes that there exist (approximately) a total of $nH\left(Y_i|Y_1Y_2\cdots Y_{i-1}\right)$ indices per row $i \in [m]$ of random matrix $\mathbf{U}$ for which the conditional entropy is close to 1. The total number of indices in $\mathbf{U}$ for which the conditional entropy terms polarize to 1 is approximately $nH(Y_1Y_2\cdots Y_m)$. The polarization phenomenon is illustrated in Figure 3.3.

Remark 5. *Since the polar transform $\mathbf{G}_n$ is invertible, $\{U_k^{1:n}\}_{k\in[1:i-1]}$ are in one-to-one correspondence with $\{Y_k^{1:n}\}_{k\in[1:i-1]}$. Therefore the conditional entropy values expressed by the terms $H\big(U_i(j)\big|U_i^{1:j-1},\{U_k^{1:n}\}_{k\in[1:i-1]}\big)$ also polarize to 0 or 1.*

3.3.4 Rate of Polarization

The Bhattacharyya parameter of random variables is closely related to the conditional entropy. The parameter is useful for characterizing the rate of polarization.

Definition 7 (Bhattacharyya Parameter)**.** *Let $(T,V)\sim P_{T,V}$ where $T\in\{0,1\}$ and $V\in\mathcal{V}$ where $\mathcal{V}$ is an arbitrary discrete alphabet. The Bhattacharyya parameter $Z(T|V)\in[0,1]$ is defined*

$$Z(T|V)=2\sum_{v\in\mathcal{V}}P_V(v)\sqrt{P_{T|V}(0|v)P_{T|V}(1|v)}. \tag{3.11}$$

As shown in Lemma 9 of Appendix 3.5, $Z(T|V)\to 1$ implies $H(T|V)\to 1$, and similarly $Z(T|V)\to 0$ implies $H(T|V)\to 0$ for T a binary random variable. Based on the Bhattacharyya parameter, the following theorem specifies sets $\mathcal{M}_i^{(n)}\subset[n]$ that will be called *message* sets.

Proposition 3 (Rate of Polarization)**.** *Consider the pair of random matrices $(\mathbf{Y},\mathbf{U})$ related through the polar transformation in (3.5). Fix constants $0<\beta<\frac{1}{2}$, $\tau>0$, $i\in[m]$. Let $\delta_n=2^{-n^\beta}$ be the rate of polarization. Define the set*

$$\mathcal{M}_i^{(n)}\triangleq\left\{j\in[n]:Z\Big(U_i(j)\Big|U_i^{1:j-1},\{Y_k^{1:n}\}_{k\in[1:i-1]}\Big)\geq 1-\delta_n\right\}. \tag{3.12}$$

Then there exists an $N_o=N_o(\beta,\tau)$ such that

$$\frac{1}{n}\left|\mathcal{M}_i^{(n)}\right|\geq H(Y_i|Y_1Y_2\cdots Y_{i-1})-\tau, \tag{3.13}$$

for all $n>N_o$.

The proposition is established via the Martingale Convergence Theorem by defining a super-martingale with respect to the Bhattacharyya parameters [6] [7]. The rate of polarization is characterized by Arıkan and Telatar in [9].

Remark 6. *The message sets $\mathcal{M}_i^{(n)}$ are computed "offline" only once during a code construction phase. The sets do not depend on the realization of random variables. In the following Section 3.3.5, a Monte Carlo sampling approach for estimating Bhattacharyya parameters is reviewed. Other highly efficient algorithms are known in the literature for finding the message indices (see e.g. Tal and Vardy [88]).*

3.3.5 Estimating Bhattacharyya Parameters

As shown in Lemma 4 in Appendix 3.5, one way to estimate the Bhattacharyya parameter $Z(T|V)$ is to sample from the distribution $P_{T,V}(t,v)$ and evaluate $\mathbb{E}_{T,V}\sqrt{\varphi(T,V)}$. The function $\varphi(t,v)$ is defined based on likelihood ratios

$$L(v) \triangleq \frac{P_{T|V}(0|v)}{P_{T|V}(1|v)},$$
$$L^{-1}(v) \triangleq \frac{P_{T|V}(1|v)}{P_{T|V}(0|v)}.$$

Similarly, to determine the indices in the message sets $\mathcal{M}_i^{(n)}$ defined in Proposition 3, the Bhattacharyya parameters $Z\left(U_i(j)\middle|U_i^{1:j-1}, \{Y_k^{1:n}\}_{k\in[i-1]}\right)$ must be estimated efficiently. For $n \geq 2$, define the likelihood ratio

$$\begin{aligned} &L_n^{(i,j)}\left(u_i^{1:j-1}, \{y_k^{1:n}\}_{k\in[1:i-1]}\right) \\ &\quad\triangleq \frac{\mathbb{P}\left(U_i(j)=0\middle|U_i^{1:j-1}=u_i^{1:j-1}, \{Y_k^{1:n}=y_k^{1:n}\}_{k\in[1:i-1]}\right)}{\mathbb{P}\left(U_i(j)=1\middle|U_i^{1:j-1}=u_i^{1:j-1}, \{Y_k^{1:n}=y_k^{1:n}\}_{k\in[1:i-1]}\right)}. \end{aligned} \tag{3.14}$$

The dynamic programming method given in [7] allows for a recursive computation of the likelihood ratio. Define the following sub-problems

$$\Xi_1 = L_{\frac{n}{2}}^{(i,j)}\left(u_{i,o}^{1:2j-2} \oplus u_{i,e}^{1:2j-2}, \{y_k^{1:\frac{n}{2}}\}_{k\in[1:i-1]}\right),$$
$$\Xi_2 = L_{\frac{n}{2}}^{(i,j)}\left(u_{i,e}^{1:2j-2}, \{y_k^{\frac{n}{2}+1:n}\}_{k\in[1:i-1]}\right),$$

where the notation $u_{i,o}^{1:2j-2}$ and $u_{i,e}^{1:2j-2}$ represents the odd and even indices respectively of the sequence $u_i^{1:2j-2}$. The recursive computation of the likelihoods is characterized by

$$L_n^{(i,2j-1)}\left(u_i^{1:2j-2}, \{y_k^{1:n}\}_{k\in[1:i-1]}\right) = \frac{\Xi_1\Xi_2+1}{\Xi_1+\Xi_2}.$$
$$L_n^{(i,2j)}\left(u_i^{1:2j-1}, \{y_k^{1:n}\}_{k\in[1:i-1]}\right) = (\Xi_1)^{\gamma}\,\Xi_2,$$

where $\gamma = 1$ if $u_i(2j-1) = 0$ and $\gamma = -1$ if $u_i(2j-1) = 1$. In the above recursive computations, the base case is for sequences of length $n = 2$.

3.4 Proof Of Main Theorem

The proof of Theorem 2 is based on binary polarization theorems as discussed in Section 3.3. The random coding arguments of C. E. Shannon prove the existence of capacity-achieving codes for point-to-point channels. Furthermore, random binning and joint-typicality arguments suffice to prove the existence of capacity-achieving codes for the deterministic DM-BC. However, it is shown in this section that there exist capacity-achieving *polar codes* for the binary-output deterministic DM-BC.

3.4.1 Broadcast Code Based on Polarization

The ordering of the receivers' rates in $\vec{R}$ is arbitrary due to symmetry. Therefore, let $\pi(i) = i$ be the identity permutation which denotes the successive order in which the message bits are allocated for each receiver. The encoder must map m independent messages $(W_1, W_2, \ldots, W_m)$ uniformly distributed over $[2^{nR_1}] \times [2^{nR_2}] \times \cdots \times [2^{nR_m}]$ to a codeword $x^n \in \mathcal{X}^n$. To construct a codeword for broadcasting m independent messages, the following binary sequences are formed at the encoder: $u_1^{1:n}, u_2^{1:n}, \ldots, u_m^{1:n}$. To determine a particular bit $u_i(j)$ in the binary sequence $u_i^{1:n}$, if $j \in \mathcal{M}_i^{(n)}$, the bit is selected as a uniformly distributed message bit intended for receiver $i \in [m]$. As defined in (3.12) of Proposition 3, the message set $\mathcal{M}_i^{(n)}$ represents those indices for bits transmitted to receiver i. The remaining *non-message* indices in the binary sequence $u_i^{1:n}$ for each user $i \in [m]$ are computed either according to a deterministic or random mapping.

3.4.1.1 Deterministic Mapping

Consider a class of deterministic boolean functions indexed by $i \in [m]$ and $j \in [n]$:

$$\psi^{(i,j)} : \{0,1\}^{n(\max\{0,i-1\})+j-1} \to \{0,1\}. \tag{3.15}$$

As an example, consider the deterministic boolean function based on the *maximum a posteriori* polar coding rule.

$$\begin{aligned} &\psi_{MAP}^{(i,j)}\left(u_i^{1:j-1}, \{y_k^{1:n}\}_{k\in[1:i-1]}\right) \\ &\triangleq \arg\max_{u\in\{0,1\}} \left\{ \mathbb{P}\left(U_i(j) = u \middle| U_i^{1:j-1} = u_i^{1:j-1}, \{Y_k^{1:n} = y_k^{1:n}\}_{k\in[1:i-1]}\right) \right\}. \end{aligned} \tag{3.16}$$

3.4.1.2 Random Mapping

Consider a class of random boolean functions indexed by $i \in [m]$ and $j \in [n]$:

$$\Psi^{(i,j)} : \{0,1\}^{n(\max\{0,i-1\})+j-1} \to \{0,1\}. \tag{3.17}$$

As an example, consider the random boolean function

$$\Psi_{RAND}^{(i,j)}\left(u_i^{1:j-1}, \{y_k^{1:n}\}_{k\in[1:i-1]}\right) \triangleq \begin{cases} 0, & \text{w.p. } \lambda_0\left(u_i^{1:j-1}, \{y_k^{1:n}\}_{k\in[1:i-1]}\right), \\ 1, & \text{w.p. } 1-\lambda_0\left(u_i^{1:j-1}, \{y_k^{1:n}\}_{k\in[1:i-1]}\right), \end{cases} \tag{3.18}$$

where

$$\lambda_0\left(u_i^{1:j-1}, \{y_k^{1:n}\}_{k\in[1:i-1]}\right) \triangleq \mathbb{P}\left(U_i(j)=0 \middle| U_i^{1:j-1}=u_i^{1:j-1}, \{Y_k^{1:n}=y_k^{1:n}\}_{k\in[1:i-1]}\right).$$

The random boolean function $\Psi_{RAND}^{(i,j)}$ may be thought of as a vector of Bernoulli random variables indexed by the input to the function. Each Bernoulli random variable of the vector has a fixed probability of being one or zero that is well-defined.

3.4.1.3 Mapping From Messages To Codeword

The binary sequences $u_i^{1:n}$ for $i \in [m]$ are formed *successively* bit by bit. If $j \in \mathcal{M}_i^{(n)}$, then the bit $u_i(j)$ is one message bit from the uniformly distributed message W_i intended for user i. If $j \notin \mathcal{M}_i^{(n)}$, $u_i(j) = \psi_{MAP}^{(i,j)}\big(u_i^{1:j-1}, \{y_k^{1:n}\}_{k\in[1:i-1]}\big)$ in the case of a deterministic mapping, or $u_i(j) = \Psi_{RAND}^{(i,j)}\big(u_i^{1:j-1}, \{y_k^{1:n}\}_{k\in[1:i-1]}\big)$ in the case of a random mapping. The encoder then applies the *inverse* polar transform for each sequence: $y_i^{1:n} = u_i^{1:n}\mathbf{G}_n^{-1}$. The codeword x^n is formed symbol-by-symbol as follows:

$$x(j) \in \bigcap_{i=1}^{m} f_i^{-1}\left(y_i(j)\right).$$

If the intersection set is empty, the encoder declares a block error. A block error only occurs at the encoder.

3.4.1.4 Decoding at Receivers

If the encoder succeeds in transmitting a codeword x^n, each receiver obtains the sequence $y_i^{1:n}$ noiselessly and applies the polar transform $\mathbf{G}_n$ to recover $u_i^{1:n}$ exactly. Since the message indices $\mathcal{M}_i^{(n)}$ are known to each receiver, the message bits in $u_i^{1:n}$ are decoded correctly by receiver i.

3.4.2 Total Variation Bound

While the deterministic mapping $\psi_{MAP}^{(i,j)}$ performs well in practice, the average probability of error $P_e^{(n)}$ of the coding scheme is more difficult to analyze in theory. The random mapping $\Psi_{RAND}^{(i,j)}$ at the encoder is more amenable to analysis via the probabilistic method. Towards

that goal, consider the following probability measure defined on the space of tuples of binary sequences[2].

$$Q\Big(u_1^n, u_2^n, \cdots, u_m^n\Big) \triangleq \prod_{i=1}^{m}\prod_{j=1}^{n} Q\Big(u_i(j)\Big|u_i^{1:j-1}, \{u_k^{1:n}\}_{k\in[1:i-1]}\Big). \tag{3.19}$$

where the conditional probability measure

$$Q\left(u_i(j)\middle|u_i^{1:j-1}, \{u_k^{1:n}\}_{k\in[1:i-1]}\right) \triangleq \begin{cases} \frac{1}{2}, & \text{if } j \in \mathcal{M}_i^{(n)}, \\ P\left(u_i(j)\middle|u_i^{1:j-1}, \{u_k^{1:n}\}_{k\in[1:i-1]}\right), & \text{otherwise.} \end{cases}$$

The probability measure Q defined in (3.19) is a perturbation of the joint probability measure P defined in (3.8) for the random variables $U_i(j)$. The only difference in definition between P and Q is due to those indices in message set $\mathcal{M}_i^{(n)}$. The following lemma provides a bound on the total variation distance between P and Q.

Lemma 1. *(*Total Variation Bound*) Let probability measures P and Q be defined as in (3.8) and (3.19) respectively. Let $0 < \beta < 1$. For sufficiently large n, the total variation distance between P and Q is bounded as*

$$\sum_{\{u_k^{1:n}\}_{k\in[m]}} \Big|P\big(\{u_k^{1:n}\}_{k\in[m]}\big) - Q\big(\{u_k^{1:n}\}_{k\in[m]}\big)\Big| \leq 2^{-n^\beta}.$$

Proof. See Section 3.6 of the Appendices. □

3.4.3 Analysis of the Average Probability of Error

For the m-user deterministic DM-BC, an error event occurs at the encoder if a codeword x^n is unable to be constructed symbol by symbol according to the broadcast protocol described in Section 3.4.1. Define the following set consisting of m-tuples of binary sequences,

$$\mathcal{T} \triangleq \Big\{(y_1^n, y_2^n, \ldots, y_m^n) : \exists j \in [n], \bigcap_{i=1}^{m} f_i^{-1}\left(y_i(j)\right) = \emptyset\Big\}. \tag{3.20}$$

The set $\mathcal{T}$ consists of those m-tuples of binary output sequences which are *inconsistent* due to the properties of the deterministic channel. In addition, due to the one-to-one correspondence between sequences $u_i^{1:n}$ and $y_i^{1:n}$, denote by $\tilde{\mathcal{T}}$ the set of m-tuples $(u_1^n, u_2^n, \ldots, u_m^n)$ that are inconsistent.

[2]A related proof technique was provided for lossy source coding based on polarization in a different context [54]. In the present thesis, a different proof is supplied that utilizes the chain rule for KL-divergence.

For the broadcast protocol, the rate $R_i = \frac{1}{n}\left|\mathcal{M}_i^{(n)}\right|$ for each receiver. Let the total sum rate for all broadcast receivers be $R_\Sigma = \sum_{i\in[m]} R_i$. If the encoder uses a fixed deterministic map $\psi^{(i,j)}$ in the broadcast protocol, the average probability of error is

$$P_e^{(n)}\left[\{\psi^{(i,j)}\}\right] = \frac{1}{2^{nR_\Sigma}} \sum_{\{u_k^{1:n}\}_{k\in[m]}} \left[\mathbb{1}_{\left[(u_1^n, u_2^n, \ldots, u_m^n)\in\tilde{\mathcal{T}}\right]} \cdot \prod_{\substack{i\in[m] \\ j\in[n]: j\notin\mathcal{M}_i^{(n)}}} \mathbb{1}_{\left[\psi^{(i,j)}\left(u_i^{1:j-1}, \{y_k^{1:n}\}_{k\in[1:i-1]}\right) = u_i(j)\right]} \right]. \tag{3.21}$$

In addition, if the random maps $\Psi^{(i,j)}$ are used at the encoder, the average probability of error is a random quantity given by

$$P_e^{(n)}\left[\{\Psi^{(i,j)}\}\right] = \frac{1}{2^{nR_\Sigma}} \sum_{\{u_k^{1:n}\}_{k\in[m]}} \left[\mathbb{1}_{\left[(u_1^n, u_2^n, \ldots, u_m^n)\in\tilde{\mathcal{T}}\right]} \cdot \prod_{\substack{i\in[m] \\ j\in[n]: j\notin\mathcal{M}_i^{(n)}}} \mathbb{1}_{\left[\Psi^{(i,j)}\left(u_i^{1:j-1}, \{y_k^{1:n}\}_{k\in[1:i-1]}\right) = u_i(j)\right]} \right]. \tag{3.22}$$

Instead of characterizing $P_e^{(n)}$ directly for deterministic maps, the analysis of $P_e^{(n)}[\{\Psi^{(i,j)}\}]$ leads to the following lemma.

Lemma 2. *Consider the broadcast protocol of Section 3.4.1. Let $R_i = \frac{1}{n}\left|\mathcal{M}_i^{(n)}\right|$ for $i \in [m]$ be the broadcast rates selected according to the criterion given in (3.12) in Proposition 3. Then for $0 < \beta < 1$ and sufficiently large n,*

$$\mathbb{E}_{\{\Psi^{(i,j)}\}}\left[P_e^{(n)}[\{\Psi^{(i,j)}\}]\right] < 2^{-n^\beta}.$$

Proof.

$$
\begin{aligned}
&\mathbb{E}_{\{\Psi^{(i,j)}\}}\left[P_e^{(n)}[\{\Psi^{(i,j)}\}]\right] \\
&= \frac{1}{2^{nR_\Sigma}} \sum_{\{u_k^{1:n}\}_{k\in[m]}} \Bigg[\mathbb{1}_{\left[(u_1^n, u_2^n, \ldots, u_m^n)\in\tilde{\mathcal{T}}\right]} \cdot \\
&\quad \prod_{\substack{i\in[m] \\ j\in[n]: j\notin\mathcal{M}_i^{(n)}}} \mathbb{P}\left\{\Psi^{(i,j)}\left(u_i^{1:j-1}, \{y_k^{1:n}\}_{k\in[1:i-1]}\right) = u_i(j)\right\} \Bigg] \\
&= \sum_{\{u_k^{1:n}\}_{k\in[m]}\in\tilde{\mathcal{T}}} Q\left(\{u_k^{1:n}\}_{k\in[m]}\right) \qquad (3.23) \\
&= \sum_{\{u_k^{1:n}\}_{k\in[m]}\in\tilde{\mathcal{T}}} \left| P\left(\{u_k^{1:n}\}_{k\in[m]}\right) - Q\left(\{u_k^{1:n}\}_{k\in[m]}\right) \right| \qquad (3.24) \\
&\leq 2^{-n^\beta}. \qquad (3.25)
\end{aligned}
$$

Step (3.23) follows since the probability measure Q matches the desired calculation exactly. Step (3.24) is due to the fact that the probability measure P has *zero mass* over m-tuples of binary sequences that are inconsistent. Step (3.25) follows directly from Lemma 1. Lastly, since the expectation over random maps $\{\Psi^{(i,j)}\}$ of the average probability of error decays stretched-exponentially, there must exist a set of deterministic maps which exhibit the same behavior. □

3.5 Proof Of Lemmas

The following lemmas provide a basis for proving polar coding theorems. A subset of the lemmas were proven in different contexts, e.g., channel vs. source coding, and contain citations to references.

Lemma 3. *Consider two random variables $X \in \{0,1\}$ and $Y \in \mathcal{Y}$ with joint distribution $P_{X,Y}(x,y)$. Let $Q(x|y) = \frac{1}{2}$ denote a uniform conditional distribution for $x \in \{0,1\}$ and $y \in \mathcal{Y}$. Then the following identity holds.*

$$
D\left(P_{X|Y}(x|y) \middle\| Q(x|y)\right) = 1 - H(X|Y). \qquad (3.26)
$$

Proof. The identity follows from standard definitions of entropy and Kullback-Leibler dis-

tance.

$$\begin{aligned}
H(X|Y) &= \sum_{y\in\mathcal{Y}} P_Y(y) \sum_{x\in\{0,1\}} P_{X|Y}(x|y) \log_2 \frac{1}{P_{X|Y}(x|y)} \\
&= \sum_{y\in\mathcal{Y}} P_Y(y) \sum_{x\in\{0,1\}} P_{X|Y}(x|y) \log_2 \frac{1}{Q(x|y)} \\
&\quad - \sum_{y\in\mathcal{Y}} P_Y(y) \sum_{x\in\{0,1\}} P_{X|Y}(x|y) \log_2 \frac{P_{X|Y}(x|y)}{Q(x|y)} \\
&= \sum_{y\in\mathcal{Y}} P_Y(y) \left[1 - \sum_{x\in\{0,1\}} P_{X|Y}(x|y) \log_2 \frac{P_{X|Y}(x|y)}{Q(x|y)} \right] \\
&= 1 - D\left(P_{X|Y}(x|y) \middle\| Q(x|y) \right).
\end{aligned}$$

□

Lemma 4 (Estimating The Bhattacharyya Parameter)**.** *Let $(T, V) \sim P_{T,V}(t, v)$ where $T \in \{0, 1\}$ and $V \in \mathcal{V}$ where $\mathcal{V}$ is an arbitrary discrete alphabet. Define a likelihood function $L(v)$ and inverse likelihood function $L^{-1}(v)$ as follows.*

$$L(v) \triangleq \frac{P_{T|V}(0|v)}{P_{T|V}(1|v)}, \quad L^{-1}(v) \triangleq \frac{P_{T|V}(1|v)}{P_{T|V}(0|v)}$$

To account for degenerate cases in which $P_{T|V}(t|v) = 0$, define the following function,

$$\varphi(t, v) \triangleq \begin{cases} 0 & \text{if } \mathbb{1}_{\left[P_{T|V}(t|v)=0\right]} \\ L(v) & \text{if } \mathbb{1}_{\left[P_{T|V}(t|v)>0\right]} \text{ and } \mathbb{1}_{[t=1]} \\ L^{-1}(v) & \text{if } \mathbb{1}_{\left[P_{T|V}(t|v)>0\right]} \text{ and } \mathbb{1}_{[t=0]} \end{cases}$$

In order to estimate $Z(T|V) \in [0, 1]$, it is convenient to sample from $P_{TV}(t, v)$ and express $Z(T|V)$ as an expectation over random variables T and V,

$$Z(T|V) = \mathbb{E}_{T,V} \sqrt{\varphi(T, V)}. \tag{3.28}$$

Proof. The following forms of the Bhattacharyya parameter are equivalent.

$$\begin{aligned}
Z(T|V) &\triangleq 2\sum_{v\in\mathcal{V}} P_V(v)\sqrt{P_{T|V}(0|v)P_{T|V}(1|v)} \\
&= 2\sum_{v\in\mathcal{V}} \sqrt{P_{TV}(0,v)P_{TV}(1,v)} \\
&= \sum_{v\in\mathcal{V}} P_V(v) \sum_{t\in\{0,1\}} \sqrt{P_{T|V}(t|v)(1-P_{T|V}(t|v))} \\
&= \sum_{t\in\{0,1\}} \sum_{\substack{v:P_{T|V}(t|v)>0 \\ v\in\mathcal{V}}} P_{TV}(t,v)\sqrt{\frac{1-P_{T|V}(t|v)}{P_{T|V}(t|v)}} \\
&= \mathbb{E}_{T,V}\sqrt{\varphi(T,V)}.
\end{aligned}$$

□

Lemma 5 (Stochastic Degradation (cf. [55]))**.** *Consider discrete random variables V, Y_1, and Y_2. Assume that $|\mathcal{V}| = 2$ and that discrete alphabets $\mathcal{Y}_1$ and $\mathcal{Y}_2$ have an* arbitrary *size. Then*

$$P_{Y_1|V}(y_1|v) \succ P_{Y_2|V}(y_2|v) \Rightarrow Z(V|Y_2) \geq Z(V|Y_1). \tag{3.29}$$

Proof. Beginning with the definition of the Bhattacharyya parameter leads to the following derivation:

$$\begin{aligned}
&Z(V|Y_2) \\
&\triangleq 2\sum_{y_2} \sqrt{P_{VY_2}(0,y_2)P_{VY_2}(1,y_2)} \\
&= 2\sum_{y_2} \sqrt{P_V(0)P_V(1)}\sqrt{P_{Y_2|V}(y_2|0)P_{Y_2|V}(y_2|1)} \\
&= 2\sqrt{P_V(0)P_V(1)}\sum_{y_2}\left[\sqrt{\sum_{y_1} P_{Y_1|V}(y_1|0)\tilde{P}_{Y_2|Y_1}(y_2|y_1)}\cdot\sqrt{\sum_{y_1} P_{Y_1|V}(y_1|1)\tilde{P}_{Y_2|Y_1}(y_2|y_1)}\right].
\end{aligned}$$

Then applying the Cauchy–Schwarz inequality yields

$$\begin{aligned}
&Z(V|Y_2) \\
&\geq 2\sqrt{P_V(0)P_V(1)}\sum_{y_2}\left[\sum_{y_1}\sqrt{P_{Y_1|V}(y_1|0)\tilde{P}_{Y_2|Y_1}(y_2|y_1)}\cdot\sum_{y_1}\sqrt{P_{Y_1|V}(y_1|1)\tilde{P}_{Y_2|Y_1}(y_2|y_1)}\right] \\
&= 2\sqrt{P_V(0)P_V(1)}\sum_{y_2}\left[\sum_{y_1}\tilde{P}_{Y_2|Y_1}(y_2|y_1)\cdot\sqrt{P_{Y_1|V}(y_1|0)P_{Y_1|V}(y_1|1)}\right].
\end{aligned}$$

Interchanging the order of summations yields

$$\begin{aligned} Z(V|Y_2) &\geq 2\sqrt{P_V(0)P_V(1)}\left[\sum_{y_1}\sqrt{P_{Y_1|V}(y_1|0)P_{Y_1|V}(y_1|1)}\cdot\sum_{y_2}\tilde{P}_{Y_2|Y_1}(y_2|y_1)\right] \\ &= Z(V|Y_1). \end{aligned}$$

□

Lemma 6 (Successive Stochastic Degradation (cf. [55]))**.** *Consider a binary random variable V, and discrete random variables Y_1 with alphabet $\mathcal{Y}_1$, and Y_2 with alphabet $\mathcal{Y}_2$. Assume that the joint distribution $P_{VY_1Y_2}$ obeys the constraint $P_{Y_1|V}(y_1|v) \succ P_{Y_2|V}(y_2|v)$. Consider two i.i.d. random copies (V^1, Y_1^1, Y_2^1) and (V^2, Y_1^2, Y_2^2) distributed according to $P_{VY_1Y_2}$. Define two binary random variables $U^1 \triangleq V^1 \oplus V^2$ and $U^2 \triangleq V^2$. Then the following holds*

$$Z\left(U^1\middle|Y_2^{1:2}\right) \geq Z\left(U^1\middle|Y_1^{1:2}\right), \tag{3.30}$$

$$Z\left(U^2\middle|U^1, Y_2^{1:2}\right) \geq Z\left(U^2\middle|U^1, Y_1^{1:2}\right). \tag{3.31}$$

Proof. Given the assumptions, the following stochastic degradation conditions hold:

$$P_{Y_1^1|V^1}(y_1^1|v^1) \succ P_{Y_2^1|V^1}(y_2^1|v^1), \tag{3.32}$$

$$P_{Y_1^2|V^2}(y_1^2|v^2) \succ P_{Y_2^2|V^2}(y_2^2|v^2). \tag{3.33}$$

The goal is to derive new stochastic degradation conditions for the polarized conditional distributions. The binary random variables U^1 and U^2 are not necessarily independent Bernoulli($\frac{1}{2}$) variables. Taking this into account,

$$\begin{aligned} &P_{Y_2^1Y_2^2|U^1}\left(y_2^1, y_2^2\middle|u^1\right) \\ &= \frac{1}{P_{U^1}(u^1)}\sum_{u^2\in\{0,1\}} P_{V^1Y_2^1}\left(u^1\oplus u^2, y_2^1\right)P_{V^2Y_2^2}\left(u^2, y_2^2\right) \\ &= \frac{1}{P_{U^1}(u^1)}\sum_{u^2\in\{0,1\}}\left[P_{Y_2^1|V^1}\left(y_2^1\middle|u^1\oplus u^2\right)P_{V^1}\left(u^1\oplus u^2\right)\cdot P_{Y_2^2|V^2}\left(y_2^2\middle|u^2\right)P_{V^2}(u^2)\right]. \end{aligned}$$

Applying the property due to the assumption in (3.32),

$$\begin{aligned} P_{Y_2^1Y_2^2|U^1}\left(y_2^1, y_2^2\middle|u^1\right) = \frac{1}{P_{U^1}(u^1)}\sum_{u^2\in\{0,1\}}\Bigg[&P_{V^1}\left(u^1\oplus u^2\right)P_{V^2}(u^2) \\ &\cdot\sum_{a\in\mathcal{Y}_1} P_{Y_1^1|V^1}\left(a\middle|u^1\oplus u^2\right)\tilde{P}_{Y_2^1|Y_1^1}\left(y_2^1\middle|a\right) \\ &\cdot\sum_{b\in\mathcal{Y}_1} P_{Y_1^2|V^2}\left(b\middle|u^2\right)\tilde{P}_{Y_2^2|Y_1^2}\left(y_2^2\middle|b\right)\Bigg]. \end{aligned}$$

Interchanging the order of summations and grouping terms involving $P_{Y_1^1Y_1^2|U^1}\big(y_1^1, y_1^2\big|u^1\big)$ yields the following

$$P_{Y_2^1Y_2^2|U^1}\big(y_2^1, y_2^2\big|u^1\big) = \sum_{a\in\mathcal{Y}_1, b\in\mathcal{Y}_1} P_{Y_1^1Y_1^2|U^1}\big(a, b\big|u^1\big)\tilde{P}_{Y_2^1|Y_1^1}\big(y_2^1\big|a\big)\tilde{P}_{Y_2^2|Y_1^2}\big(y_2^2\big|b\big).$$

The above derivation proves that

$$P_{Y_1^1Y_1^2|U^1}\big(y_1^1, y_1^2\big|u^1\big) \succ P_{Y_2^1Y_2^2|U^1}\big(y_2^1, y_2^2\big|u^1\big).$$

Combined with Lemma 5, this concludes the proof for the ordering of the Bhattacharyya parameters given in (3.30).

In a similar way, it is possible to show that

$$\begin{aligned}
&P_{Y_2^1Y_2^2U^1|U^2}\big(y_2^1, y_2^2, u^1\big|u^2\big)\\
&\quad= \frac{1}{P_{U^2}(u^2)}P_{V^1Y_2^1}\big(u^1\oplus u^2, y_2^1\big)P_{V^2Y_2^2}\big(u^2, y_2^2\big)\\
&\quad= \frac{1}{P_{U^2}(u^2)}\Big[P_{Y_2^1|V^1}\big(y_2^1\big|u^1\oplus u^2\big)P_{V^1}\big(u^1\oplus u^2\big)\cdot P_{Y_2^2|V^2}\big(y_2^2\big|u^2\big)P_{V^2}(u^2)\Big].
\end{aligned}$$

Applying the property due to the assumption in (3.33),

$$\begin{aligned}
P_{Y_2^1Y_2^2U^1|U^2}\big(y_2^1, y_2^2, u^1\big|u^2\big) = \frac{1}{P_{U^2}(u^2)}\Big[&P_{V^1}\big(u^1\oplus u^2\big)P_{V^2}(u^2)\\
&\cdot\sum_{a\in\mathcal{Y}_1}P_{Y_1^1|V^1}\big(a\big|u^1\oplus u^2\big)\tilde{P}_{Y_2^1|Y_1^1}\big(y_2^1\big|a\big)\\
&\cdot\sum_{b\in\mathcal{Y}_1}P_{Y_1^2|V^2}\big(b\big|u^2\big)\tilde{P}_{Y_2^2|Y_1^2}\big(y_2^2\big|b\big)\Big].
\end{aligned}$$

Interchanging the order of the terms and grouping terms involving $P_{Y_1^1Y_1^2U^1|U^2}\big(y_1^1, y_1^2, u^1\big|u^2\big)$ yields the following

$$\begin{aligned}
&P_{Y_2^1Y_2^2U^1|U^2}\big(y_2^1, y_2^2, u^1\big|u^2\big)\\
&\quad= \sum_{a\in\mathcal{Y}_1, b\in\mathcal{Y}_1}\Big[P_{Y_1^1Y_1^2U^1|U^2}\big(a, b, u^1\big|u^2\big)\tilde{P}_{Y_2^1|Y_1^1}\big(y_2^1\big|a\big)\tilde{P}_{Y_2^2|Y_1^2}\big(y_2^2\big|b\big)\Big],\\
&\quad= \sum_{a\in\mathcal{Y}_1, b\in\mathcal{Y}_1, c\in\{0,1\}}\Big[P_{Y_1^1Y_1^2U^1|U^2}\big(a, b, c\big|u^2\big)\tilde{P}_{Y_2^1|Y_1^1}\big(y_2^1\big|a\big)\tilde{P}_{Y_2^2|Y_1^2}\big(y_2^2\big|b\big)\mathbb{1}_{[u^1=c]}\Big].
\end{aligned}$$

The above derivation proves that

$$P_{Y_1^1Y_1^2U^1|U^2}\big(y_1^1, y_1^2, u^1\big|u^2\big) \succ P_{Y_2^1Y_2^2U^1|U^2}\big(y_2^1, y_2^2, u^1\big|u^2\big).$$

Combined with Lemma 5, this concludes the proof for the ordering of the Bhattacharyya parameters given in (3.31). □

Lemma 7 (Pinsker's Inequality)**.** *Consider two discrete probability measures $P(y)$ and $Q(y)$ for $y \in \mathcal{Y}$. The following inequality holds for a constant $\kappa \triangleq 2\ln 2$.*

$$\sum_{y\in\mathcal{Y}}\Big|P(y)-Q(y)\Big| \leq \sqrt{\kappa D\left(P(y)\big\|Q(y)\right)}.$$

Lemma 8 (Arıkan [7])**.** *Consider two discrete random variables $X \in \{0,1\}$ and $Y \in \mathcal{Y}$. The Bhattacharyya parameter and conditional entropy are related as follows.*

$$\begin{aligned} Z(X|Y)^2 &\leq H(X|Y) \\ H(X|Y) &\leq \log_2(1+Z(X|Y)) \end{aligned}$$

Lemma 9 (Bhattacharyya vs. Entropy Parameters)**.** *Consider two discrete random variables $X \in \{0,1\}$ and $Y \in \mathcal{Y}$. For any $0 < \delta < \frac{1}{2}$,*

$$\begin{aligned} Z(X|Y) \geq 1-\delta &\Rightarrow H(X|Y) \geq 1-2\delta. \\ Z(X|Y) \leq \delta &\Rightarrow H(X|Y) \leq \log_2(1+\delta). \end{aligned}$$

Proof. Due to Lemma 8, $H(X|Y) \geq Z(X|Y)^2 \geq (1-\delta)^2 \geq 1-2\delta+\delta^2 \geq 1-2\delta$. It follows that if $Z(X|Y) \geq 1-\delta$ and $\delta \to 0$, then $H(X|Y) \to 1$ as well. Similarly, due to Lemma 8, taking constant $\kappa = \frac{1}{\log_e 2}$ and using the series expansion of $\log_e(1+\delta)$, if $Z(X|Y) \leq \delta$ then $H(X|Y) \leq \log_2(1+\delta) = \kappa\left(\sum_{k=1}^{\infty}(-1)^{k+1}\frac{\delta^k}{k}\right) \leq \kappa\delta$. It follows that if $Z(X|Y) \leq \delta$ and $\delta \to 0$, then $H(X|Y) \to 0$ as well. □

3.6 Proof of Total Variation Bound

The total variation bound of Lemma 1 is decomposed in a simple way due to the chain rule for Kullback-Leibler distance between discrete probability measures. The joint probability measures P and Q were defined in (3.8) and (3.19) respectively. According to definition, if $P\big(\{u_i^{1:n}\}_{i\in[m]}\big) > 0$ then $Q\big(\{u_i^{1:n}\}_{i\in[m]}\big) > 0$. Therefore the Kullback-Leibler distance $D(P\|Q)$ is well-defined and upper bounded as follows.

$$
\begin{aligned}
&D\Big(P\big(\{u_i^{1:n}\}_{i\in[m]}\big)\Big\|Q\big(\{u_i^{1:n}\}_{i\in[m]}\big)\Big)\\
&=\sum_{i=1}^{m}\sum_{j=1}^{n}\left[D\Big(P\left(u_i(j)\Big|u_i^{1:j-1},\{u_k^{1:n}\}_{k\in[1:i-1]}\right)\Big\|Q\left(u_i(j)\Big|u_i^{1:j-1},\{u_k^{1:n}\}_{k\in[1:i-1]}\right)\Big)\right] &(3.34)\\
&=\sum_{i=1}^{m}\sum_{j\in\mathcal{M}_i^{(n)}}\left[D\Big(P\left(u_i(j)\Big|u_i^{1:j-1},\{u_k^{1:n}\}_{k\in[1:i-1]}\right)\Big\|Q\left(u_i(j)\Big|u_i^{1:j-1},\{u_k^{1:n}\}_{k\in[1:i-1]}\right)\Big)\right] &(3.35)\\
&=\sum_{i=1}^{m}\sum_{j\in\mathcal{M}_i^{(n)}}1-H\left(U_i(j)\Big|U_i^{1:j-1},\{U_k^{1:n}\}_{k\in[1:i-1]}\right) &(3.36)\\
&=\sum_{i=1}^{m}\sum_{j\in\mathcal{M}_i^{(n)}}1-H\left(U_i(j)\Big|U_i^{1:j-1},\{Y_k^{1:n}\}_{k\in[1:i-1]}\right) &(3.37)\\
&\leq\sum_{i=1}^{m}2\delta_n\left|\mathcal{M}_i^{(n)}\right|. &(3.38)
\end{aligned}
$$

The equality in (3.34) is due to the chain rule for Kullback-Leibler distance. The equality in (3.35) is valid because for indices $j\notin\mathcal{M}_i^{(n)}$,

$$P\left(u_i(j)\Big|u_i^{1:j-1},\{u_k^{1:n}\}_{k\in[1:i-1]}\right)=Q\left(u_i(j)\Big|u_i^{1:j-1},\{u_k^{1:n}\}_{k\in[1:i-1]}\right).$$

The equality in (3.36) is valid due to Lemma 3 and the fact that

$$Q\left(u_i(j)\Big|u_i^{1:j-1},\{u_k^{1:n}\}_{k\in[1:i-1]}\right)=\frac{1}{2},$$

for indices $j\in\mathcal{M}_i^{(n)}$. The equality in (3.37) follows due to the one-to-one correspondence between variables $\{U_k^{1:n}\}_{k\in[1:i-1]}$ and $\{Y_k^{1:n}\}_{k\in[1:i-1]}$. The last inequality (3.38) follows from Lemma 9 due to the fact that $Z\left(U_i(j)\Big|U_i^{1:j-1},\{Y_k^{1:n}\}_{k\in[1:i-1]}\right)\geq 1-\delta_n$ for indices $j\in\mathcal{M}_i^{(n)}$.

To finish the proof of Lemma 1,

$$
\begin{aligned}
&\sum_{\{u_k^{1:n}\}_{k\in[m]}}\left|P\big(\{u_k^{1:n}\}_{k\in[m]}\big)-Q\big(\{u_k^{1:n}\}_{k\in[m]}\big)\right|\\
&\qquad\leq\sqrt{\kappa D\left(P\left(\{u_k^{1:n}\}_{k\in[m]}\right)\Big\|Q\left(\{u_k^{1:n}\}_{k\in[m]}\right)\right)} &(3.39)\\
&\qquad\leq\sqrt{\kappa\sum_{i=1}^{m}2\delta_n\left|\mathcal{M}_i^{(n)}\right|} &(3.40)\\
&\qquad\leq\sqrt{(2\kappa)(m\cdot n)(2^{-n^{\beta'}})}.
\end{aligned}
$$

The inequality in (3.39) is due to Pinsker's inequality given in Lemma 7. The inequality in (3.40) was proven in (3.38). Finally for $\beta' \in (\beta, \frac{1}{2})$,

$$\sqrt{(2\kappa)(m \cdot n)(2^{-n^{\beta'}})} < 2^{-n^{\beta}}$$

for sufficiently large n. Hence the total variation distance is bounded by $\mathcal{O}(2^{-n^{\beta}})$ for any $0 < \beta < \frac{1}{2}$.

Chapter 4

Superposition Coding

4.1 Classes of Broadcast Channels

Coding for noisy broadcast channels is now considered using polarization methods. By contrast to the deterministic case, a decoding error event occurs at the receivers on account of the randomness due to noise. For the remaining sections, it is assumed that there exist $m = 2$ users in the DM-BC. The private-message capacity region for the DM-BC is unknown even for binary input, binary output two-user channels such as the skew-symmetric DM-BC. However, the private-message capacity region is known for specific classes.

4.1.1 Special Classes of Noisy DM-BCs

Definition 8. *The two-user* physically degraded *DM-BC is a channel $P_{Y_1Y_2|X}(y_1, y_2|x)$ for which $X - Y_1 - Y_2$ form a Markov chain, i.e. one of the receivers is statistically stronger than the other:*

$$P_{Y_1Y_2|X}(y_1, y_2|x) = P_{Y_1|X}(y_1|x)P_{Y_2|Y_1}(y_2|y_1). \tag{4.1}$$

Definition 9. *A two-user DM-BC $P_{Y_1Y_2|X}(y_1, y_2|x)$ is* stochastically degraded *if its conditional marginal distributions are the same as that of a physically degraded DM-BC, i.e., if there exists a distribution $\tilde{P}_{Y_2|Y_1}(y_2|y_1)$ such that*

$$P_{Y_2|X}(y_2|x) = \sum_{y_1 \in \mathcal{Y}_1} P_{Y_1|X}(y_1|x)\tilde{P}_{Y_2|Y_1}(y_2|y_1). \tag{4.2}$$

If (4.2) holds for two conditional distributions $P_{Y_1|X}(y_1|x)$ and $P_{Y_2|X}(y_2|x)$ defined over the same input, then the property is denoted as follows: $P_{Y_1|X}(y_1|x) \succ P_{Y_2|X}(y_2|x)$.

Definition 10. *A two-user DM-BC $P_{Y_1Y_2|X}(y_1, y_2|x)$ for which $V - X - (Y_1, Y_2)$ forms a Markov chain is said to be* less noisy *if*

$$\forall P_{VX}(v, x) : I(V; Y_1) \geq I(V; Y_2). \tag{4.3}$$

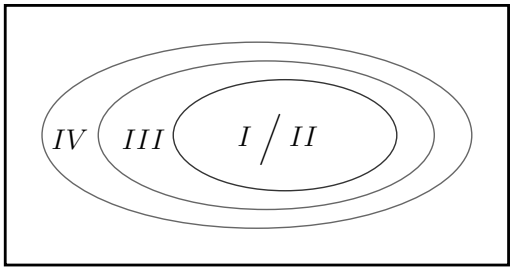


Figure 4.1: Class hierarchy of special broadcast channels: Class I/II stochastically-degraded channels; Class III "less-noisy" channels; Class IV "more capable" channels.

Definition 11. *A two-user DM-BC $P_{Y_1Y_2|X}(y_1, y_2|x)$ is said to be* more capable *if*

$$\forall P_X(x) : I(X;Y_1) \geq I(X;Y_2). \tag{4.4}$$

The following lemma relates the properties of the special classes of noisy broadcast channels. A more comprehensive treatment of special classes is given by C. Nair in [65].

Lemma 10. *Consider a two-user DM-BC $P_{Y_1Y_2|X}(y_1, y_2|x)$. Let $V - X - (Y_1, Y_2)$ form a Markov chain, $|\mathcal{V}| > 1$, and $P_V(v) > 0$. The following implications hold:*

$$\begin{aligned} & X - Y_1 - Y_2 \\ & \quad \Rightarrow P_{Y_1|X}(y_1|x) \succ P_{Y_2|X}(y_2|x) && (4.5) \\ & \quad \Leftrightarrow \forall P_{X|V}(x|v) : P_{Y_1|V}(y_1|v) \succ P_{Y_2|V}(y_2|v) && (4.6) \\ & \quad \Rightarrow \forall P_{VX}(v,x) : I(V;Y_1) \geq I(V;Y_2) && (4.7) \\ & \quad \Rightarrow \forall P_X(x) : I(X;Y_1) \geq I(X;Y_2). && (4.8) \end{aligned}$$

The converse statements for (4.5), (4.7), and (4.8) do not *hold in general. Figure 4.1 illustrates the different types of broadcast channels as a hierarchy. Class II represents broadcast channels for which $V - X - (Y_1, Y_2)$ and $P_{Y_2|V}(y_2|v) \succ P_{Y_1|V}(y_1|v)$ for all $P_{X|V}(x|v)$. Class II is equivalent to Class I which represents stochastically-degraded broadcast channels. Class III represents "less-noisy" channels, and Class IV "more capable" channels.*

Proof. See Section 4.5 of the Appendices. □

4.2 Cover's Inner Bound

Superposition coding involves one auxiliary random variable V which conveys a "cloud center" or a coarse message decoded by both receivers [22]. One of the receivers then decodes an additional "satellite codeword" conveyed through X containing a fine-grain message that is superimposed upon the coarse information.

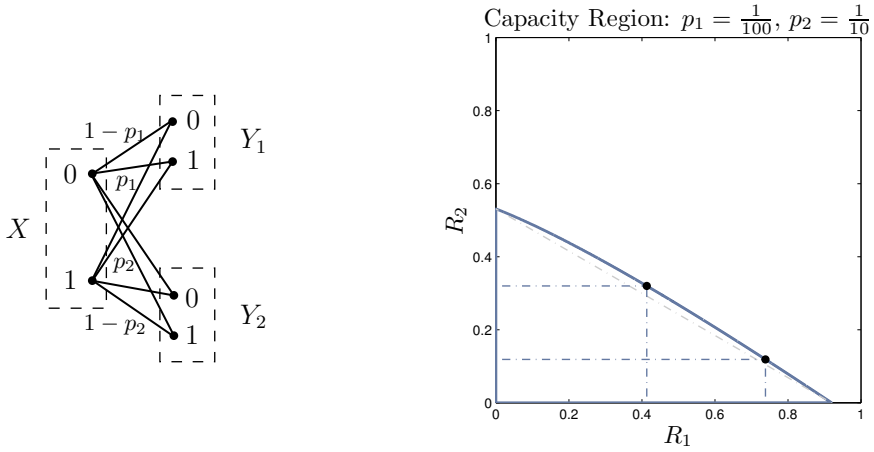


Figure 4.2: The superposition coding inner bound and capacity region of a two-user broadcast channel comprised of a BSC(p_1) and a BSC(p_2).

Proposition 4 (Cover's Inner Bound)**.** *For any two-user DM-BC, the rates* $(R_1, R_2) \in \mathbb{R}_+^2$ *are achievable in the region* $\mathfrak{R}(X, V, Y_1, Y_2)$ *where*

$$\mathfrak{R}(X,V,Y_1,Y_2) \triangleq \Big\{ R_1, R_2 \;\Big|\; \begin{aligned} R_1 &\le I(X;Y_1|V), \\ R_2 &\le I(V;Y_2), \\ R_1 + R_2 &\le I(X;Y_1) \end{aligned} \Big\}. \tag{4.9}$$

and where random variables X, V, Y_1, Y_2 *obey the Markov chain* $V - X - (Y_1, Y_2)$.

Remark 7. *Cover's inner bound is applicable for* any *broadcast channel. By symmetry, the following rate region is also achievable:* $\{R_1, R_2 \mid R_2 \le I(X;Y_2|V), R_1 \le I(V;Y_1), R_1 + R_2 \le I(X;Y_2)\}$ *for random variables obeying the Markov chain* $V - X - (Y_1, Y_2)$.

Remark 8. *The inner bound is the capacity region for degraded, less-noisy, and more-capable DM-BCs (i.e. Class I through Class IV as shown in Figure 4.1). For the degraded and less-noisy special classes, the capacity region is simplified to* $\{R_1, R_2 \mid R_1 \le I(X;Y_1|V), R_2 \le I(V;Y_2)\}$. *To see this, note that* $I(V;Y_2) \le I(V;Y_1)$ *which implies* $I(V;Y_2) + I(X;Y_1|V) \le I(V;Y_1) + I(X;Y_1|V) = I(X;Y_1)$. *Therefore the sum-rate constraint* $R_1 + R_2 \le I(X;Y_1)$ *of the rate-region in (4.9) is automatically satisfied.*

Example 4 (Binary Symmetric DM-BC)**.** *The two-user binary symmetric DM-BC consists of a binary symmetric channel with flip probability* p_1 *denoted as* BSC(p_1) *and a second channel* BSC(p_2). *Assume that* $p_1 < p_2 < \frac{1}{2}$ *which implies stochastic degradation as defined in (4.2). For* $\alpha \in [0, \frac{1}{2}]$, *Cover's superposition inner bound is the region,*

$$\Big\{ R_1, R_2 \;\Big|\; \begin{aligned} R_1 &\le h_b(\alpha * p_1) - h_b(p_1), \\ R_2 &\le 1 - h_b(\alpha * p_2) \end{aligned} \Big\} \tag{4.10}$$

The above inner bound is determined by evaluating (4.9) where V is a Bernoulli random variable with $P_V(v) = \frac{1}{2}$, $X = V \oplus S$, and S is a Bernoulli random variable with $P_S(1) = \alpha$. For a fixed auxiliary and input distribution $P_{VX}(v, x)$, the superposition inner bound is plotted as a rectangle in $\mathbb{R}_+^2$ for $\alpha = \frac{1}{10}$ and $\alpha = \frac{1}{4}$ in Figure 4.2. The corner points of this rectangle given in (4.10) lie on the capacity boundary. For this example, polar codes achieve all points on the capacity boundary.

Example 5 (DM-BC with BEC(ϵ) and BSC(p)[65])**.** *Consider a two-user DM-BC comprised of a* BSC*(p) from X to Y_1 and a* BEC*(ϵ) from X to Y_2. Then it can be shown that the following cases hold:*

- $0 < \epsilon \leq 2p$*: Y_1 is degraded with respect to Y_2.*
- $2p < \epsilon \leq 4p(1-p)$*: Y_2 is less noisy than Y_1 but Y_1 is not degraded with respect to Y_2.*
- $4p(1-p) < \epsilon \leq h_b(p)$*: Y_2 is more capable than Y_1 but not less noisy.*
- $h_b(p) < \epsilon < 1$*: The channel does not belong to the special classes.*

The capacity region for all channel parameters for this example is achieved using superposition coding.

4.3 Polar Coding Theorem

Theorem 3 (Polarization-Based Superposition Code)**.** *Consider any two-user DM-BC with binary input alphabet $\mathcal{X} = \{0, 1\}$ and arbitrary output alphabets $\mathcal{Y}_1$, $\mathcal{Y}_2$. There exists a sequence of polar broadcast codes over n channel uses which achieves the following rate region*

$$\mathfrak{R}(V, X, Y_1, Y_2) \triangleq \Big\{ R_1, R_2 \;\Big|\; R_1 \leq I(X; Y_1|V), \\ R_2 \leq I(V; Y_2) \Big\}, \tag{4.11}$$

where random variables V, X, Y_1, Y_2 have the following listed properties:

- *V is a binary random variable.*
- *$P_{Y_1|V}(y_1|v) \succ P_{Y_2|V}(y_2|v)$.*
- *$V - X - (Y_1, Y_2)$ form a Markov chain.*

For $0 < \beta < \frac{1}{2}$, the average error probability of this code sequence decays as $P_e^{(n)} = \mathcal{O}(2^{-n^\beta})$. The complexity of encoding and decoding is $\mathcal{O}(n \log n)$.

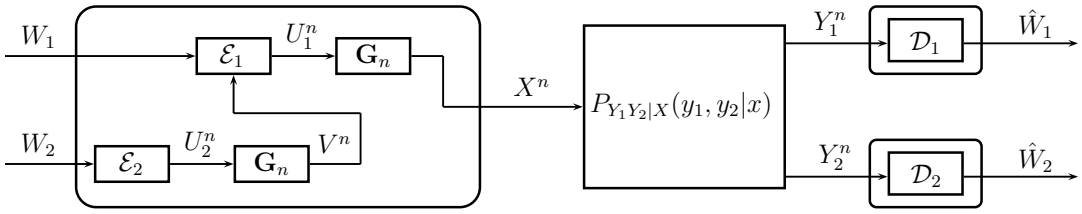


Figure 4.3: Block diagram of a polar code based on Cover's superposition coding.

Remark 9. *The requirement that auxiliary V is a binary random variable is due to the use of binary polarization theorems in the proof. Indeed, the auxiliary V may need to have a larger alphabet in the case of broadcast channels. An extension to q-ary random variables is entirely possible if q-ary polarization theorems are utilized.*

Remark 10. *The requirement that $V - X - (Y_1, Y_2)$ holds is standard for superposition coding over noisy channels. However, the listed property $P_{Y_1|V}(y_1|v) \succ P_{Y_2|V}(y_2|v)$ is due to the structure of polarization and is used in the proof to guarantee that polarization indices are* aligned. *If both receivers are able to decode the coarse message carried by the auxiliary random variable V, the polarization indices for the coarse message must be nested for the two receivers' channels.*

4.4 Proof of Main Theorem

To prove Theorem 3, consider the block diagram for polarization-based superposition coding given in Figure 4.3. Similar to random codes in Shannon theory, polarization-based codes rely on n-length $i.i.d.$ statistics of random variables; however, a specific polarization structure based on the chain rule of entropy allows for efficient encoding and decoding. The key idea of Cover's inner bound is to superimpose two messages of information onto one codeword.

4.4.1 Polar Transform

Consider the $i.i.d.$ sequence of random variables

$$(V^j, X^j, Y_1^j, Y_2^j) \sim P_V(v)P_{X|V}(x|v)P_{Y_1Y_2|X}(y_1, y_2|x),$$

where the index $j \in [n]$. Let the n-length sequence of auxiliary and input variables (V^j, X^j) be organized into the random matrix

$$\mathbf{\Omega} \triangleq \begin{bmatrix} X^1 & X^2 & X^3 & \dots & X^n \\ V^1 & V^2 & V^3 & \dots & V^n \end{bmatrix}. \tag{4.12}$$

Applying the polar transform to $\mathbf{\Omega}$ results in the random matrix $\mathbf{U} \triangleq \mathbf{\Omega}\mathbf{G}_n$. Let the random variables in the random matrix $\mathbf{U}$ be indexed as follows:

$$\mathbf{U} = \begin{bmatrix} U_1^1 & U_1^2 & U_1^3 & \dots & U_1^n \\ U_2^1 & U_2^2 & U_2^3 & \dots & U_2^n \end{bmatrix}. \tag{4.13}$$

The above definitions are consistent with the block diagram given in Figure 4.3 (and noting that $\mathbf{G}_n = \mathbf{G}_n^{-1}$). The polar transform extracts the randomness of $\mathbf{\Omega}$. In the transformed domain, the joint distribution of the random variables in $\mathbf{U}$ is given by

$$P_{U_1^n U_2^n}\left(u_1^n, u_2^n\right) \triangleq P_{X^n V^n}\left(u_1^n \mathbf{G}_n, u_2^n \mathbf{G}_n\right). \tag{4.14}$$

For polar coding purposes, the joint distribution is decomposed as follows,

$$P_{U_1^n U_2^n}\left(u_1^n, u_2^n\right) = P_{U_2^n}(u_2^n) P_{U_1^n|U_2^n}\left(u_1^n \middle| u_2^n\right) = \prod_{j=1}^{n} P\left(u_2(j) \middle| u_2^{1:j-1}\right) P\left(u_1(j) \middle| u_1^{1:j-1}, u_2^n\right). \tag{4.15}$$

The conditional distributions may be computed efficiently using recursive protocols as already mentioned. The polarized variables in $\mathbf{U}$ are *not i.i.d.* random variables.

4.4.2 Polarization Theorems Revisited

Definition 12 (Polarization Sets for Superposition Coding)**.** *Let V^n, X^n, Y_1^n, Y_2^n be the sequence of random variables as introduced in Section 4.4.1. In addition, let $U_1^n = X^n \mathbf{G}_n$ and $U_2^n = V^n \mathbf{G}_n$. Let $\delta_n = 2^{-n^\beta}$ for $0 < \beta < \frac{1}{2}$. The following* polarization sets *are defined:*

$$\begin{aligned}
\mathcal{H}_{X|V}^{(n)} &\triangleq \left\{ j \in [n] : Z\left(U_1(j) \middle| U_1^{1:j-1}, V^n\right) \geq 1 - \delta_n \right\}, \\
\mathcal{L}_{X|VY_1}^{(n)} &\triangleq \left\{ j \in [n] : Z\left(U_1(j) \middle| U_1^{1:j-1}, V^n, Y_1^n\right) \leq \delta_n \right\}, \\
\mathcal{L}_{V|Y_1}^{(n)} &\triangleq \left\{ j \in [n] : Z\left(U_2(j) \middle| U_2^{1:j-1}, Y_1^n\right) \leq \delta_n \right\}. \\
\mathcal{H}_{V}^{(n)} &\triangleq \left\{ j \in [n] : Z\left(U_2(j) \middle| U_2^{1:j-1}\right) \geq 1 - \delta_n \right\}, \\
\mathcal{L}_{V|Y_2}^{(n)} &\triangleq \left\{ j \in [n] : Z\left(U_2(j) \middle| U_2^{1:j-1}, Y_2^n\right) \leq \delta_n \right\}.
\end{aligned}$$

Definition 13 (Message Sets for Superposition Coding)**.** *In terms of the polarization sets given in Definition 12, the following* message sets *are defined:*

$$\mathcal{M}_{1v}^{(n)} \triangleq \mathcal{H}_{V}^{(n)} \cap \mathcal{L}_{V|Y_1}^{(n)}, \tag{4.16}$$

$$\mathcal{M}_{1}^{(n)} \triangleq \mathcal{H}_{X|V}^{(n)} \cap \mathcal{L}_{X|VY_1}^{(n)}. \tag{4.17}$$

$$\mathcal{M}_{2}^{(n)} \triangleq \mathcal{H}_{V}^{(n)} \cap \mathcal{L}_{V|Y_2}^{(n)}. \tag{4.18}$$

Proposition 5 (Polarization)**.** *Consider the polarization sets given in Definition 12 and the message sets given in Definition 13 with parameter $\delta_n = 2^{-n^\beta}$ for $0 < \beta < \frac{1}{2}$. Fix a constant $\tau > 0$. Then there exists an $N_o = N_o(\beta, \tau)$ such that*

$$\frac{1}{n}\left|\mathcal{M}_1^{(n)}\right| \geq \Big(H(X|V) - H(X|V, Y_1)\Big) - \tau, \tag{4.19}$$

$$\frac{1}{n}\left|\mathcal{M}_2^{(n)}\right| \geq \Big(H(V) - H(V|Y_2)\Big) - \tau, \tag{4.20}$$

for all $n > N_o$.

Lemma 11. *Consider the message sets defined in Definition 13. If the property $P_{Y_1|V}(y_1|v) \succ P_{Y_2|V}(y_2|v)$ holds for conditional distributions $P_{Y_1|V}(y_1|v)$ and $P_{Y_2|V}(y_2|v)$, then the Bhattacharyya parameters*

$$Z\left(U_2(j)\middle|U_2^{1:j-1}, Y_1^n\right) \leq Z\left(U_2(j)\middle|U_2^{1:j-1}, Y_2^n\right)$$

for all $j \in [n]$. As a result,

$$\mathcal{M}_2^{(n)} \subseteq \mathcal{M}_{1v}^{(n)}.$$

Proof. The proof follows from Lemma 5 and repeated application of Lemma 6 in Appendix 3.5. □

4.4.3 Broadcast Encoding Blocks: $(\mathcal{E}_1, \mathcal{E}_2)$

The polarization theorems of the previous section are useful for defining a multi-user communication system as diagrammed in Figure 4.3. The broadcast encoder must map two independent messages (W_1, W_2) uniformly distributed over $[2^{nR_1}] \times [2^{nR_2}]$ to a codeword $x^n \in \mathcal{X}^n$ in such a way that the decoding at each separate receiver is successful. The achievable rates for a particular block length n are

$$R_1 = \frac{1}{n}\left|\mathcal{M}_1^{(n)}\right|,$$
$$R_2 = \frac{1}{n}\left|\mathcal{M}_2^{(n)}\right|.$$

To construct a codeword, the encoder first produces two binary sequences $u_1^n \in \{0,1\}^n$ and $u_2^n \in \{0,1\}^n$. To determine $u_1(j)$ for $j \in \mathcal{M}_1^{(n)}$, the bit is selected as a uniformly distributed message bit intended for the first receiver. To determine $u_2(j)$ for $j \in \mathcal{M}_2^{(n)}$, the bit is selected as a uniformly distributed message bit intended for the second receiver. The remaining *non-message* indices of u_1^n and u_2^n are computed according to deterministic or random functions which are *shared* between the encoder and decoder.

4.4.3.1 Deterministic Mapping

Consider the following deterministic boolean functions indexed by $j \in [n]$:

$$\psi_1^{(j)} : \{0,1\}^{n+j-1} \to \{0,1\}, \tag{4.21}$$

$$\psi_2^{(j)} : \{0,1\}^{j-1} \to \{0,1\}. \tag{4.22}$$

As an example, consider the deterministic boolean functions based on the *maximum a posteriori* polar coding rule.

$$\psi_1^{(j)}\left(u_1^{1:j-1}, v^n\right) \triangleq \arg\max_{u\in\{0,1\}} \left\{ \mathbb{P}\left(U_1(j) = u \middle| U_1^{1:j-1} = u_1^{1:j-1}, V^n = v^n\right) \right\}. \tag{4.23}$$

$$\psi_2^{(j)}\left(u_2^{1:j-1}\right) \triangleq \arg\max_{u\in\{0,1\}} \left\{ \mathbb{P}\left(U_2(j) = u \middle| U_2^{1:j-1} = u_2^{1:j-1}\right) \right\}. \tag{4.24}$$

4.4.3.2 Random Mapping

Consider the following class of random boolean functions indexed by $j \in [n]$:

$$\Psi_1^{(j)} : \{0,1\}^{n+j-1} \to \{0,1\}, \tag{4.25}$$

$$\Psi_2^{(j)} : \{0,1\}^{j-1} \to \{0,1\}. \tag{4.26}$$

As an example, consider the random boolean functions

$$\Psi_1^{(j)}\big(u_1^{1:j-1}, v^n\big) \triangleq \begin{cases} 0, & \text{w.p.} \quad \lambda_0\big(u_1^{1:j-1}, v^n\big), \\ 1, & \text{w.p.} \quad 1 - \lambda_0\big(u_1^{1:j-1}, v^n\big), \end{cases} \tag{4.27}$$

$$\Psi_2^{(j)}\big(u_2^{1:j-1}\big) \triangleq \begin{cases} 0, & \text{w.p.} \quad \lambda_0\big(u_2^{1:j-1}\big), \\ 1, & \text{w.p.} \quad 1 - \lambda_0\big(u_2^{1:j-1}\big), \end{cases} \tag{4.28}$$

where

$$\lambda_0\big(u_2^{1:j-1}\big) \triangleq \mathbb{P}\big(U_2(j) = 0 \big| U_2^{1:j-1} = u_2^{1:j-1}\big).$$

$$\lambda_0\big(u_1^{1:j-1}, v^n\big) \triangleq \mathbb{P}\big(U_1(j) = 0 \big| U_1^{1:j-1} = u_1^{1:j-1}, V^n = v^n\big).$$

The random boolean functions $\Psi_1^{(j)}$ and $\Psi_2^{(j)}$ may be thought of as a vector of independent Bernoulli random variables indexed by the input to the function. Each Bernoulli random variable of the vector is zero or one with a fixed probability.

4.4.3.3 Protocol

The encoder constructs the sequence u_2^n first using the message bits W_2 and either (4.24) or (4.28). Next, the sequence $v^n = u_2^n \mathbf{G}_n$ is created. Finally, the sequence u_1^n is constructed using the message bits W_1, the sequence v^n, and either the deterministic maps defined in (4.23) or the randomized maps in (4.27). The transmitted codeword is $x^n = u_1^n \mathbf{G}_n$.

4.4.4 Broadcast Decoding Based on Polarization

4.4.4.1 Decoding At First Receiver

Decoder $\mathcal{D}_1$ decodes the binary sequence $\hat{u}_2^n$ first using its observations y_1^n. It then reconstructs $\hat{v}^n = \hat{u}_2^n \mathbf{G}_n$. Using the sequence $\hat{v}^n$ and observations y_1^n, the decoder reconstructs $\hat{u}_1^n$. The message W_1 is located at the indices $j \in \mathcal{M}_1^{(n)}$ in the sequence $\hat{u}_1^n$. More precisely, define the following deterministic polar decoding functions:

$$\xi_v^{(j)}\left(u_2^{1:j-1}, y_1^n\right) \triangleq \arg\max_{u\in\{0,1\}} \left\{ \mathbb{P}\left(U_2(j) = u \middle| U_2^{1:j-1} = u_2^{1:j-1}, Y_1^n = y_1^n\right) \right\}. \tag{4.29}$$

$$\xi_{u_1}^{(j)}\left(u_1^{1:j-1}, v^n, y_1^n\right) \triangleq \arg\max_{u\in\{0,1\}} \left\{ \mathbb{P}\left(U_1(j) = u \middle| U_1^{1:j-1} = u_1^{1:j-1}, V^n = v^n, Y_1^n = y_1^n\right) \right\}. \tag{4.30}$$

The decoder $\mathcal{D}_1$ reconstructs $\hat{u}_2^n$ bit-by-bit successively as follows using the *identical* shared random mapping $\Psi_2^{(j)}$ (or possibly the identical shared mapping $\psi_2^{(j)}$) used at the encoder:

$$\hat{u}_2(j) = \begin{cases} \xi_v^{(j)}\left(\hat{u}_2^{1:j-1}, y_1^n\right), & \text{if } j \in \mathcal{M}_2^{(n)}, \\ \Psi_2^{(j)}\left(\hat{u}_2^{1:j-1}\right), & \text{otherwise.} \end{cases} \tag{4.31}$$

If Lemma 11 holds, note that $\mathcal{M}_2^{(n)} \subseteq \mathcal{M}_{1v}^{(n)}$. With $\hat{u}_2^n$, decoder $\mathcal{D}_1$ reconstructs $\hat{v}^n = \hat{u}_2^n \mathbf{G}_n$. Then the sequence $\hat{u}_1^n$ is constructed bit-by-bit successively as follows using the *identical* shared random mapping $\Psi_1^{(j)}$ (or possibly the identical shared mapping $\psi_1^{(j)}$) used at the encoder:

$$\hat{u}_1(j) = \begin{cases} \xi_{u_1}^{(j)}\left(\hat{u}_1^{1:j-1}, \hat{v}^n, y_1^n\right), & \text{if } j \in \mathcal{M}_1^{(n)}, \\ \Psi_1^{(j)}\left(\hat{u}_1^{1:j-1}, \hat{v}^n\right), & \text{otherwise.} \end{cases} \tag{4.32}$$

4.4.4.2 Decoding At Second Receiver

The decoder $\mathcal{D}_2$ decodes the binary sequence $\hat{u}_2^n$ using observations y_2^n. The message W_2 is located at the indices $j \in \mathcal{M}_2^{(n)}$ of the sequence $\hat{u}_2^n$. More precisely, define the following polar decoding functions

$$\xi_v^{(j)}\left(u_2^{1:j-1}, y_2^n\right) \triangleq \arg\max_{u\in\{0,1\}} \left\{ \mathbb{P}\left(U_2(j) = u \middle| U_2^{1:j-1} = u_2^{1:j-1}, Y_2^n = y_2^n\right) \right\}. \tag{4.33}$$

The decoder $\mathcal{D}_2$ reconstructs $\hat{u}_2^n$ bit-by-bit successively as follows using the *identical* shared random mapping $\Psi_2^{(j)}$ (or possibly the identical shared mapping $\psi_2^{(j)}$) used at the encoder:

$$\hat{u}_2(j) = \begin{cases} \xi_v^{(j)}\left(\hat{u}_2^{1:j-1}, y_2^n\right), & \text{if } j \in \mathcal{M}_2^{(n)}, \\ \Psi_2^{(j)}\left(\hat{u}_2^{1:j-1}\right), & \text{otherwise.} \end{cases} \tag{4.34}$$

Remark 11. *The encoder and decoders execute* the same *protocol for reconstructing bits at the* non-message *indices. This is achieved by applying the same deterministic maps* $\psi_1^{(j)}$ *and* $\psi_2^{(j)}$ *or randomized maps* $\Psi_1^{(j)}$ *and* $\Psi_2^{(j)}$.

4.4.5 Total Variation Bound

To analyze the average probability of error $P_e^{(n)}$ via the probabilistic method, it is assumed that both the encoder and decoder share the *randomized* mappings $\Psi_1^{(j)}$ and $\Psi_2^{(j)}$. Define the following probability measure on the space of tuples of binary sequences.

$$Q\big(u_1^n, u_2^n\big) \triangleq Q\big(u_2^n\big)Q\big(u_1^n\big|u_2^n\big) = \prod_{j=1}^{n} Q\Big(u_2(j)\Big|u_2^{1:j-1}\Big)Q\Big(u_1(j)\Big|u_1^{1:j-1}, u_2^n\Big). \tag{4.35}$$

In (4.35), the conditional probability measures are defined as

$$Q\Big(u_2(j)\Big|u_2^{1:j-1}\Big) \triangleq \begin{cases} \frac{1}{2}, & \text{if } j \in \mathcal{M}_2^{(n)}, \\ P\left(u_2(j)\Big|u_2^{1:j-1}\right), & \text{otherwise.} \end{cases}$$

$$Q\Big(u_1(j)\Big|u_1^{1:j-1}, u_2^n\Big) \triangleq \begin{cases} \frac{1}{2}, & \text{if } j \in \mathcal{M}_1^{(n)}, \\ P\left(u_1(j)\Big|u_1^{1:j-1}, u_2^n\right), & \text{otherwise.} \end{cases}$$

The probability measure Q defined in (4.35) is a perturbation of the joint probability measure $P_{U_1^n U_2^n}(u_1^n, u_2^n)$ in (4.15). The only difference in definition between P and Q is due to those indices in message sets $\mathcal{M}_1^{(n)}$ and $\mathcal{M}_2^{(n)}$. The following lemma provides a bound on the total variation distance between P and Q. The lemma establishes the fact that inserting uniformly distributed message bits in the proper indices $\mathcal{M}_1^{(n)}$ and $\mathcal{M}_2^{(n)}$ at the encoder *does not* perturb the statistics of the n-length random variables too much.

Lemma 12. *(*Total Variation Bound*) Let probability measures P and Q be defined as in (4.15) and (4.35) respectively. Let $0 < \beta < 1$. For sufficiently large n, the total variation distance between P and Q is bounded as*

$$\sum_{\substack{u_1^n \in \{0,1\}^n \\ u_2^n \in \{0,1\}^n}} \Big|P_{U_1^n U_2^n}\big(u_1^n, u_2^n\big) - Q\big(u_1^n, u_2^n\big)\Big| \leq 2^{-n^\beta}.$$

Proof. See Section 4.6 of the Appendices. □

4.4.6 Error Sequences

The decoding protocols for $\mathcal{D}_1$ and $\mathcal{D}_2$ were established in Section 4.4.4. To analyze the probability of error of successive cancelation (SC) decoding, consider the sequences u_1^n and u_2^n formed at the encoder, and the resulting observations y_1^n and y_2^n received by the decoders. It is convenient to group the sequences together and consider all tuples $(u_1^n, u_2^n, y_1^n, y_2^n)$.

Decoder $\mathcal{D}_1$ makes an SC decoding error on the j-th bit for the following tuples:

$$\begin{aligned}
\mathcal{T}_{1v}^j \triangleq \Big\{ & \big(u_1^n, u_2^n, y_1^n, y_2^n\big): \\
& P_{U_2^j \left| U_2^{1:j-1} Y_1^n \right.}\big(u_2(j) \big| u_2^{1:j-1}, y_1^n\big) \leq \\
& P_{U_2^j \left| U_2^{1:j-1} Y_1^n \right.}\big(u_2(j) \oplus 1 \big| u_2^{1:j-1}, y_1^n\big) \Big\}, \\
\mathcal{T}_1^j \triangleq \Big\{ & \big(u_1^n, u_2^n, y_1^n, y_2^n\big): \\
& P_{U_1^j \left| U_1^{1:j-1} V^n Y_1^n \right.}\big(u_1(j) \big| u_1^{1:j-1}, u_2^n \mathbf{G}_n, y_1^n\big) \leq \\
& P_{U_1^j \left| U_1^{1:j-1} V^n Y_1^n \right.}\big(u_1(j) \oplus 1 \big| u_1^{1:j-1}, u_2^n \mathbf{G}_n, y_1^n\big) \Big\}.
\end{aligned} \tag{4.36}$$

The set $\mathcal{T}_{1v}^j$ represents those tuples causing an error at $\mathcal{D}_1$ in the case $u_2(j)$ is inconsistent with respect to observations y_1^n and the decoding rule. The set $\mathcal{T}_1^j$ represents those tuples causing an error at $\mathcal{D}_1$ in the case $u_1(j)$ is inconsistent with respect to $v^n = u_2^n \mathbf{G}_n$, observations y_1^n, and the decoding rule. Similarly, decoder $\mathcal{D}_2$ makes an SC decoding error on the j-th bit for the following tuples:

$$\begin{aligned}
\mathcal{T}_2^j \triangleq \Big\{ & \big(u_1^n, u_2^n, y_1^n, y_2^n\big) \colon P_{U_2 \left| U_2^{1:j-1} Y_2^n \right.}\big(u_2 \big| u_2^{1:j-1}, y_2^n\big) \leq \\
& P_{U_2 \left| U_2^{1:j-1} Y_2^n \right.}\big(u_2 \oplus 1 \big| u_2^{1:j-1}, y_2^n\big) \Big\}.
\end{aligned}$$

The set $\mathcal{T}_2^j$ represents those tuples causing an error at $\mathcal{D}_2$ in the case $u_2(j)$ is inconsistent with respect to observations y_2^n and the decoding rule. Since both decoders $\mathcal{D}_1$ and $\mathcal{D}_2$ only declare errors for those indices in the message sets, the set of tuples causing an error is

$$\mathcal{T}_{1v} \triangleq \bigcup_{j \in \mathcal{M}_2^{(n)} \subseteq \mathcal{M}_{1v}^{(n)}} \mathcal{T}_{1v}^j, \tag{4.37}$$

$$\mathcal{T}_1 \triangleq \bigcup_{j \in \mathcal{M}_1^{(n)}} \mathcal{T}_1^j, \tag{4.38}$$

$$\mathcal{T}_2 \triangleq \bigcup_{j \in \mathcal{M}_2^{(n)}} \mathcal{T}_2^j. \tag{4.39}$$

The complete set of tuples causing a broadcast error is

$$\mathcal{T} \triangleq \mathcal{T}_{1v} \cup \mathcal{T}_1 \cup \mathcal{T}_2. \tag{4.40}$$

The goal is to show that the probability of choosing tuples of error sequences in the set $\mathcal{T}$ is small under the distribution induced by the broadcast code.

4.4.7 Average Error Probability

Denote the total sum rate of the broadcast protocol as $R_\Sigma = R_1 + R_2$. Consider first the use of fixed deterministic maps $\psi_1^{(j)}$ and $\psi_2^{(j)}$ shared between the encoder and decoders. Then the probability of error of broadcasting the two messages at rates R_1 and R_2 is given by

$$P_e^{(n)}\left[\{\psi_1^{(j)},\psi_2^{(j)}\}\right] = \sum_{\{u_1^n,u_2^n,y_1^n,y_2^n\}\in\mathcal{T}}\Bigg[P_{Y_1^nY_2^n\left|U_1^nU_2^n\right.}\left(y_1^n,y_2^n\middle|u_1^n,u_2^n\right) \cdot \frac{1}{2^{nR_2}}\prod_{j\in[n]:j\notin\mathcal{M}_2^{(n)}} \mathbb{1}_{\left[\psi_2^{(j)}\left(u_2^{1:j-1}\right)=u_2(j)\right]} \cdot \frac{1}{2^{nR_1}}\prod_{j\in[n]:j\notin\mathcal{M}_1^{(n)}} \mathbb{1}_{\left[\psi_1^{(j)}\left(u_1^{1:j-1},u_2^n\mathbf{G}_n\right)=u_1(j)\right]}\Bigg].$$

If the encoder and decoders share randomized maps $\Psi_1^{(j)}$ and $\Psi_2^{(j)}$, then the average probability of error is a random quantity determined as follows

$$P_e^{(n)}\left[\{\Psi_1^{(j)},\Psi_2^{(j)}\}\right] = \sum_{\{u_1^n,u_2^n,y_1^n,y_2^n\}\in\mathcal{T}}\Bigg[P_{Y_1^nY_2^n\left|U_1^nU_2^n\right.}\left(y_1^n,y_2^n\middle|u_1^n,u_2^n\right) \cdot \frac{1}{2^{nR_2}}\prod_{j\in[n]:j\notin\mathcal{M}_2^{(n)}} \mathbb{1}_{\left[\Psi_2^{(j)}\left(u_2^{1:j-1}\right)=u_2(j)\right]} \cdot \frac{1}{2^{nR_1}}\prod_{j\in[n]:j\notin\mathcal{M}_1^{(n)}} \mathbb{1}_{\left[\Psi_1^{(j)}\left(u_1^{1:j-1},u_2^n\mathbf{G}_n\right)=u_1(j)\right]}\Bigg].$$

By averaging over the randomness in the encoders and decoders, the expected block error probability is upper bounded in the following lemma.

Lemma 13. *Consider the polarization-based superposition code described in Section 4.4.3 and Section 4.4.4. Let R_1 and R_2 be the broadcast rates selected according to the Bhattacharyya criterion given in Proposition 5. Then for $0<\beta<1$ and sufficiently large n,*

$$\mathbb{E}_{\{\Psi_1^{(j)},\Psi_2^{(j)}\}}\left[P_e^{(n)}[\{\Psi_1^{(j)},\Psi_2^{(j)}\}]\right] < 2^{-n^\beta}.$$

Proof. See Section 4.6 of the Appendices. □

If the average probability of error decays to zero in expectation over the random maps $\{\Psi_1^{(j)}\}$ and $\{\Psi_2^{(j)}\}$, then there must exist at least one fixed set of maps for which $P_e^{(n)}\to 0$.

4.5 Proof Of Lemmas

To prove Lemma 10, note that the implication in (4.5) follows since $X - Y_1 - Y_2$ means that

$$P_{Y_2|X}(y_2|x) = \sum_{y_1} P_{Y_1|X}(y_1|x) P_{Y_2|Y_1}(y_2|y_1).$$

The implication in (4.6) follows by observing that

$$\begin{aligned}
P_{Y_2|V}(y_2|v) &= \sum_{y_1 \in \mathcal{Y}_1} P_{Y_1 Y_2|V}(y_1, y_2|v) \\
&= \sum_{x \in \mathcal{X}} \sum_{y_1 \in \mathcal{Y}_1} P_{X|V}(x|v) P_{Y_1 Y_2|X}(y_1, y_2|x) \\
&= \sum_{x \in \mathcal{X}} P_{X|V}(x|v) \sum_{y_1 \in \mathcal{Y}_1} P_{Y_1 Y_2|X}(y_1, y_2|x) \\
&= \sum_{x \in \mathcal{X}} P_{X|V}(x|v) P_{Y_2|X}(y_2|x) \\
&= \sum_{x \in \mathcal{X}} P_{X|V}(x|v) \sum_{y_1 \in \mathcal{Y}_1} P_{Y_1|X}(y_1|x) \tilde{P}_{Y_2|Y_1}(y_2|y_1) \qquad (4.41) \\
&= \sum_{y_1 \in \mathcal{Y}_1} \sum_{x \in \mathcal{X}} P_{X|V}(x|v) P_{Y_1|X}(y_1|x) \tilde{P}_{Y_2|Y_1}(y_2|y_1) \\
&= \sum_{y_1 \in \mathcal{Y}_1} P_{Y_1|V}(y_1|v) \tilde{P}_{Y_2|Y_1}(y_2|y_1).
\end{aligned}$$

In step (4.41), the assumed stochastic degraded condition $P_{Y_1|X}(y_1|x) \succ P_{Y_2|X}(y_2|x)$ ensures the existence of the distribution $\tilde{P}_{Y_2|Y_1}(y_2|y_1)$. The converse to (4.6) follows since it is possible to select $P_{X|V}(x|v) = \mathbb{1}_{[x=v]}$ where the alphabet $\mathcal{V} = \mathcal{X}$. In this case, for any $v \in \mathcal{X}$,

$$\begin{aligned}
P_{Y_2|V}(y_2|v) &= \sum_{x \in \mathcal{X}} P_{X|V}(x|v) P_{Y_2|X}(y_2|x) \\
&= \sum_{x \in \mathcal{X}} \mathbb{1}_{[x=v]} P_{Y_2|X}(y_2|x) \\
&= P_{Y_2|X}(y_2|v).
\end{aligned}$$

Similarly, $P_{Y_1|V}(y_1|v) = P_{Y_1|X}(y_1|v)$ for any $v \in \mathcal{X}$. Due to the assumed stochastic degradedness condition $P_{Y_2|V}(y_2|v) = \sum_{y_1} P_{Y_1|V}(y_1|v) \tilde{P}_{Y_2|Y_1}(y_2|y_1)$, for any $v \in \mathcal{X}$,

$$\begin{aligned}
P_{Y_2|X}(y_2|v) &= P_{Y_2|V}(y_2|v) \\
&= \sum_{y_1} P_{Y_1|V}(y_1|v) \tilde{P}_{Y_2|Y_1}(y_2|y_1) \\
&= \sum_{y_1} P_{Y_1|X}(y_1|v) \tilde{P}_{Y_2|Y_1}(y_2|y_1).
\end{aligned}$$

Therefore the stochastic degradedness property $P_{Y_1|X}(y_1|x) \succ P_{Y_2|X}(y_2|x)$ must hold as well. The statement of (4.6) means that Class I and Class II are equivalent as shown in Figure 4.1. The implication in (4.7) follows because assuming the stochastic degradedness property $P_{Y_1|V}(y_1|v) \succ P_{Y_2|V}(y_2|v)$ holds for all $P_{X|V}(x|v)$, there exists a $\tilde{Y}_1$ such that $V - \tilde{Y}_1 - Y_2$ form a Markov chain and $P_{\tilde{Y}_1|V}(\tilde{y}_1|v) = P_{Y_1|V}(\tilde{y}_1|v)$ for all $P_{X|V}(x|v)$. By the data processing inequality, $I(V;\tilde{Y}_1) \geq I(V;Y_2)$. If $P_{\tilde{Y}_1|V}(\tilde{y}_1|v) = P_{Y_1|V}(\tilde{y}_1|v)$, then $P_{V\tilde{Y}_1}(v,\tilde{y}_1) = P_{VY_1}(v,\tilde{y}_1)$ for all $P_V(v)$. It follows that for all $P_{VX}(v,x)$, the mutual information $I(V;\tilde{Y}_1) = I(V;Y_1)$. The implication in (4.8) follows by setting $P_{VX}(v,x) = \mathbb{1}_{[v=x]}P_X(x)$ and letting $\mathcal{V} = \mathcal{X}$. Then for any $v \in \mathcal{X}$,

$$\begin{aligned} P_{VY_1}(v,y_1) &= \sum_{x\in\mathcal{X}} P_{VX}(v,x)P_{Y_1|X}(y_1|x) \\ &= \sum_{x\in\mathcal{X}} \mathbb{1}_{[v=x]}P_X(x)P_{Y_1|X}(y_1|x) \\ &= P_X(v)P_{Y_1|X}(y_1|v) \\ &= P_{XY_1}(v,y_1). \end{aligned}$$

Similarly for any $v \in \mathcal{X}$, $P_{VY_2}(v,y_2) = P_{XY_2}(v,y_2)$. Therefore for the particular choice of $P_{VX}(v,x) = \mathbb{1}_{[v=x]}P_X(x)$, $I(V;Y_1) = I(X;Y_1)$ and $I(V;Y_2) = I(X;Y_2)$. The converse statements for (4.5), (4.7), and (4.8) do *not* hold due to a counterexample involving a DM-BC comprised of a binary erasure channel BEC(ϵ) and a binary symmetric channel BSC(p) as described in Example 5.

4.6 Bounding the Probability Of Error

The total variation bound of Lemma 12 is decomposed in a simple way due to the chain rule for Kullback-Leibler distance between discrete probability measures. The joint probability measures P and Q were defined in (4.15) and (4.35) respectively. According to definition, if $P_{U_1^nU_2^n}(u_1^n,u_2^n) > 0$ then $Q(u_1^n,u_2^n) > 0$. Therefore the Kullback-Leibler distance $D(P\|Q)$ is well-defined. Applying the chain rule,

$$\begin{aligned} D\Big(P_{U_1^nU_2^n}(u_1^n,u_2^n)\Big\|Q(u_1^n,u_2^n)\Big) &= \sum_{j=1}^{n} D\Big(P\left(u_1(j)\Big|u_1^{1:j-1}\right)\Big\|Q\left(u_1(j)\Big|u_1^{1:j-1}\right)\Big) \\ &\quad + \sum_{j=1}^{n} D\Big(P\left(u_2(j)\Big|u_2^{1:j-1},u_1^n\right)\Big\|Q\left(u_2(j)\Big|u_2^{1:j-1},u_1^n\right)\Big) \\ &= \sum_{j\in\mathcal{M}_1^{(n)}} D\Big(P\left(u_1(j)\Big|u_1^{1:j-1}\right)\Big\|Q\left(u_1(j)\Big|u_1^{1:j-1}\right)\Big) \\ &\quad + \sum_{j\in\mathcal{M}_2^{(n)}} D\Big(P\left(u_2(j)\Big|u_2^{1:j-1},u_1^n\right)\Big\|Q\left(u_2(j)\Big|u_2^{1:j-1},u_1^n\right)\Big). \end{aligned}$$

Applying Lemma 3, the one-to-one relation between U_1^n and V^n, and Lemma 9 leads to the following result.

$$\begin{aligned}
&D\Big(P_{U_1^nU_2^n}\left(u_1^n,u_2^n\right)\Big\|Q\left(u_1^n,u_2^n\right)\Big)\\
&=\sum_{j\in\mathcal{M}_1^{(n)}}\left[1-H\left(U_1(j)\Big|U_1^{1:j-1}\right)\right]+\sum_{j\in\mathcal{M}_2^{(n)}}\left[1-H\left(U_2(j)\Big|U_2^{1:j-1}U_1^n\right)\right]\\
&=\sum_{j\in\mathcal{M}_1^{(n)}}\left[1-H\left(U_1(j)\Big|U_1^{1:j-1}\right)\right]+\sum_{j\in\mathcal{M}_2^{(n)}}\left[1-H\left(U_2(j)\Big|U_2^{1:j-1}V^n\right)\right]\\
&\leq 2\delta_n\left[\left|\mathcal{M}_1^{(n)}\right|+\left|\mathcal{M}_2^{(n)}\right|\right].
\end{aligned}$$

Using identical arguments as applied in the proof of Lemma 1, the total variation distance between P and Q is bounded as $\mathcal{O}(2^{-n^\beta})$.

To prove Lemma 13, the expectation of the average probability of error of the polarization-based superposition code is written as

$$\begin{aligned}
&\mathbb{E}_{\{\Psi_1^{(j)},\Psi_2^{(j)}\}}\left[P_e^{(n)}[\{\Psi_1^{(j)},\Psi_2^{(j)}\}]\right]=\\
&\quad\sum_{\{u_1^n,u_2^n,y_1^n,y_2^n\}\in\mathcal{T}}\Bigg[P_{Y_1^nY_2^n\left|U_1^nU_2^n\right.}\left(y_1^n,y_2^n\middle|u_1^n,u_2^n\right)\\
&\quad\cdot\frac{1}{2^{nR_2}}\prod_{j\in[n]:j\notin\mathcal{M}_2^{(n)}}\mathbb{P}\left\{\Psi_2^{(j)}\left(u_2^{1:j-1}\right)=u_2(j)\right\}\\
&\quad\cdot\frac{1}{2^{nR_1}}\prod_{j\in[n]:j\notin\mathcal{M}_1^{(n)}}\mathbb{P}\left\{\Psi_1^{(j)}\left(u_1^{1:j-1},u_2^n\mathbf{G}_n\right)=u_1(j)\right\}\Bigg].
\end{aligned}$$

From the definitions of the random boolean functions $\Psi_1^{(j)}$ in (4.27) and $\Psi_2^{(j)}$ in (4.28), it follows that

$$\begin{aligned}
&\mathbb{P}\left\{\Psi_1^{(j)}\left(u_1^{1:j-1},u_2^n\mathbf{G}_n\right)=u_1(j)\right\}\\
&\quad=\mathbb{P}\left\{U_1(j)=u_1(j)\middle|U_1^{1:j-1}=u_1^{1:j-1},V^n=u_2^n\mathbf{G}_n\right\}\\
&\quad=\mathbb{P}\left\{U_1(j)=u_1(j)\middle|U_1^{1:j-1}=u_1^{1:j-1},U_2^n=u_2^n\right\},\\
&\mathbb{P}\left\{\Psi_2^{(j)}\left(u_2^{1:j-1}\right)=u_2(j)\right\}\\
&\quad=\mathbb{P}\left\{U_2(j)=u_2(j)\middle|U_2^{1:j-1}=u_2^{1:j-1}\right\}.
\end{aligned}$$

The expression for the expected average probability of error is then simplified by substituting the definition for $Q(u_1^n, u_2^n)$ provided in (4.35) as follows,

$$\mathbb{E}_{\{\Psi_1^{(j)},\Psi_2^{(j)}\}}\Big[P_e^{(n)}[\{\Psi_1^{(j)},\Psi_2^{(j)}\}]\Big] = \sum_{\{u_1^n,u_2^n,y_1^n,y_2^n\}\in\mathcal{T}}\Bigg[P_{Y_1^nY_2^n\big|U_1^nU_2^n}\big(y_1^n,y_2^n\big|u_1^n,u_2^n\big)Q(u_1^n,u_2^n)\Bigg].$$

The next step in the proof is to split the error term $\mathbb{E}_{\{\Psi_1^{(j)},\Psi_2^{(j)}\}}\Big[P_e^{(n)}[\{\Psi_1^{(j)},\Psi_2^{(j)}\}]\Big]$ into *two* main parts, one part due to the error caused by polar decoding functions, and the other part due to the total variation distance between probability measures.

$$\begin{aligned}
&\mathbb{E}_{\{\Psi_1^{(j)},\Psi_2^{(j)}\}}\Big[P_e^{(n)}[\{\Psi_1^{(j)},\Psi_2^{(j)}\}]\Big]\\
&= \sum_{\{u_1^n,u_2^n,y_1^n,y_2^n\}\in\mathcal{T}}\Bigg[P_{Y_1^nY_2^n\big|U_1^nU_2^n}\big(y_1^n,y_2^n\big|u_1^n,u_2^n\big)\\
&\quad\cdot\Big(Q\big(u_1^n,u_2^n\big)-P_{U_1^nU_2^n}\big(u_1^n,u_2^n\big)+P_{U_1^nU_2^n}\big(u_1^n,u_2^n\big)\Big)\Bigg]\\
&\leq \Bigg[\sum_{\{u_1^n,u_2^n,y_1^n,y_2^n\}\in\mathcal{T}} P_{U_1^nU_2^nY_1^nY_2^n}\big(u_1^n,u_2^n,y_1^n,y_2^n\big)\Bigg]\\
&\qquad+\Bigg[\sum_{\substack{u_1^n\in\{0,1\}^n\\ u_2^n\in\{0,1\}^n}}\Big|P_{U_1^nU_2^n}\big(u_1^n,u_2^n\big)-Q\big(u_1^n,u_2^n\big)\Big|\Bigg].
\end{aligned}\tag{4.42}$$

Lemma 12 established that the error term due to the total variation distance is upper bounded as $\mathcal{O}(2^{-n^\beta})$. Therefore, it remains to upper bound the error term due to the polar decoding functions. Towards this end, note first that $\mathcal{T} = \mathcal{T}_{1v}\cup\mathcal{T}_1\cup\mathcal{T}_2$, $\mathcal{T}_{1v} = \cup_j\mathcal{T}_{1v}^j$ for $j\in\mathcal{M}_2^{(n)}\subseteq\mathcal{M}_{1v}^{(n)}$, $\mathcal{T}_1 = \cup_j\mathcal{T}_1^j$ for $j\in\mathcal{M}_1^{(n)}$, and $\mathcal{T}_2 = \cup_j\mathcal{T}_2^j$ for $j\in\mathcal{M}_2^{(n)}$. It is convenient to bound each type of error bit by bit successively at both decoder $\mathcal{D}_1$ and $\mathcal{D}_2$ as follows.

$$\begin{aligned}
\mathcal{E}_{1v}^j &\triangleq \sum_{\{u_1^n,u_2^n,y_1^n,y_2^n\}\in\mathcal{T}_{1v}^j} P_{U_1^nU_2^nY_1^nY_2^n}\big(u_1^n,u_2^n,y_1^n,y_2^n\big)\\
&= \sum_{(u_2^{1:j},y_1^n)\in\{0,1\}^j\times\mathcal{Y}_1^n} P_{U_2^{1:j}Y_1^n}\big(u_2^{1:j},y_1^n\big)\\
&\qquad\cdot\mathbb{1}\Bigg[P_{U_2^j\big|U_2^{1:j-1}Y_1^n}\big(u_2(j)\big|u_2^{1:j-1},y_1^n\big)\leq\\
&\qquad\qquad P_{U_2^j\big|U_2^{1:j-1}Y_1^n}\big(u_2(j)\oplus 1\big|u_2^{1:j-1},y_1^n\big)\Bigg].
\end{aligned}$$

In this form, it is possible to upper bound the error term $\mathcal{E}_{1v}^{j}$ with the corresponding Bhattacharyya parameter as follows,

$$\begin{aligned}
\mathcal{E}_{1v}^{j} &= \sum_{\substack{u_2^{1:j}\in\{0,1\}^j \\ y_1^n\in\mathcal{Y}_1^n}} P\big(u_2^{1:j-1}, y_1^n\big) P\big(u_2^j \big| u_2^{1:j-1}, y_1^n\big) \\
&\quad \cdot \mathbb{1}\Bigg[P_{U_2^j \left| U_2^{1:j-1} Y_1^n \right.}\big(u_2(j) \big| u_2^{1:j-1}, y_1^n\big) \leq \\
&\qquad\qquad P_{U_2^j \left| U_2^{1:j-1} Y_1^n \right.}\big(u_2(j)\oplus 1 \big| u_2^{1:j-1}, y_1^n\big) \Bigg], \\
&\leq \sum_{\substack{u_2^{1:j}\in\{0,1\}^j \\ y_1^n\in\mathcal{Y}_1^n}} P\big(u_2^{1:j-1}, y_1^n\big) P\big(u_2^j \big| u_2^{1:j-1}, y_1^n\big) \\
&\quad \cdot \sqrt{\frac{P_{U_2^j \left| U_2^{1:j-1} Y_1^n \right.}\big(u_2(j)\oplus 1 \big| u_2^{1:j-1}, y_1^n\big)}{P_{U_2^j \left| U_2^{1:j-1} Y_1^n \right.}\big(u_2(j) \big| u_2^{1:j-1}, y_1^n\big)}} \\
&= Z\big(U_2^j \big| U_2^{1:j-1}, Y_1^n\big).
\end{aligned}$$

Using identical arguments, the following upper bounds apply for the individual bit-by-bit error terms caused by successive decoding at both $\mathcal{D}_1$ and $\mathcal{D}_2$.

$$\mathcal{E}_{1v}^{j} \leq Z\big(U_2^j \big| U_2^{1:j-1}, Y_1^n\big), \tag{4.43}$$

$$\mathcal{E}_{1}^{j} \leq Z\big(U_1^j \big| U_1^{1:j-1}, V^n, Y_1^n\big), \tag{4.44}$$

$$\mathcal{E}_{2}^{j} \leq Z\big(U_2^j \big| Y_2^n\big). \tag{4.45}$$

Therefore, the total error due to decoding at the receivers is upper bounded as

$$\begin{aligned}
\mathcal{E} &\triangleq \sum_{\{u_1^n, u_2^n, y_1^n, y_2^n\}\in\mathcal{T}} P_{U_1^n U_2^n Y_1^n Y_2^n}\big(u_1^n, u_2^n, y_1^n, y_2^n\big) \\
&\leq \sum_{j\in\mathcal{M}_2^{(n)}\subseteq\mathcal{M}_{1v}^{(n)}} Z\big(U_2^j \big| U_2^{1:j-1}, Y_1^n\big) + \sum_{j\in\mathcal{M}_1^{(n)}} Z\big(U_1^j \big| U_1^{1:j-1}, V^n, Y_1^n\big) + \sum_{j\in\mathcal{M}_2^{(n)}} Z\big(U_2^j \big| Y_2^n\big) \\
&\leq \delta_n \left[\left|\mathcal{M}_{1v}^{(n)}\right| + \left|\mathcal{M}_1^{(n)}\right| + \left|\mathcal{M}_2^{(n)}\right| \right] \\
&\leq 3n\delta_n.
\end{aligned}$$

This concludes the proof demonstrating that the expected average probability of error is upper bounded as $\mathcal{O}(2^{-n^\beta})$.

Chapter 5

Marton's Broadcast Construction

5.1 Marton's Inner Bound

For general noisy broadcast channels, Marton's inner bound involves two correlated auxiliary random variables V_1 and V_2 [63]. The intuition behind the coding strategy is to identify two "virtual" channels, one from V_1 to Y_1, and the other from V_2 to Y_2. Somewhat surprisingly, although the broadcast messages are independent, the auxiliary random variables V_1 and V_2 may be correlated to increase rates to both receivers. While there exist generalizations of Marton's strategy, the basic version of the inner bound is presented in this section[1].

Proposition 6 (Marton's Inner Bound)**.** *For any two-user DM-BC, the rates* $(R_1, R_2) \in \mathbb{R}_+^2$ *in the pentagonal region* $\mathfrak{R}(X, V_1, V_2, Y_1, Y_2)$ *are achievable where*

$$\begin{aligned}\mathfrak{R}(X, V_1, V_2, Y_1, Y_2) \triangleq \Big\{ R_1, R_2 \;\Big|\; & R_1 \le I(V_1; Y_1), \\ & R_2 \le I(V_2; Y_2), \\ & R_1 + R_2 \le I(V_1; Y_1) + I(V_2; Y_2) - I(V_1; V_2) \Big\}. \end{aligned} \tag{5.1}$$

and where X, V_1, V_2, Y_1, Y_2 *have a joint distribution given by*

$$P_{V_1V_2}(v_1, v_2) P_{X|V_1V_2}(x|v_1, v_2) P_{Y_1Y_2|X}(y_1, y_2|x).$$

Remark 12. *It can be shown that for Marton's inner bound there is no loss of generality if* $P_{X|V_1V_2}(x|v_1, v_2) = \mathbb{1}_{[x=\phi(v_1,v_2)]}$ *where* $\phi(v_1, v_2)$ *is a deterministic function [33, Section 8.3]. Thus, by allowing a larger alphabet size for the auxiliaries,* X *may be a deterministic function of auxiliaries* (V_1, V_2)*. Marton's inner bound is tight for the class of* semi-deterministic *DM-BCs for which one of the outputs is a deterministic function of the input.*

[1] In addition, it is difficult even to evaluate Marton's inner bound for general channels due to the need for proper cardinality bounds on the auxiliaries [43].

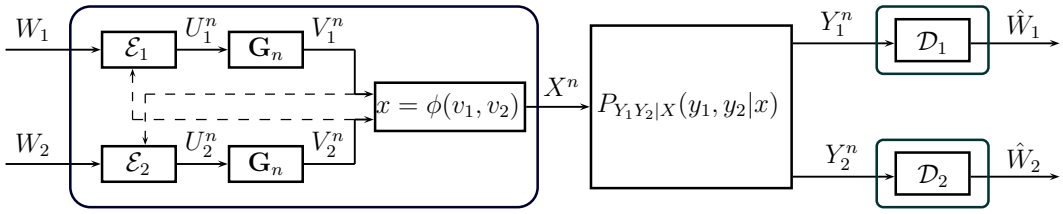


Figure 5.1: Block diagram of a polar code based on Marton's broadcast construction.

5.2 Polar Coding Theorem

Theorem 4 (Polarization-Based Marton Code)**.** *Consider any two-user DM-BC with arbitrary input and output alphabets. There exist sequences of polar broadcast codes over n channel uses which achieve the following rate region*

$$\mathfrak{R}(V_1, V_2, X, Y_1, Y_2) \triangleq \Big\{ R_1, R_2 \;\Big|\; R_1 \le I(V_1; Y_1), \\ R_2 \le I(V_2; Y_2) - I(V_1; V_2) \Big\}, \tag{5.2}$$

where random variables V_1, V_2, X, Y_1, Y_2 have the following listed properties:

- *V_1 and V_2 are binary random variables.*
- *$P_{Y_2|V_2}(y_2|v_2) \succ P_{V_1|V_2}(v_1|v_2)$.*
- *For a deterministic function $\phi : \{0,1\}^2 \to \mathcal{X}$, the joint distribution of all random variables is given by*

$$P_{V_1V_2XY_1Y_2}(v_1, v_2, x, y_1, y_2) = P_{V_1V_2}(v_1, v_2)\mathbb{1}_{[x=\phi(v_1,v_2)]}P_{Y_1Y_2|X}(y_1, y_2|x).$$

For $0 < \beta < \frac{1}{2}$, the average error probability of this code sequence decays as $P_e^{(n)} = \mathcal{O}(2^{-n^\beta})$. The complexity of encoding and decoding is $\mathcal{O}(n \log n)$.

Remark 13. *The listed property $P_{Y_2|V_2}(y_2|v_2) \succ P_{V_1|V_2}(v_1|v_2)$ is necessary in the proof due to polarization-based codes requiring an* alignment *of polarization indices. The property is a* natural *restriction since it also implies that $I(Y_2; V_2) > I(V_1; V_2)$ so that $R_2 > 0$. However, certain joint distributions on random variables are not permitted using the analysis of polarization presented here. It is not clear whether a different approach obviates the need for an alignment of indices.*

Remark 14. *By symmetry, the rate tuple $(R_1, R_2) = (I(V_1; Y_1) - I(V_1; V_2), I(V_2, Y_2))$ is achievable with low-complexity codes under similar constraints on the joint distribution of V_1, V_2, X, Y_1, Y_2. The rate tuple is a corner point of the pentagonal rate region of Marton's inner bound given in (5.1).*

5.3 Proof of Main Theorem

To prove Theorem 4, consider the block diagram for polarization-based Marton coding given in Figure 5.1. Marton's strategy differs form Cover's superposition coding with the presence of two auxiliaries and the function $\phi(v_1, v_2)$ which forms the codeword symbol-by-symbol. The polar transform is applied to each n-length *i.i.d.* sequence of auxiliary random variables.

5.3.1 Polar Transform

Consider the *i.i.d.* sequence of random variables

$$(V_1^j, V_2^j, X^j, Y_1^j, Y_2^j) \sim P_{V_1V_2}(v_1, v_2)P_{X|V_1V_2}(x|v_1, v_2)P_{Y_1Y_2|X}(y_1, y_2|x),$$

where the index $j \in [n]$. For the particular coding strategy analyzed in this section, $P_{X|V_1V_2}(x|v_1, v_2) = \mathbb{1}_{[x=\phi(v_1,v_2)]}$. Let the n-length sequence of auxiliary variables (V_1^j, V_2^j) be organized into the random matrix

$$\mathbf{\Omega} \triangleq \begin{bmatrix} V_1^1 & V_1^2 & V_1^3 & \dots & V_1^n \\ V_2^1 & V_2^2 & V_2^3 & \dots & V_2^n \end{bmatrix}. \tag{5.3}$$

Applying the polar transform to $\mathbf{\Omega}$ results in the random matrix $\mathbf{U} \triangleq \mathbf{\Omega}\mathbf{G}_n$. Index the random variables of $\mathbf{U}$ as follows:

$$\mathbf{U} = \begin{bmatrix} U_1^1 & U_1^2 & U_1^3 & \dots & U_1^n \\ U_2^1 & U_2^2 & U_2^3 & \dots & U_2^n \end{bmatrix}. \tag{5.4}$$

The above definitions are consistent with the block diagram given in Figure 5.1 (and noting that $\mathbf{G}_n = \mathbf{G}_n^{-1}$). The polar transform extracts the randomness of $\mathbf{\Omega}$. In the transformed domain, the joint distribution of the variables in $\mathbf{U}$ is given by

$$P_{U_1^nU_2^n}\big(u_1^n, u_2^n\big) \triangleq P_{V_1^nV_2^n}\big(u_1^n\mathbf{G}_n, u_2^n\mathbf{G}_n\big). \tag{5.5}$$

However, for polar coding purposes, the joint distribution is decomposed as follows,

$$P_{U_1^nU_2^n}\big(u_1^n, u_2^n\big) = P_{U_1^n}(u_1^n)P_{U_2^n|U_1^n}\big(u_2^n\big|u_1^n\big) = \prod_{j=1}^{n} P\big(u_1(j)\big|u_1^{1:j-1}\big)P\big(u_2(j)\big|u_2^{1:j-1}, u_1^n\big). \tag{5.6}$$

The above conditional distributions may be computed efficiently using recursive protocols. The polarized random variables of $\mathbf{U}$ do *not* have an *i.i.d.* distribution.

5.3.2 Effective Channel

Marton's achievable strategy establishes virtual channels for the two receivers via the function $\phi(v_1, v_2)$. The virtual channel is given by

$$P^{\phi}_{Y_1Y_2|V_1V_2}\Big(y_1, y_2\Big|v_1, v_2\Big) \triangleq P_{Y_1Y_2|X}\Big(y_1, y_2\Big|\phi\big(v_1, v_2\big)\Big).$$

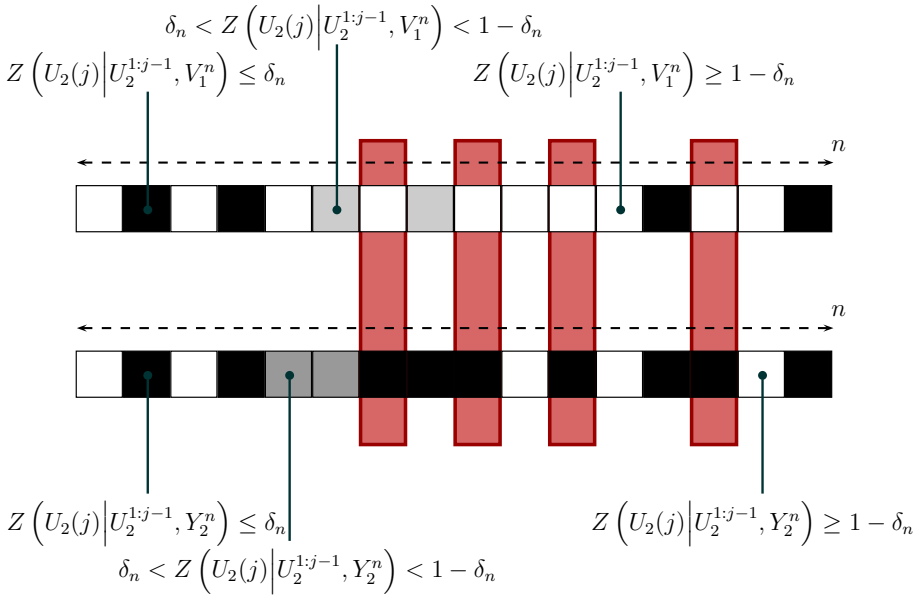


Figure 5.2: The alignment of polarization indices for Marton's broadcast construction.

Due to the memoryless property of the DM-BC, the effective channel between auxiliaries and channel outputs is given by

$$P^{\phi}_{Y_1^n Y_2^n|V_1^n V_2^n}\left(y_1^n, y_2^n \middle| v_1^n, v_2^n\right) \triangleq \prod_{i=1}^{n} P_{Y_1Y_2|X}\left(y_1(i), y_2(i) \middle| \phi\big(v_1(i), v_2(i)\big)\right).$$

The polarization-based Marton code establishes a different effective channel between polar-transformed auxiliaries and the channel outputs. The effective polarized channel is

$$P^{\phi}_{Y_1^n Y_2^n|U_1^n U_2^n}\left(y_1^n, y_2^n \middle| u_1^n, u_2^n\right) \triangleq P^{\phi}_{Y_1^n Y_2^n|V_1^n V_2^n}\left(y_1^n, y_2^n \middle| u_1^n \mathbf{G}_n, u_2^n \mathbf{G}_n\right). \tag{5.7}$$

5.3.3 Polarization Theorems Revisited

Definition 14 (Polarization Sets for Marton Coding)**.** *Let $V_1^n, V_2^n, X^n, Y_1^n, Y_2^n$ be the sequence of random variables as introduced in Section 5.3.1. In addition, let $U_1^n = V_1^n \mathbf{G}_n$ and*

$U_2^n = V_2^n \mathbf{G}_n$. *Let* $\delta_n = 2^{-n^\beta}$ *for* $0 < \beta < \frac{1}{2}$. *The following* polarization sets *are defined:*

$$\begin{aligned}
\mathcal{H}_{V_1}^{(n)} &\triangleq \left\{ j \in [n] : Z\left(U_1(j) \middle| U_1^{1:j-1}\right) \geq 1 - \delta_n \right\}, \\
\mathcal{L}_{V_1|Y_1}^{(n)} &\triangleq \left\{ j \in [n] : Z\left(U_1(j) \middle| U_1^{1:j-1}, Y_1^n\right) \leq \delta_n \right\}, \\
\mathcal{H}_{V_2|V_1}^{(n)} &\triangleq \left\{ j \in [n] : Z\left(U_2(j) \middle| U_2^{1:j-1}, V_1^n\right) \geq 1 - \delta_n \right\}, \\
\mathcal{L}_{V_2|V_1}^{(n)} &\triangleq \left\{ j \in [n] : Z\left(U_2(j) \middle| U_2^{1:j-1}, V_1^n\right) \leq \delta_n \right\}, \\
\mathcal{H}_{V_2|Y_2}^{(n)} &\triangleq \left\{ j \in [n] : Z\left(U_2(j) \middle| U_2^{1:j-1}, Y_2^n\right) \geq 1 - \delta_n \right\}, \\
\mathcal{L}_{V_2|Y_2}^{(n)} &\triangleq \left\{ j \in [n] : Z\left(U_2(j) \middle| U_2^{1:j-1}, Y_2^n\right) \leq \delta_n \right\}.
\end{aligned}$$

Definition 15 (Message Sets for Marton Coding)**.** *In terms of the polarization sets given in Definition 14, the following* message sets *are defined:*

$$\mathcal{M}_1^{(n)} \triangleq \mathcal{H}_{V_1}^{(n)} \cap \mathcal{L}_{V_1|Y_1}^{(n)}, \tag{5.8}$$

$$\mathcal{M}_2^{(n)} \triangleq \mathcal{H}_{V_2|V_1}^{(n)} \cap \mathcal{L}_{V_2|Y_2}^{(n)}. \tag{5.9}$$

Proposition 7 (Polarization)**.** *Consider the polarization sets given in Definition 14 and the message sets given in Definition 15 with parameter* $\delta_n = 2^{-n^\beta}$ *for* $0 < \beta < \frac{1}{2}$. *Fix a constant* $\tau > 0$. *Then there exists an* $N_o = N_o(\beta, \tau)$ *such that*

$$\frac{1}{n}\left|\mathcal{M}_1^{(n)}\right| \geq \Big(H(V_1) - H(V_1|Y_1)\Big) - \tau, \tag{5.10}$$

$$\frac{1}{n}\left|\mathcal{M}_2^{(n)}\right| \geq \Big(H(V_2|V_1) - H(V_2|Y_2)\Big) - \tau, \tag{5.11}$$

for all $n > N_o$.

Lemma 14. *Consider the polarization sets defined in Proposition 7. If the "degraded-ness" property* $P_{Y_2|V_2}(y_2|v_2) \succ P_{V_1|V_2}(v_1|v_2)$ *holds for conditional distributions* $P_{Y_2|V_2}(y_2|v_2)$ *and* $P_{V_1|V_2}(v_1|v_2)$, *then* $I(V_2; Y_2) > I(V_1; V_2)$ *and the Bhattacharyya parameters*

$$Z\left(U_2(j) \middle| U_2^{1:j-1}, Y_2^n\right) \leq Z\left(U_2(j) \middle| U_2^{1:j-1}, V_1^n\right)$$

for all $j \in [n]$. *As a result,*

$$\begin{aligned}
\mathcal{L}_{V_2|V_1}^{(n)} &\subseteq \mathcal{L}_{V_2|Y_2}^{(n)}, \\
\mathcal{H}_{V_2|Y_2}^{(n)} &\subseteq \mathcal{H}_{V_2|V_1}^{(n)}.
\end{aligned}$$

Proof. The proof follows from Lemma 5 and repeated application of Lemma 6 in Appendix 3.5. □

Remark 15. *The alignment of polarization indices characterized by Lemma 14 is diagrammed in Figure 5.2. The message set $\mathcal{M}_2^{(n)}$ is highlighted by the vertical red rectangles. At finite code length n, exact alignment is not possible due to partially-polarized indices pictured in gray. The alignment ensures the existence of polarization indices in the set $\mathcal{M}_2^{(n)}$ for the message W_2 to have a positive rate $R_2 > 0$. The indices in $\mathcal{M}_2^{(n)}$ represent those bits freely set at the broadcast encoder and simultaneously those bits that may be decoded by $\mathcal{D}_2$ given its observations.*

5.3.4 Partially-Polarized Indices

As shown in Figure 5.2, for the Marton coding scheme, exact alignment of polarization indices is not possible. However, the alignment holds for all but $o(n)$ indices. The sets of partially-polarized indices shown in Figure 5.2 are defined as follows.

Definition 16 (Sets of Partially-Polarized Indices)**.**

$$\Delta_1 \triangleq [n] \setminus \left(\mathcal{H}_{V_2|V_1}^{(n)} \cup \mathcal{L}_{V_2|V_1}^{(n)}\right), \tag{5.12}$$

$$\Delta_2 \triangleq [n] \setminus \left(\mathcal{H}_{V_2|Y_2}^{(n)} \cup \mathcal{L}_{V_2|Y_2}^{(n)}\right). \tag{5.13}$$

As implied by Arıkan's polarization theorems, the number of partially-polarized indices is negligible asymptotically as $n \to \infty$. For an arbitrarily small $\eta > 0$,

$$\frac{\left|\Delta_1 \cup \Delta_2\right|}{n} \leq \eta, \tag{5.14}$$

for all n sufficiently large enough. As will be discussed, providing these $o(n)$ bits as "genie-given" bits to the decoders results in a rate penalty; however, the rate penalty is negligible for sufficiently large code lengths.

5.3.5 Broadcast Encoding Blocks: $(\mathcal{E}_1, \mathcal{E}_2)$

As diagrammed in Figure 5.1, the broadcast encoder must map two independent messages (W_1, W_2) uniformly distributed over $[2^{nR_1}] \times [2^{nR_2}]$ to a codeword $x^n \in \mathcal{X}^n$ in such a way that the decoding at each separate receiver is successful. The achievable rates for a particular block length n are

$$R_1 = \frac{1}{n}\left|\mathcal{M}_1^{(n)}\right|,$$

$$R_2 = \frac{1}{n}\left|\mathcal{M}_2^{(n)}\right|.$$

To construct a codeword, the encoder first produces two binary sequences $u_1^n \in \{0,1\}^n$ and $u_2^n \in \{0,1\}^n$. To determine $u_1(j)$ for $j \in \mathcal{M}_1^{(n)}$, the bit is selected as a uniformly distributed message bit intended for the first receiver. To determine $u_2(j)$ for $j \in \mathcal{M}_2^{(n)}$, the bit is selected as a uniformly distributed message bit intended for the second receiver. The remaining *non-message* indices of u_1^n and u_2^n are decided *randomly* according to the proper statistics as will be described in this section. The transmitted codeword is formed symbol-by-symbol via the ϕ function,

$$\forall j \in [n] : x(j) = \phi\big(v_1(j), v_2(j)\big)$$

where $v_1^n = u_1^n \mathbf{G}_n$ and $v_2^n = u_2^n \mathbf{G}_n$. A valid codeword sequence is always guaranteed to be formed unlike in the case of coding for deterministic broadcast channels.

5.3.5.1 Random Mapping

To fill in the non-message indices, we define the following random mappings. Consider the following class of random boolean functions where $j \in [n]$:

$$\Psi_1^{(j)} : \{0,1\}^{j-1} \to \{0,1\}, \tag{5.15}$$

$$\Psi_2^{(j)} : \{0,1\}^{n+j-1} \to \{0,1\}, \tag{5.16}$$

$$\Gamma : [n] \to \{0,1\}. \tag{5.17}$$

More concretely, we consider the following specific random boolean functions based on the statistics derived from polarization methods:

$$\Psi_1^{(j)}\left(u_1^{1:j-1}\right) \triangleq \begin{cases} 0, & \text{w.p.} \quad \lambda_0\left(u_1^{1:j-1}\right), \\ 1, & \text{w.p.} \quad 1-\lambda_0\left(u_1^{1:j-1}\right), \end{cases} \tag{5.18}$$

$$\Psi_2^{(j)}\left(u_2^{1:j-1}, v_1^n\right) \triangleq \begin{cases} 0, & \text{w.p.} \quad \lambda_0\left(u_2^{1:j-1}, v_1^n\right), \\ 1, & \text{w.p.} \quad 1-\lambda_0\left(u_2^{1:j-1}, v_1^n\right) \end{cases} \tag{5.19}$$

$$\Gamma(j) \triangleq \begin{cases} 0, & \text{w.p.} \quad \frac{1}{2}, \\ 1, & \text{w.p.} \quad \frac{1}{2}, \end{cases} \tag{5.20}$$

where

$$\lambda_0\left(u_1^{1:j-1}\right) \triangleq \mathbb{P}\left(U_1(j) = 0 \middle| U_1^{1:j-1} = u_1^{1:j-1}\right).$$

$$\lambda_0\left(u_2^{1:j-1}, v_1^n\right) \triangleq \mathbb{P}\left(U_2(j) = 0 \middle| U_2^{1:j-1} = u_2^{1:j-1}, V_1^n = v_1^n\right).$$

For a fixed $j \in [n]$, the random boolean functions $\Psi_1^{(j)}$, $\Psi_2^{(j)}$ may be thought of as a vector of independent Bernoulli random variables indexed by the input to the function. Each

Bernoulli random variable of the vector is zero or one with a fixed well-defined probability that is efficiently computable. The random boolean function Γ may be thought of as an n-length vector of Bernoulli($\frac{1}{2}$) random variables.

5.3.5.2 Encoding Protocol

The broadcast encoder constructs the sequence u_1^n bit-by-bit successively,

$$u_1(j) = \begin{cases} W_1 \text{ message bit}, & \textit{if } j \in \mathcal{M}_1^{(n)}, \\ \Psi_1^{(j)}\big(u_1^{1:j-1}\big), & \textit{otherwise.} \end{cases} \tag{5.21}$$

The encoder then computes the sequence $v_1^n = u_1^n \mathbf{G}_n$. To generate v_2^n, the encoder constructs the sequence u_2^n (given v_1^n) as follows,

$$u_2(j) = \begin{cases} W_2 \text{ message bit}, & \textit{if } j \in \mathcal{M}_2^{(n)}, \\ \Gamma(j), & \textit{if } j \in \mathcal{H}_{V_2|V_1}^{(n)} \setminus \mathcal{M}_2^{(n)}, \\ \Psi_2^{(j)}\big(u_2^{1:j-1}, v_1^n\big), & \textit{otherwise.} \end{cases} \tag{5.22}$$

Then the sequence $v_2^n = u_2^n \mathbf{G}_n$. The randomness in the above encoding protocol over non-message indices ensures that the pair of sequences (u_1^n, u_2^n) has the correct statistics as if drawn from the joint distribution of (U_1^n, U_2^n). In the last step, the encoder transmits a codeword x^n formed symbol-by-symbol: $x(j) = \phi\big(v_1(j), v_2(j)\big)$ for all $j \in [n]$. For $j \in \Delta_2$, where Δ_2 is the set of partially-polarized indices defined in (5.13), the encoder records the realization of $u_2(j)$. These indices will be provided to the second receiver's decoder $\mathcal{D}_2$ as "genie-given" bits.

5.3.6 Broadcast Decoding Based on Polarization

5.3.6.1 Decoding At First Receiver

Decoder $\mathcal{D}_1$ decodes the binary sequence $\hat{u}_1^n$ using its observations y_1^n. The message W_1 is located at the indices $j \in \mathcal{M}_1^{(n)}$ in the sequence $\hat{u}_1^n$. More precisely, we define the following deterministic polar decoding function for the j-th bit:

$$\xi_{u_1}^{(j)}\left(u_1^{1:j-1}, y_1^n\right) \triangleq \arg\max_{u \in \{0,1\}} \left\{ \mathbb{P}\left(U_1(j) = u \middle| U_1^{1:j-1} = u_1^{1:j-1}, Y_1^n = y_1^n\right) \right\}. \tag{5.23}$$

Decoder $\mathcal{D}_1$ reconstructs $\hat{u}_1^n$ bit-by-bit successively as follows using the identical random mapping $\Psi_1^{(j)}$ at the encoder:

$$\hat{u}_1(j) = \begin{cases} \xi_{u_1}^{(j)}\big(\hat{u}_1^{1:j-1}, y_1^n\big), & \textit{if } j \in \mathcal{M}_1^{(n)}, \\ \Psi_1^{(j)}\big(\hat{u}_1^{1:j-1}\big), & \textit{otherwise.} \end{cases} \tag{5.24}$$

Given that all previous bits $\hat{u}_1^{1:j-1}$ have been decoded correctly, decoder $\mathcal{D}_1$ makes a mistake on the j-th bit $\hat{u}_1(j)$ only if $j \in \mathcal{M}_1^{(n)}$. For the remaining indices, the decoder produces the same bit produced at the encoder due to the shared random maps.

5.3.6.2 Decoding At Second Receiver

The decoder $\mathcal{D}_2$ decodes the binary sequence $\hat{u}_2^n$ using observations y_2^n. The message W_2 is located at the indices $j \in \mathcal{M}_2^{(n)}$ of the sequence $\hat{u}_2^n$. Define the following deterministic polar decoding functions

$$\xi_{u_2}^{(j)}\left(u_2^{1:j-1}, y_2^n\right) \triangleq \arg\max_{u\in\{0,1\}}\left\{\mathbb{P}\left(U_2(j)=u\middle|U_2^{1:j-1}=u_2^{1:j-1}, Y_2^n=y_2^n\right)\right\}. \tag{5.25}$$

Decoder $\mathcal{D}_2$ reconstructs $\hat{u}_2^n$ bit-by-bit successively as follows using the *identical* shared random mapping Γ used at the encoder. Including all but $o(n)$ of the indices,

$$\hat{u}_2(j) = \begin{cases} \xi_{u_2}^{(j)}\left(\hat{u}_2^{1:j-1}, y_2^n\right), & \text{if } j \in \mathcal{L}_{V_2|Y_2}^{(n)}, \\ \Gamma(j), & \text{if } j \in \mathcal{H}_{V_2|Y_2}^{(n)}. \end{cases} \tag{5.26}$$

For those indices $j \in \Delta_2$ where Δ_2 is the set of partially-polarized indices defined in (5.13), the decoder $\mathcal{D}_2$ is provided with "genie-given" bits from the encoder. Thus, all bits are decoded, and $\mathcal{D}_2$ only makes a successive cancelation error for those indices $j \in \mathcal{L}_{V_2|Y_2}^{(n)}$. Communicating the genie-given bits from the encoder to decoder results in a rate penalty. However, since the number of genie-given bits scales asymptotically as $o(n)$, the rate penalty can be made arbitrarily small.

Remark 16. *It is notable that decoder $\mathcal{D}_2$ reconstructs $\hat{u}_2^n$ using only the observations y_2^n. At the encoder, the sequence u_2^n was generated with the realization of a sequence v_1^n as given in (5.22). However, decoder $\mathcal{D}_2$ does* not *reconstruct the sequence $\hat{v}_1^n$. From this operational perspective, Marton's scheme differs crucially from Cover's superposition scheme because there does not exist the notion of a "stronger" receiver which reconstructs all the sequences decoded at the "weaker" receiver.*

5.3.7 Total Variation Bound

To analyze the average probability of error $P_e^{(n)}$, it is assumed that both the encoder and decoder share the *randomized* mappings $\Psi_1^{(j)}$, $\Psi_2^{(j)}$, and Γ (where $\Psi_2^{(j)}$ is not utilized at decoder $\mathcal{D}_2$). Define the following probability measure on the space of tuples of binary sequences.

$$Q\big(u_1^n, u_2^n\big) \triangleq Q\big(u_1^n\big)Q\big(u_1^n\big|u_2^n\big) = \prod_{j=1}^{n} Q\big(u_1(j)\big|u_1^{1:j-1}\big)Q\big(u_2(j)\big|u_2^{1:j-1}, u_1^n\big), \tag{5.27}$$

where the conditional probability measures are defined as

$$Q\Big(u_1(j)\Big|u_1^{1:j-1}\Big) \triangleq \begin{cases} \frac{1}{2}, & \text{if } j \in \mathcal{M}_1^{(n)}, \\ P\left(u_1(j)\Big|u_1^{1:j-1}\right), & \text{otherwise.} \end{cases}$$

$$Q\Big(u_2(j)\Big|u_2^{1:j-1}, u_1^n\Big) \triangleq \begin{cases} \frac{1}{2}, & \text{if } j \in \mathcal{H}_{V_2|V_1}^{(n)}, \\ P\left(u_2(j)\Big|u_2^{1:j-1}, u_1^n\right), & \text{otherwise.} \end{cases}$$

The probability measure Q defined in (5.27) is a perturbation of the joint probability measure $P_{U_1^n U_2^n}(u_1^n, u_2^n)$ in (5.6). The only difference in definition between P and Q is due to those indices in message sets $\mathcal{M}_1^{(n)}$ and $\mathcal{H}_{V_2|V_1}^{(n)}$ (note: $\mathcal{M}_2^{(n)} \subseteq \mathcal{H}_{V_2|V_1}^{(n)}$). The following lemma provides a bound on the total variation distance between P and Q. The lemma establishes the fact that inserting uniformly distributed message bits in the proper indices $\mathcal{M}_1^{(n)}$ and $\mathcal{M}_2^{(n)}$ (or the entire set $\mathcal{H}_{V_2|V_1}^{(n)}$) at the encoder *does not* perturb the statistics of the n-length random variables too much.

Lemma 15. *(*Total Variation Bound*) Let probability measures P and Q be defined as in* (5.6) *and* (5.27) *respectively. Let $0 < \beta < 1$. For sufficiently large n, the total variation distance between P and Q is bounded as*

$$\sum_{\substack{u_1^n \in \{0,1\}^n \\ u_2^n \in \{0,1\}^n}} \Big| P_{U_1^n U_2^n}(u_1^n, u_2^n) - Q(u_1^n, u_2^n) \Big| \leq 2^{-n^\beta}.$$

Proof. Omitted. The proof follows via the chain rule for KL-divergence and is identical to the previous proofs of Lemma 1 and Lemma 12. □

5.3.8 Error Sequences

The decoding protocols for $\mathcal{D}_1$ and $\mathcal{D}_2$ were established in Section 5.3.6. To analyze the probability of error of successive cancelation (SC) decoding, consider the sequences u_1^n and u_2^n formed at the encoder, and the resulting observations y_1^n and y_2^n received by the decoders. The effective polarized channel $P^{\phi}_{Y_1^n Y_2^n | U_1^n U_2^n}(y_1^n, y_2^n | u_1^n, u_2^n)$ was defined in (5.7) for a fixed ϕ function. It is convenient to group the sequences together and consider all tuples $(u_1^n, u_2^n, y_1^n, y_2^n)$.

Decoder $\mathcal{D}_1$ makes an SC decoding error on the j-th bit for the following tuples:

$$\begin{aligned} \mathcal{T}_1^j \triangleq \Big\{ & \big(u_1^n, u_2^n, y_1^n, y_2^n\big): \\ & P_{U_1^j | U_1^{1:j-1} Y_1^n}\big(u_1(j) \big| u_1^{1:j-1}, y_1^n\big) \leq \\ & P_{U_1^j | U_1^{1:j-1} Y_1^n}\big(u_1(j) \oplus 1 \big| u_1^{1:j-1}, y_1^n\big) \Big\}. \end{aligned} \tag{5.28}$$

The set $\mathcal{T}_1^j$ represents those tuples causing an error at $\mathcal{D}_1$ in the case $u_1(j)$ is inconsistent with respect to observations y_1^n and the decoding rule. Similarly, decoder $\mathcal{D}_2$ makes an SC decoding error on the j-th bit for the following tuples:

$$\begin{aligned}\mathcal{T}_2^j \triangleq \Big\{ &\big(u_1^n, u_2^n, y_1^n, y_2^n\big): \\ &P_{U_2\left|U_2^{1:j-1}Y_2^n\right.}\big(u_2\big|u_2^{1:j-1}, y_2^n\big) \leq \\ &P_{U_2\left|U_2^{1:j-1}Y_2^n\right.}\big(u_2 \oplus 1\big|u_2^{1:j-1}, y_2^n\big)\Big\}.\end{aligned}$$

The set $\mathcal{T}_2^j$ represents those tuples causing an error at $\mathcal{D}_2$ in the case $u_2(j)$ is inconsistent with respect to observations y_2^n and the decoding rule. The set of tuples causing an error is

$$\mathcal{T}_1 \triangleq \bigcup_{j \in \mathcal{M}_1^{(n)}} \mathcal{T}_1^j, \tag{5.29}$$

$$\mathcal{T}_2 \triangleq \bigcup_{j \in \mathcal{L}_{V_2|V_1}^{(n)}} \mathcal{T}_2^j, \tag{5.30}$$

$$\mathcal{T} \triangleq \mathcal{T}_1 \cup \mathcal{T}_2. \tag{5.31}$$

The goal is to show that the probability of choosing tuples of error sequences in the set $\mathcal{T}$ is small under the distribution induced by the broadcast code.

5.3.9 Average Error Probability

If the encoder and decoders share randomized maps $\Psi_1^{(j)}$, $\Psi_2^{(j)}$, and Γ, then the average probability of error is a random quantity determined as follows

$$\begin{aligned}P_e^{(n)}\left[\{\Psi_1^{(j)}, \Psi_2^{(j)}, \Gamma\}\right] = \sum_{\{u_1^n, u_2^n, y_1^n, y_2^n\} \in \mathcal{T}} \Bigg[& P^{\phi}_{Y_1^n Y_2^n\left|U_1^n U_2^n\right.}\big(y_1^n, y_2^n\big|u_1^n, u_2^n\big) \\ & \cdot \frac{1}{2^{nR_1}} \prod_{j \in [n]: j \notin \mathcal{M}_1^{(n)}} \mathbb{1}_{\left[\Psi_1^{(j)}\left(u_1^{1:j-1}\right) = u_1(j)\right]} \\ & \cdot \frac{1}{2^{nR_2}} \prod_{j \in \mathcal{H}_{V_2|V_1}^{(n)} \setminus \mathcal{M}_2^{(n)}} \mathbb{1}_{[\Gamma(j) = u_2(j)]} \\ & \cdot \prod_{j \in [n]: j \notin \mathcal{H}_{V_2|V_1}^{(n)}} \mathbb{1}_{\left[\Psi_2^{(j)}\left(u_2^{1:j-1}, u_1^n \mathbf{G}_n\right) = u_2(j)\right]} \Bigg].\end{aligned}$$

By averaging over the randomness in the encoders and decoders, the expected block error probability is upper bounded in the following lemma.

Lemma 16. *Consider the polarization-based Marton code described in Section 5.3.5 and Section 5.3.6. Let R_1 and R_2 be the broadcast rates selected according to the Bhattacharyya criterion given in Proposition 7. Then for $0 < \beta < 1$ and sufficiently large n,*

$$\mathbb{E}_{\{\Psi_1^{(j)},\Psi_2^{(j)},\Gamma\}}\left[P_e^{(n)}[\{\Psi_1^{(j)},\Psi_2^{(j)},\Gamma\}]\right] < 2^{-n^\beta}.$$

Proof. See Section 5.4 of the Appendices. □

If the average probability of block error decays to zero in expectation over the random maps $\{\Psi_1^{(j)}\}$, $\{\Psi_2^{(j)}\}$, and Γ, then there must exist at least one fixed set of maps for which $P_e^{(n)} \to 0$. Hence, polar codes for Marton's inner bound exist under suitable restrictions on distributions and they achieve reliable transmission according to the advertised rates (except for a small set of $o(n)$ polarization indices as is discussed next).

5.3.10 Rate Penalty Due to Partial Polarization

Lemma 16 is true assuming that decoder $\mathcal{D}_2$ obtains "genie-given" bits for the set of indices Δ_2 defined in (5.13). The set Δ_2 represents those indices that are partially-polarized and which cause a slight misalignment of polarization indices in the Marton scheme. Fortunately, the set Δ_2 contains a vanishing fraction of indices: $\frac{1}{n}\left|\Delta_2\right| \leq \eta$ for $\eta > 0$ arbitrarily small and n sufficiently large. Therefore, a two-phase strategy suffices for sending the "genie-given" bits. In the first phase of communication, the encoder sends several n-length blocks while decoder $\mathcal{D}_2$ waits to decode. After accumulating several blocks of output sequences, the encoder transmits all the known bits in the set Δ_2 for all the first-phase transmissions. The encoder and decoder can use any reliable point-to-point polar code with non-vanishing rate for communication. Having received the "genie-aided" bits in the second-phase, the second receiver then decodes all the first-phase blocks. The number of blocks sent in the first-phase is $\mathcal{O}(\frac{1}{\eta})$. The rate penalty is $\mathcal{O}(\eta)$ where η can be made arbitrarily small. A similar argument was provided in [54] for designing polar codes for the Gelfand-Pinsker problem.

5.3.11 Concluding Remarks

Coding for broadcast channels is fundamental to our understanding of communication systems. Broadcast codes based on polarization methods achieve rates on the capacity boundary for several classes of DM-BCs. In the case of m-user deterministic DM-BCs, polarization of random variables from the channel output provides the ability to extract uniformly random message bits while maintaining broadcast constraints at the encoder. As referenced in the literature, maintaining multi-user constraints for the DM-BC is a difficult task for traditional belief propagation algorithms and LDPC codes.

For two-user noisy DM-BCs, polar codes were designed based on Marton's coding strategy and Cover's superposition strategy. Constraints on auxiliary and input distributions were

placed in both cases to ensure alignment of polarization indices in the multi-user setting. The asymptotic behavior of the average error probability was shown to be $P_e^{(n)} = \mathcal{O}(2^{-n^\beta})$ with an encoding and decoding complexity of $\mathcal{O}(n \log n)$. Recent simulations have supplemented the theory with experimental evidence of the error-correcting capability of polar codes over simulated channels for finite code lengths. The results demonstrate that polar codes have a potential for use in several *network communication* scenarios.

5.4 Bounding the Probability of Error

To prove Lemma 16, the expectation of the average probability of error of the polarization-based Marton code is written as

$$\begin{aligned}
&\mathbb{E}_{\{\Psi_1^{(j)},\Psi_2^{(j)},\Gamma\}}\Big[P_e^{(n)}[\{\Psi_1^{(j)},\Psi_2^{(j)},\Gamma\}]\Big] = \\
&\quad \sum_{\{u_1^n,u_2^n,y_1^n,y_2^n\}\in\mathcal{T}} \Bigg[P^{\phi}_{Y_1^nY_2^n\left|U_1^nU_2^n\right.}\left(y_1^n,y_2^n\middle|u_1^n,u_2^n\right) \\
&\quad \cdot \frac{1}{2^{nR_1}} \prod_{j\in[n]:j\notin\mathcal{M}_1^{(n)}} \mathbb{P}\Big\{\Psi_1^{(j)}\left(u_1^{1:j-1}\right) = u_1(j)\Big\} \\
&\quad \cdot \frac{1}{2^{nR_2}} \prod_{j\in\mathcal{H}_{V_2|V_1}^{(n)}\setminus\mathcal{M}_2^{(n)}} \mathbb{P}\Big\{\Gamma(j) = u_2(j)\Big\} \\
&\quad \cdot \prod_{j\in[n]:j\notin\mathcal{H}_{V_2|V_1}^{(n)}} \mathbb{P}\Big\{\Psi_2^{(j)}\left(u_2^{1:j-1}, u_1^n\mathbf{G}_n\right) = u_2(j)\Big\}\Bigg].
\end{aligned}$$

The expression is then simplified by substituting the definition of $Q(u_1^n, u_2^n)$ provided in (5.27), and then splitting the error term into two parts:

$$\begin{aligned}
&\mathbb{E}_{\{\Psi_1^{(j)},\Psi_2^{(j)},\Gamma\}}\Big[P_e^{(n)}[\{\Psi_1^{(j)},\Psi_2^{(j)},\Gamma\}]\Big] = \\
&\quad \sum_{\{u_1^n,u_2^n,y_1^n,y_2^n\}\in\mathcal{T}} \left[P^{\phi}_{Y_1^nY_2^n\left|U_1^nU_2^n\right.}\left(y_1^n,y_2^n\middle|u_1^n,u_2^n\right) Q(u_1^n,u_2^n)\right], \\
&\quad \leq \left[\sum_{\{u_1^n,u_2^n,y_1^n,y_2^n\}\in\mathcal{T}} P_{U_1^nU_2^nY_1^nY_2^n}\left(u_1^n,u_2^n,y_1^n,y_2^n\right)\right] \\
&\qquad + \left[\sum_{\substack{u_1^n\in\{0,1\}^n \\ u_2^n\in\{0,1\}^n}} \left| P_{U_1^nU_2^n}\left(u_1^n,u_2^n\right) - Q\left(u_1^n,u_2^n\right)\right|\right].
\end{aligned}$$

The error term pertaining to the total variation distance was already upper bounded as in Lemma 15. The error due to successive cancelation decoding at the receivers is upper

bounded as follows.

$$\begin{aligned}
\mathcal{E} &\triangleq \sum_{\{u_1^n, u_2^n, y_1^n, y_2^n\} \in \mathcal{T}} P_{U_1^n U_2^n Y_1^n Y_2^n}\left(u_1^n, u_2^n, y_1^n, y_2^n\right) \\
&\leq \sum_{j \in \mathcal{M}_1^{(n)}} Z\left(U_1^j \middle| U_1^{1:j-1}, Y_1^n\right) + \sum_{j \in \mathcal{L}_{V_2|Y_2}^{(n)}} Z\left(U_2^j \middle| U_2^{1:j-1}, Y_2^n\right), \\
&\leq \delta_n \left[\left| \mathcal{M}_1^{(n)} \right| + \left| \mathcal{L}_{V_2|Y_2}^{(n)} \right| \right] \\
&\leq 2n\delta_n.
\end{aligned}$$

This concludes the proof demonstrating that the expectation of the average probability of block error is upper bounded as $\mathcal{O}(2^{-n^\beta})$.

Part II

Communication and Computation in Networks

Chapter 6

Network Coding and Network Computing

6.1 Overview of Literature

Recently coding for computation in networks has received considerable attention with applications in sensor networks [38] and cloud computing scenarios [26, 27]. In a sensor network, a fusion node may be interested in computing a relevant function of the measurements from various data nodes. In a cloud computing scenario, a client may download a function or part of the original source information that is distributed (e.g. using a maximum distance separable code) across multiple data nodes.

The simplest setting for computation in networks consists of multiple sources transmitting information to a single receiver which computes a function of the original sources. Appuswamy et al. study the fundamental limits of computation for linear and general target function classes for single receiver networks [5]. The problem of linear function computation in single-receiver networks has been solved in part due to a duality theorem establishing an equivalence to the classical problem of communication with multi-cast demands [3]. In the classical multi-cast setting, cut-set bounds provide tight limits on communication. Similar cut-set bounds may be given for computation in single-receiver networks.

Several results over the past decade have contributed to the understanding of classical communication in multi-cast networks. In a multi-cast network, raw messages are transmitted to a set of receivers with identical message demands. The celebrated work of Ahlswede et al. [3] established that the cut-set bound is tight for multicast communication. Subsequent research developed practical linear network coding strategies ranging from random linear codes to deterministic polynomial-time code constructions [59, 53, 47, 49]. The success of traditional multi-cast communication motivates us to explore the fundamental limits of multi-casting a linear function in *multi-receiver* networks as a natural next step. For this open problem, some facts are known based on special examples: (a) Random codes are insufficient in achieving capacity limits, and structured codes achieve higher computation

rates [67]; (b) Linear codes are insufficient in general for computation over multi-receiver networks (cf. both [74] and [29]) and non-linear codes may achieve higher computation rates.

To make progress on the problem of multicasting a function in multi-receiver networks, we consider the simplest two transmitter two-receiver network in which both receivers compute a linear function (modulo-2 sum) of two independent Bernoulli sources generated at the transmitters. Specifically, we consider the Avestimehr-Diggavi-Tse (ADT) deterministic single-hop network model [10] which captures superposition and broadcast properties of wireless Gaussian networks and is a generalization of networks of orthogonal links. We develop a new achievable coding scheme termed function alignment, inspired by the concept of interference alignment [60, 18]. We also derive a new converse theorem that is tighter than cut-set based bounds and genie-aided bounds. As a consequence of this capacity result, we find that unlike the single-receiver case, the cut-set based bound is not achieved due to competition for shared network resources that arise in satisfying function demands at multiple receivers. As a byproduct of our analysis, we develop a network decomposition theorem to identify elementary parallel subnetworks that can constitute an original network without loss of optimality for in-network computation. The network decomposition approach offers a conceptually simpler proof for an achievable code and extends to L-transmitter L-receiver symmetric single-hop networks. In addition, the design of structured computation codes using network decomposition could be applicable in multi-hop networks.

In [76, 75, 74], the computing capacity for multi-casting a sum of sources is explored for arbitrary multiple-source multiple-destination networks. It is shown that there exists a linearly solvable and equivalent sum-network for any multiple-unicast network and vice-versa. The authors characterized necessary and sufficient conditions for communicating sums of sources of two-source L-destination (or L-source two-destination) networks, when the entropy of each source is limited by 1. On the other hand, our work considers sources without entropy constraints and establishes the exact capacity of a particular multi-receiver network which is a generalization of traditional network coding models with orthogonal links.

Renewed interest in network coding has emerged recently due to the intimate connection between *wireless information flow* and wired networks. Due to [10], specific deterministic models closely approximate Gaussian channels and networks in the limit of high signal-to-noise ratios. Further connections between wireless communication and network coding were made in [68] where the compute-and-forward framework was introduced for multi-hop networks in which relay nodes reliably compute and forward functions of messages. Computation alignment over real vector spaces within the compute-and-forward framework was introduced in [69].

6.2 A Simple Multiple-Unicast Network

Before the study of network computation, it is instructive to understand a simple multiple-unicast network for which the cut-set bound is not tight. The cut-set bound is motivated

by a network's graph representation. Why is it not tight in certain cases? An informal answer could be that the *mixing* of disparate information in bottleneck, shared paths causes the graph-theoretic notion to break-down both for communication and computation. While graph-theoretic upper bounds on information transmission are desirable, often it is not easily possible and new information-theoretic upper bounds must be specified. The following lemma introduces a three-node example which inspired Kramer and Savari to develop new edge-cut bounds in [58].

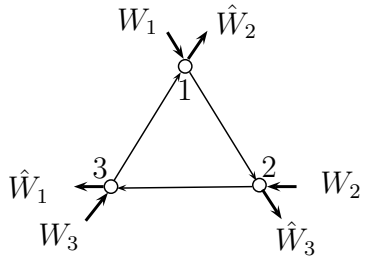


Figure 6.1: A directed cyclic network with multiple-unicast demands.

Lemma 17 (Capacity Region of a Multi-Hop Network)**.** *Consider the network depicted in Figure 6.1. Assume unit capacities for the noiseless links. The capacity region is given by*

$$\Big\{(R_1, R_2, R_3) \in \mathbb{R}_3^+ \;\Big|\; R_i + R_j \leq 1, i \neq j\Big\}. \tag{6.1}$$

Remark 17. *It is interesting to note that the cut-set bound is not tight for this communication network with multiple-unicast demands. The cut-set bound is* $0 \leq R_i \leq 1$ *for* $i \in \{1, 2, 3\}$.

Proof. The achievable code is self-evident because each transmitter may send 1 bit to its respective receiver if all other transmitters are silent. Time-sharing establishes the achievable

region. The first steps of the converse proof below are due to Fano's inequality.

$$\begin{aligned}
&N(R_1+R_2)\\
&= H(W_1)+H(W_2)\\
&\le I(W_1;X_{23}^N,W_3)+I(W_2;X_{31}^N,W_1)+N\epsilon_{1,N}+N\epsilon_{2,N}\\
&\le I(W_1;X_{23}^N,W_3)+I(W_2;X_{23}^N,X_{31}^N,W_1,W_3)+N\epsilon_{1,N}+N\epsilon_{2,N}\\
&= I(W_1;X_{23}^N,W_3)+I(W_2;X_{23}^N,W_1,W_3)+N\epsilon_{1,N}+N\epsilon_{2,N}\\
&= I(W_1;X_{23}^N \mid W_3)+I(W_2;X_{23}^N,W_1 \mid W_3)+N\epsilon_{1,N}+N\epsilon_{2,N}\\
&= I(W_1,W_2;X_{23}^N \mid W_3)+N\epsilon_{1,N}+N\epsilon_{2,N}\\
&= H(X_{23}^N \mid W_3)-H(X_{23}^N \mid W_1,W_2,W_3)+N\epsilon_{1,N}+N\epsilon_{2,N}\\
&= H(X_{23}^N \mid W_3)+N\epsilon_{1,N}+N\epsilon_{2,N}\\
&\le \sum_{i=1}^{N} H(X_{23}^{(i)})+N\epsilon_{1,N}+N\epsilon_{2,N}\\
&\le N+N\epsilon_{1,N}+N\epsilon_{2,N}.
\end{aligned}$$

Therefore, $R_1+R_2 \le 1+\epsilon_{1,N}+\epsilon_{2,N}$ where $\epsilon_{1,N}\to 0$ and $\epsilon_{2,N}\to 0$ as $N\to\infty$. By symmetry, we obtain all the upper bounds of Eqn. (6.1). In the above derivation, $I(W_2;X_{23}^N,X_{31}^N,W_1,W_3)$ is equivalent to $I(W_2;X_{23}^N,W_1,W_3)$ because X_{31}^N is a function of W_3 and X_{23}^N. In addition, $H(X_{23}^N \mid W_1,W_2,W_3)$ is zero because all transmissions are functions of the original messages. □

6.3 Network Computing Model

As discovered in the literature, function computation in networks is closely related to communication with multiple-unicast demands. In the following definitions, a single-hop network model is introduced for network computing which encapsulates many of the challenges associated with coding in multiple-unicast networks. For most of this chapter, an $L=2$ user model is assumed, where L is the number of transmitter-receiver pairs. Figure 6.2 illustrates the network model.

Definition 17 (Source Symbols)**.** *Each transmitter $\ell\in[L]$ observes source symbols S_ℓ^K in which each symbol $S_{\ell,k}$ for $k\in[K]$ is drawn uniformly from a finite field $\mathbb{F}_2$. Thus the source distribution is Bernoulli($\frac{1}{2}$).*

Definition 18 (Encoders)**.** *Let $\ell\in[L]$, $j\in[N]$, and $q>0$ be a positive integer. Transmitter ℓ uses encoder $\mathcal{E}_\ell^{(N)}$ to map its message S_ℓ^K to a length-N codeword X_ℓ^N where $X_\ell[j]\in\mathbb{F}_2^{q\times 1}$ is the channel input vector for the j^{th} channel use. The mapping over N channel uses is*

$$\mathcal{E}_\ell^{(N)}:\mathbb{F}_2^K\to\mathbb{F}_2^{q\times N}.$$

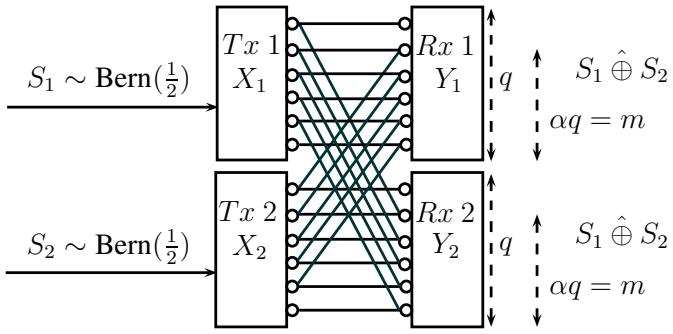


Figure 6.2: A symmetric network computing model with parameters $(m, q, L) = (5, 6, 2)$.

Definition 19 (Channel Model)**.** *The channel model is a discrete memoryless model. Transmitter $\ell \in [L]$ transmits input $X_\ell[j] \in \mathbb{F}_2^{q\times 1}$ in the j^{th} time slot where $j \in [N]$. The channel output for receiver $\ell \in [L]$ is given by $Y_\ell[j] \in \mathbb{F}_2^{q\times 1}$. The input-output relationship is defined by,*

$$Y_\ell[j] = X_\ell[j] \oplus \bigoplus_{\ell' \in [L], \ell' \neq \ell} \mathbf{G}^{q-m} X_{\ell'}[j]. \tag{6.2}$$

The channel matrix is a downshift *matrix characterized by kernel $\mathbf{G} \in \mathbb{F}_2^{q\times q}$ containing entries $[\mathbf{G}]_{st} = \mathbb{1}_{[s=t+1]}$ for $0 \leq s \leq q$ and $0 \leq t \leq q$. It will be convenient to define the ratio parameter $\alpha \triangleq \frac{m}{q}$ which is a rational number for $m \in \mathbb{Z}^+$. Each network is compactly identified by parameters (m, q, L).*

Example 6. *The channel model corresponds to a class of symmetric linear deterministic models.*[1] *The channel model includes* broadcast and superposition *which allows the possibility for* in-network *computation. Figure 6.2 illustrates a model with parameters $(m, q, L) = (5, 6, 2)$ and $\alpha = \frac{5}{6}$.*

Definition 20 (Decoders)**.** *Each receiver $\ell \in [L]$ observes channel output vectors $\{Y_\ell[j]\}_{j=1}^N$ over N channel uses. The goal for all receivers is to reconstruct the identical modulus function $\bigoplus_{\ell=1}^L S_\ell^K$ using a decoder $\mathcal{D}_\ell^N$:*

$$\mathcal{D}_\ell^{(N)} : \mathbb{F}_2^{q\times N} \to \mathbb{F}_2^K.$$

Definition 21 (Computation Rate)**.** *A computation rate*

$$R_{\text{COMP}} = \frac{K}{N}$$

[1]Several related types of linear deterministic channels have been studied as approximations to Gaussian channels and networks; see [10] for an overview and further references.

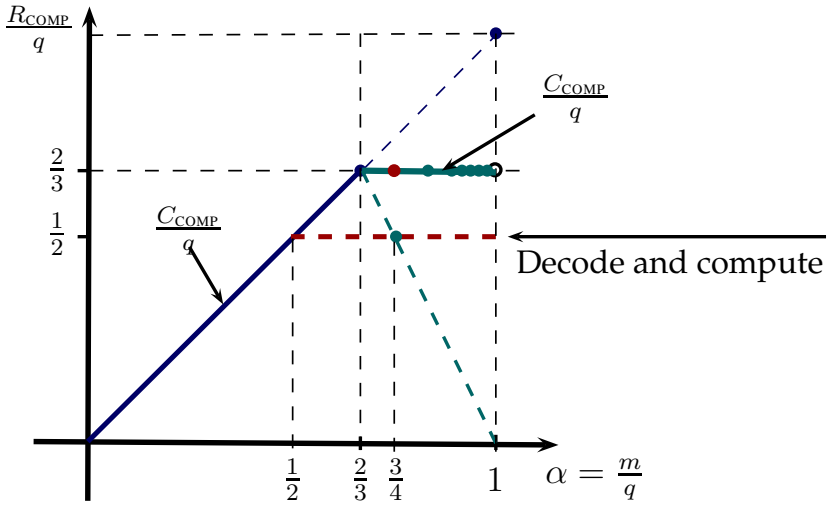


Figure 6.3: The computation capacity region for a countably infinite class of networks parameterized by $\alpha \triangleq \frac{m}{q}$ with $L = 2$ transmitters and receivers.

is achievable *in a network if all receivers reliably compute the modulus sum of source symbols, i.e. if for any $\epsilon > 0$ and block length N large enough, there exist encoders $\mathcal{E}_\ell^{(N)}$ and decoders $\mathcal{D}_\ell^{(N)}$ such that $\mathbb{P}\left(\mathcal{D}_\ell(Y_\ell^N) \neq \bigoplus_{\ell=1}^L S_\ell^K\right) \leq \epsilon$ for all $\ell \in [L]$.*

Definition 22 (Computation Capacity)**.** *The* computation capacity C_{COMP} *is the supremum of the achievable rates.*

Definition 23 (Zero-Error Linear Coding Capacity for Computation)**.** *The* zero-error *network coding capacity for computing the modulus sum function is defined as*

$$C_{\text{COMP}}^{\text{ZE}} = \sup\left\{\frac{K}{N} : \exists(K,N) \text{ code that computes the } \bigoplus\text{-function with zero error.}\right\}$$

A code computes the modulus sum function with zero-error if for all $\ell \in [L]$, there exist encoders $\mathcal{E}_\ell^{(N)}$ and decoders $\mathcal{D}_\ell^{(N)}$ such that $\mathcal{D}_\ell(Y_\ell^N) = \bigoplus_{\ell=1}^L S_\ell^K$ with zero probability of error. The linear coding capacity for computation $C_{\text{COMP}}^{\text{LIN}}$ is defined as the zero-error network coding capacity under the restriction that encoders $\mathcal{E}_\ell^{(N)}$ and decoders $\mathcal{D}_\ell^{(N)}$ are linear mappings.

6.4 Computation Capacity Region

Theorem 5 (Capacity Region [41, 87])**.** *Consider a network model with parameters* $(m, q, L = 2)$ *and* $\alpha \triangleq \frac{m}{q}$*. The normalized computation capacity is*

$$\frac{C_{\text{COMP}}}{q} = \begin{cases} \alpha & \text{if } 0 \le \alpha \le \frac{2}{3}, \quad (6.3a) \\ \frac{2}{3} & \text{if } \frac{2}{3} < \alpha < 1, \quad (6.3b) \\ 1 & \text{if } \alpha = 1. \quad (6.3c) \end{cases}$$

In the regime $\frac{2}{3} < \alpha < 1$, vector linear coding achieves higher computation rates than scalar linear coding.

Corollary 1 (Limiting Capacity)**.** *As established by Theorem 5, there exists a discontinuity at* $\alpha = 1$*. For a sequence of networks with* α *increasing to* 1 *(but strictly less than* 1*), the computation capacity is limited by* $\frac{2}{3}$*. In the case* $\alpha = 1$ *exactly, the computation capacity is exactly* 1*. Figure 6.3 illustrates the capacity region.*

6.4.1 Scalar vs. Vector Linear Coding

A basic coding strategy at each receiver is to first decode both sources S_1^K and S_2^K separately, and then compute the function. The multi-cast capacity for transmitting both messages to both receivers for an $(m, q, L = 2)$ network is given by $R_1 \le m$, $R_2 \le m$, and $R_1 + R_2 \le q$. Therefore, a lower bound on the computation rate is $R_{\text{COMP}} \ge \min\{m, \frac{q}{2}\}$ which yields

$$\frac{R_{\text{COMP}}}{q} \ge \min\left\{\alpha, \frac{1}{2}\right\}. \quad (6.4)$$

Decoding both messages provides the optimal coding strategy for $0 \le \alpha \le \frac{1}{2}$. In order to achieve higher computation rates, the *channel structure* must be exploited for *in-network* computation. Both scalar and vector linear codes are necessary.

In the regime $\frac{1}{2} \le \alpha \le \frac{2}{3}$, a scalar linear code suffices, and the code construction is provided in Fig. 6.4. For the figure, we introduce the notation $a_k \triangleq S_{1,k}$ and $b_k \triangleq S_{2,k}$ for $k \in [K]$ to represent the source symbols of the first and second transmitter respectively. The specific example is for the $(3, 5)$ model. The channel structure is exploited to compute the $\bigoplus_2$-function of message bits.

As will be derived in the next section, coding over N channel uses of the network for the (m, q, L) model is equivalent to coding over one channel use of the (mN, qN, L) model. In this case, vector linear coding over $\mathbb{F}_2$ may be characterized by beam-forming vectors

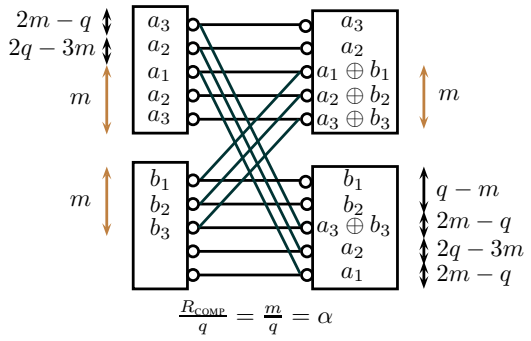


Figure 6.4: Scalar linear code construction for $(m, q, L = 2)$ networks in the regime $\frac{1}{2} \leq \alpha \leq \frac{2}{3}$.

$\mathbf{v}_{1,k} \in \mathbb{F}_2^{qN}$ and $\mathbf{v}_{2,k} \in \mathbb{F}_2^{qN}$ for $k \in [K]$ such that

$$\tilde{X}_1 = \bigoplus_{k=1}^{K} a_k \mathbf{v}_{1,k},$$
$$\tilde{X}_2 = \bigoplus_{k=1}^{K} b_k \mathbf{v}_{2,k}.$$

Here the modified network inputs $\tilde{X}_1, \tilde{X}_2 \in \mathbb{F}_2^{qN}$ represent coding over N channel uses. The code construction consists of designing all beam-forming vectors at the transmitters so that the receivers may recover the computations $a_k \oplus b_k$ for all $k \in [K]$.

6.5 Network Decomposition Into Parallel Models

For general (m, q, L) computing models, we develop a network decomposition theorem which identifies elementary subnetworks such that the computation capacity of the subnetworks is the same as the computation capacity of the original network. This theorem identifies fundamental building blocks that can constitute an original network without loss of optimality, thus establishing a *separation principle* among the building blocks. The theorem also encompasses L-transmitter L-receiver symmetric networks, thus serving to establish the linear coding capacity for computing in a generalized network.

Theorem 6 (Network Decomposition)**.** *Consider an (m, q, L) network where $m \neq q$. The following network decompositions hold:*[2]

[2]The symbol $\times$ denotes the concatenation of orthogonal models as by analogy to the mathematical notation $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

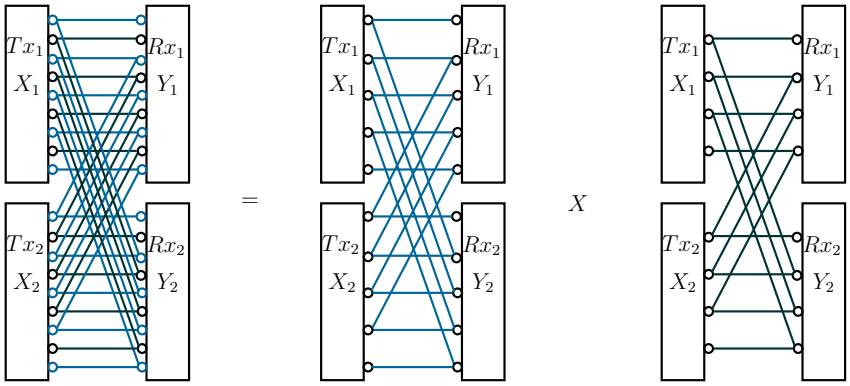


Figure 6.5: Network decomposition of the $(m, q, L) = (7, 9, 2)$ model into parallel models.

(1) *For any* $\lambda \in \mathbb{Z}^+$,

$$(\lambda m, \lambda q, L) = (m, q, L)^{\lambda} = (m, q, L) \times (m, q, L) \times \ldots \times (m, q, L).$$

(2) $(2m + 1, 2q + 1, L) = (m, q, L) \times (m + 1, q + 1, L)$

(3) *For arbitrary* (m, q, L) *models,*

$$(m, q, L) = \begin{cases} (r, r+1, L)^{q-m-a} \times (r+1, r+2, L)^{a}, & m < q; \\ (r+1, r, L)^{m-q-a} \times (r+2, r+1, L)^{a}, & m > q. \end{cases} \tag{6.5}$$

where

$$\begin{aligned} r &= \left\lfloor \frac{\min\{m, q\}}{|q - m|} \right\rfloor, \\ a &= \min\{m, q\} \mod |q - m|. \end{aligned} \tag{6.6}$$

Example 7. *The following* (m, q, L) *network decompositions into orthogonal components hold as examples:* $(7, 9, 2) = (3, 4, 2) \times (4, 5, 2)$ *and* $(17, 21, 2) = (8, 10, 2) \times (9, 11, 2) = (4, 5, 2)^3 \times (5, 6, 2)$. *In Figure 6.5, an example is provided for the* $(7, 9, 2)$ *model. As established in Theorem 6, the idea is to use graph coloring with* $|q - m| = 2$ *colors. The colors separate the original network into two parallel "gap-1" models.*

Remark 18. *Unlike the* $L = 2$ *case, for* $L \geq 3$, *the case* $m < n$ *is not symmetric with* $m > n$. *Nevertheless, the above symmetric decomposition holds even when* $L \geq 3$. □

Remark 19. *The separation principle among these decomposed subnetworks is not generally true. It is well known that for parallel interference channels, the optimal performance can be attained by coding over orthogonal components.* □

6.5.1 Proof of Theorem 6

For Part *(1)*, consider the $(\lambda m, \lambda q, L)$ model. The proof uses graph coloring with λ colors, identified by integers $\{0, 1, \ldots, \lambda - 1\}$. At transmitter 1, assign to level p (for $p = 1, 2, \ldots, \lambda \max(m, q)$) the color $(p-1) \mod \lambda$. Use exactly the same rule to color the vertices of receiver 1 as well as the transmitters and receivers of the remaining $(L-1)$ users. It is seen by inspection that each color represents an independent graph. Moreover, each color represents precisely an (m, q, L) model.

For Part *(2)*, graph coloring with two colors suffices. At all transmitters and receivers, assign one color to the even-numbered levels and the other color to the odd-numbered levels. By inspection, it can be verified that each color represents an independent graph. Moreover, one color represents an (m, q, L) model and the other represents an $(m+1, q+1, L)$ model.

For Part *(3)*, we use graph coloring with $|q-m|$ colors, identified by integers $\{0, 1, \ldots, |q-m| - 1\}$. At transmitter 1, assign to level p (for $p = 1, 2, \ldots, \max(m, q)$) the color $(p-1) \mod |q-m|$. Use exactly the same rule to color the levels of receiver 1 as well as the transmitters and receivers of the remaining $(L-1)$ users. It is seen by inspection that each color represents an independent graph. A tedious but straightforward calculation shows that of the resulting $|q-m|$ independent graphs, there are a number of models $(r+1, r+2)$ and $q-m-a$ number of models $(r, r+1)$, with the claimed values for r and a.

6.6 Function Alignment

In the regime $\frac{2}{3} \leq \alpha < 1$, vector linear codes are necessary to achieve the computation capacity. In this regime, linear codes achieve $\frac{R_{\text{COMP}}}{q} = \frac{2}{3}$. Due to Theorem 6, an arbitrary network is decomposed into "gap-1" models. Surprisingly, it suffices to consider separate coding over the "gap-1" parallel models.

Theorem 7 (Computation Rate in "Gap-1" Models)**.** *In any "gap-1" model defined by* $(m, q, L) = (r, r+1, 2)$ *with* $r \geq 2$*, the computation rate achieved by linear codes is* $\frac{R_{\text{COMP}}}{q} \geq \frac{2}{3}$.

Proof. We prove Theorem 7 by classifying network models $(r, r+1)$ with $r \geq 2$ into three different cases:

1. $(r+1) \mod 3 = 0$.
2. $(r+1) \mod 3 = 1$.
3. $(r+1) \mod 3 = 2$.

Each of these three cases is proved separately in the following sections.

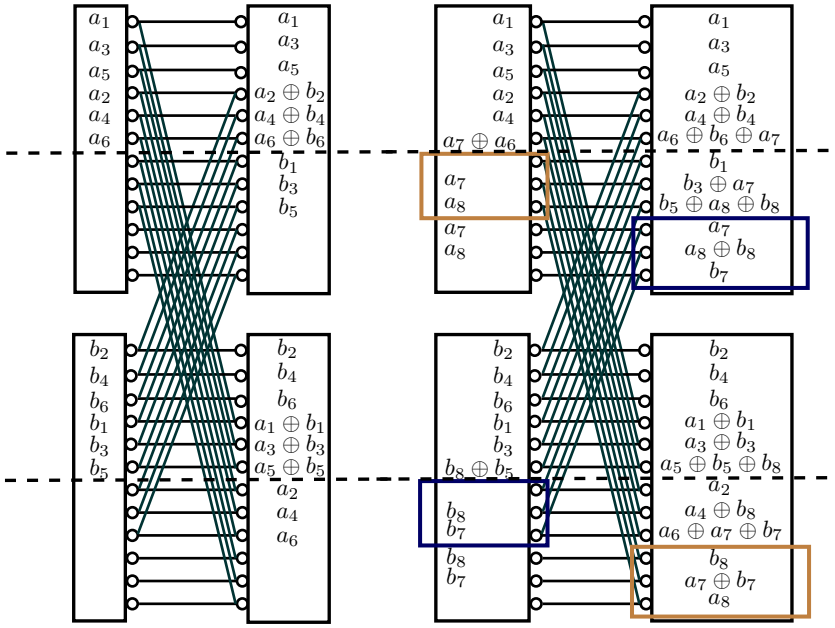


Figure 6.6: Scalar linear code for the $(m, q, L) = (9, 12, 2)$ model and vector linear code over $N = 3$ channel uses of the $(3, 4, 2)$ model.

6.6.1 The Case of $(r + 1)$ mod $3 = 0$

For these networks, e.g. $(2, 3)$, $(5, 6)$, $(8, 9)$, $(11, 12)$, only scalar network coding is necessary. For $r = 2$, an explicit code is as follows: $X_{1,1} = a_1, X_{1,2} = a_2, X_{1,3} = 0$ and $X_{2,1} = b_2, X_{2,2} = b_1, X_{2,3} = 0$. It is straightforward to verify that both receivers can reconstruct $a_1 \oplus b_1$ and $a_2 \oplus b_2$, hence, a computation rate of 2 is attained. For the general case, we set $X_{1,3k-2} = a_{2k-1}, X_{1,3k-1} = a_{2k}, X_{1,3k} = 0$ and $X_{2,3k-2} = b_{2k}, X_{2,3k-1} = b_{2k-1}, X_{2,3k} = 0$, for $k = 1, 2, \ldots, p$, where $p \triangleq \frac{(r+1)}{3}$. Each receiver can reconstruct all $2p$ sums $a_k \oplus b_k$ and thus, the computation rate is $2p = \frac{2}{3}(r + 1)$.

6.6.2 The Case of $(r + 1)$ mod $3 = 1$

For these networks, e.g. $(3, 4)$, $(6, 7)$, $(9, 10)$, $(12, 13)$, vector network coding is necessary and we show that $N = 3$ channel uses is sufficient. Consider first the "indecomposable" model $(3, 4)$ as an example. Figure 6.6 provides one linear code over $N = 3$ channel uses which achieves a normalized computation rate of $\frac{2}{3}$. A total of 8 computations $a_k \oplus b_k$ are extracted at *both* receivers using only $N(r + 1) = 12$ transmitted symbols.

For general network models in this class, we construct a vector linear code over $N = 3$ channel uses. It is observed (via network equivalences) that vector coding with $N = 3$ for an $(r, r + 1)$ model is identical to scalar linear coding over the model $(3r, 3(r + 1))$. As an

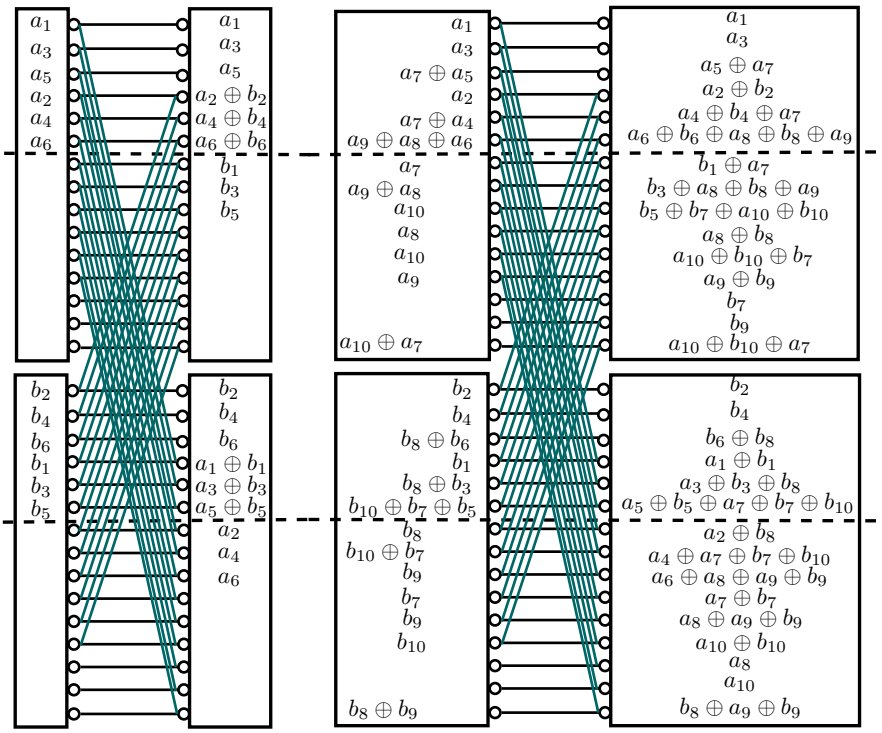


Figure 6.7: Scalar linear code for the $(m, q, L) = (12, 15, 2)$ model and vector linear code over $N = 3$ channel uses of the $(4, 5, 2)$ model.

example, vector coding with $N = 3$ for the model $(6, 7)$ is equivalent to scalar linear coding for the model $(18, 21)$. We now show that linear code construction for the $(18, 21)$ model follows in a straightforward manner from the achievable strategies already presented. On the left side of Figure 6.6, we observe that 6 computations are achieved over a total of 9 dimensions at both receivers. Subtracting these 9 dimensions completely from the $(18, 21)$ model exactly "resets" the network model to a $(9, 12)$ model for which we know that using the code construction given in Figure 6.6, as many as 8 computations are possible. Thus, a total of $8 + 6$ computations are possible in the $(18, 21)$ model which yields the normalized rate $\frac{2}{3}$ for computation. The discussed approach generalizes to all network models of this class.

Example 8. *Figure 6.6 illustrates a code achieving the optimal computation rate* $\frac{R_{comp}}{L} = \frac{8}{12} = \frac{2}{3}$ *for the* $(m, q, L) = (3, 4, 2)$ *model made possible by* computation alignment. *On the left, a total of* 6 *computation bits are possible using alternating computation alignment. On the right,* 2 *more computation bits for both receivers are possible due to careful alignment of encoding vectors within the received dimensions.*

6.6.3 The Case of $(r+1)$ mod $3 = 2$

For these networks, e.g. $(4,5)$, $(7,8)$, $(10,11)$, $(13,14)$, vector network coding is again necessary over $N = 3$ channel uses. The code for the "indecomposable" $(4,5)$ model is provided in Figure 6.7. For other models in this series, we repeat our reasoning. As an example, vector coding with $N = 3$ for the model $(7,8)$ is equivalent to scalar linear coding for the $(21,24)$ model. The $(21,24)$ model is first "reset" by subtracting out 9 dimensions (achieving 6 computations), resulting in a $(12,15)$ model which is equivalent to coding for the $(4,5)$ model over $N = 3$ channel uses. Similarly, all network models of this class are "reset" to yield the indecomposable $(4,5)$ model.

Example 9. *Figure 6.7 illustrates a code achieving the optimal computation rate* $\frac{R_{comp}}{L} = \frac{10}{15} = \frac{2}{3}$ *for the* $(m,q,L) = (4,5,2)$ *model. On the left, a total of* 6 *computation bits are possible using alternating* computation alignment*. On the right,* 4 *more computation bits for both receivers are possible due to careful alignment of encoding vectors within the received dimensions.*

□

6.7 Linear Coding Upper Bound

Theorem 8 (Linear Coding Upper Bound)**.** *Let* m, n, q *be integers such that* $0 < m \leq n$ *and* $q \geq n$*. Consider a network defined by input* $X_1, X_2 \in \mathbb{F}_2^q$*, output* $Y_1, Y_2 \in \mathbb{F}_2^q$*, and transfer function*

$$Y_1 = \mathbf{G}^{q-n} X_1 \oplus \mathbf{G}^{q-m} X_2,$$
$$Y_2 = \mathbf{G}^{q-m} X_1 \oplus \mathbf{G}^{q-n} X_2,$$

where shift-matrix $\mathbf{G} \in \mathbb{F}_2^{q \times q}$ *is defined by* $[\mathbf{G}]_{ij} = \mathbb{1}_{[i=j+1]}$ *for* $0 \leq i \leq q$ *and* $0 \leq j \leq q$*. Let* K *be the number of computations recovered by each receiver separately. Then over* N *uses of the network, the linear computation capacity of the network is bounded by the following two inequalities,*

$$K \leq mN, \tag{6.7}$$
$$3K \leq 2qN. \tag{6.8}$$

Proof. Let $\mathbf{H} \in \mathbb{F}_2^{qN \times qN}$ be defined by $[\mathbf{H}]_{ij} = \mathbb{1}_{[i=j+1]}$ where $0 \leq i \leq qN$ and $0 \leq j \leq qN$. A key observation is that coding over N uses of the described network is equivalent to coding over a single use of the following shift network

$$\tilde{Y}_1 = \mathbf{H}^{N(q-n)} \tilde{X}_1 \oplus \mathbf{H}^{N(q-m)} \tilde{X}_2, \tag{6.9}$$
$$\tilde{Y}_2 = \mathbf{H}^{N(q-m)} \tilde{X}_1 \oplus \mathbf{H}^{N(q-n)} \tilde{X}_2, \tag{6.10}$$

where $\tilde{X}_1, \tilde{X}_2 \in \mathbb{F}_2^{qN}$, $\tilde{Y}_1, \tilde{Y}_2 \in \mathbb{F}_2^{qN}$. To see this, consider the block-diagonal matrix $\mathbf{H}' \in \mathbb{F}_2^{qN \times qN}$ consisting of N copies of $\mathbf{G}^t$ on the diagonal where integer $t \geq 0$:

$$\mathbf{H}' \triangleq \begin{bmatrix} \mathbf{G}^t & \mathbf{0}^{q\times q} & \dots & \mathbf{0}^{q\times q} \\ \mathbf{0}^{q\times q} & \mathbf{G}^t & \dots & \mathbf{0}^{q\times q} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}^{q\times q} & \mathbf{0}^{q\times q} & \mathbf{0}^{q\times q} & \mathbf{G}^t \end{bmatrix}.$$

Due to the fact that $\mathbf{H}'$ contains sub-matrices $\mathbf{G}^t$ as copies along its diagonal, there exists a permutation matrix $\mathbf{P}$ such that $\mathbf{H}'\mathbf{P} = \mathbf{H}^{tN}$ for integer $t \geq 0$. Therefore, without loss of generality, it is sufficient to analyze linear coding over N uses of our original network by considering linear coding over a *single use* of the extended shift network given via Eqn. (6.9) and Eqn. (6.10).

Consider linear encoding at both transmitters and linear decoding at both receivers. Denote the source bits at the first and second transmitters by $\{s_{1k}\}$ and $\{s_{2k}\}$ respectively where $1 \leq k \leq K$. The definition of linear coding (over $\mathbb{F}_2$) at the transmitters implies that there exist beam-forming vectors $\mathbf{v}_{1,k} \in \mathbb{F}_2^{qN}$ and $\mathbf{v}_{2,k} \in \mathbb{F}_2^{qN}$ such that

$$\tilde{X}_1 = \bigoplus_{k=1}^{K} s_{1,k}\mathbf{v}_{1,k},$$
$$\tilde{X}_2 = \bigoplus_{k=1}^{K} s_{2,k}\mathbf{v}_{2,k}.$$

The output signals of the receivers are deterministic functions of the input:

$$\tilde{Y}_1 = \left[\bigoplus_{k=1}^{K} s_{1,k}\mathbf{H}^{N(q-n)}\mathbf{v}_{1,k} \oplus s_{2,k}\mathbf{H}^{N(q-m)}\mathbf{v}_{2,k}\right], \tag{6.11}$$

$$\tilde{Y}_2 = \left[\bigoplus_{k=1}^{K} s_{1,k}\mathbf{H}^{N(q-m)}\mathbf{v}_{1,k} \oplus s_{2,k}\mathbf{H}^{N(q-n)}\mathbf{v}_{2,k}\right]. \tag{6.12}$$

Definition 24 (Alignment Set at First Receiver)**.** *Either* $\mathbf{H}^{N(q-n)}\mathbf{v}_{1,k} = \mathbf{H}^{N(q-m)}\mathbf{v}_{2,k}$ *holds or the case* $\mathbf{H}^{N(q-n)}\mathbf{v}_{1,k} \neq \mathbf{H}^{N(q-m)}\mathbf{v}_{2,k}$ *holds. If* $\mathbf{H}^{N(q-n)}\mathbf{v}_{1,k} = \mathbf{H}^{N(q-m)}\mathbf{v}_{2,k}$ *holds, this is defined as an* alignment *of beam-forming vectors at the first receiver. Let the alignment set at the first receiver be defined as*

$$\mathcal{A}_1 \triangleq \left\{k \in [K] : \mathbf{H}^{N(q-n)}\mathbf{v}_{1,k} = \mathbf{H}^{N(q-m)}\mathbf{v}_{2,k}\right\}.$$

Definition 25 (Alignment Set at Second Receiver)**.** *Either* $\mathbf{H}^{N(q-m)}\mathbf{v}_{1,k} = \mathbf{H}^{N(q-n)}\mathbf{v}_{2,k}$ *holds or the case* $\mathbf{H}^{N(q-m)}\mathbf{v}_{1,k} \neq \mathbf{H}^{N(q-n)}\mathbf{v}_{2,k}$ *holds. If* $\mathbf{H}^{N(q-m)}\mathbf{v}_{1,k} = \mathbf{H}^{N(q-n)}\mathbf{v}_{2,k}$ *holds, this is defined as an* alignment *of beam-forming vectors at the second receiver. Let the alignment set at the second receiver be defined as*

$$\mathcal{A}_2 \triangleq \left\{k \in [K] : \mathbf{H}^{N(q-m)}\mathbf{v}_{1,k} = \mathbf{H}^{N(q-n)}\mathbf{v}_{2,k}\right\}.$$

Lemma 18 (Simultaneous Alignment is Impossible)**.** *The following* key implication *holds for two-user symmetric networks where* $0 < m < n$ *and* $q \geq n$*:* $\mathcal{A}_1 \cap \mathcal{A}_2 = \emptyset$*. In other words,*

$$\forall k: \quad \mathbf{H}^{N(q-n)}\mathbf{v}_{1,k} = \mathbf{H}^{N(q-m)}\mathbf{v}_{2,k} \;\Rightarrow\; \mathbf{H}^{N(q-m)}\mathbf{v}_{1,k} \neq \mathbf{H}^{N(q-n)}\mathbf{v}_{2,k}, \tag{6.13}$$

$$\forall k: \quad \mathbf{H}^{N(q-m)}\mathbf{v}_{1,k} = \mathbf{H}^{N(q-n)}\mathbf{v}_{2,k} \;\Rightarrow\; \mathbf{H}^{N(q-n)}\mathbf{v}_{1,k} \neq \mathbf{H}^{N(q-m)}\mathbf{v}_{2,k}. \tag{6.14}$$

Eqn (6.13) and Eqn (6.14) of the above lemma state that alignment is possible with respect to each receiver, but *not to both* receivers simultaneously. To see this more clearly, consider the implication in Eqn (6.13). The assumption is that $\mathbf{v}_{1,k} = \mathbf{H}^{N(n-q)}\mathbf{H}^{N(q-m)}\mathbf{v}_{2,k} = \mathbf{H}^{N(n-m)}\mathbf{v}_{2,k}$. However,

$$\mathbf{H}^{N(q-m)}\mathbf{v}_{1,k} = \mathbf{H}^{N(q-m)}\mathbf{H}^{N(n-m)}\mathbf{v}_{2,k} = \mathbf{H}^{N(q+n-2m)}\mathbf{v}_{2,k} \neq \mathbf{H}^{N(q-n)}\mathbf{v}_{2,k}$$

unless $n = m$. Similarly, the implication in Eqn (6.14) follows.

According to Definition 24, in terms of alignment set $\mathcal{A}_1$, the received vector $\tilde{Y}_1 \in \mathbb{F}_2^{qN}$ is a linear combination of the following vectors:

$$\tilde{Y}_1 = \left[\bigoplus_{k\in\mathcal{A}_1}(s_{1,k} \oplus s_{2,k})\mathbf{H}^{N(q-n)}\mathbf{v}_{1,k}\right] \oplus \left[\bigoplus_{k\in\mathcal{A}_1^c} s_{1,k}\mathbf{H}^{N(q-n)}\mathbf{v}_{1,k} \oplus s_{2,k}\mathbf{H}^{N(q-m)}\mathbf{v}_{2,k}\right], \tag{6.15}$$

$$= \left[\bigoplus_{k\in\mathcal{A}_1}(s_{1,k} \oplus s_{2,k})\mathbf{H}^{N(q-m)}\mathbf{v}_{2,k}\right] \oplus \left[\bigoplus_{k\in\mathcal{A}_1^c} s_{1,k}\mathbf{H}^{N(q-n)}\mathbf{v}_{1,k} \oplus s_{2,k}\mathbf{H}^{N(q-m)}\mathbf{v}_{2,k}\right]. \tag{6.16}$$

According to Definition 25, in terms of alignment set $\mathcal{A}_2$, the received vector $\tilde{Y}_2 \in \mathbb{F}_2^{qN}$ is a linear combination of the following vectors:

$$\tilde{Y}_2 = \left[\bigoplus_{k\in\mathcal{A}_2}(s_{1,k} \oplus s_{2,k})\mathbf{H}^{N(q-m)}\mathbf{v}_{1,k}\right] \oplus \left[\bigoplus_{k\in\mathcal{A}_2^c} s_{1,k}\mathbf{H}^{N(q-m)}\mathbf{v}_{1,k} \oplus s_{2,k}\mathbf{H}^{N(q-n)}\mathbf{v}_{2,k}\right], \tag{6.17}$$

$$= \left[\bigoplus_{k\in\mathcal{A}_2}(s_{1,k} \oplus s_{2,k})\mathbf{H}^{N(q-n)}\mathbf{v}_{2,k}\right] \oplus \left[\bigoplus_{k\in\mathcal{A}_2^c} s_{1,k}\mathbf{H}^{N(q-m)}\mathbf{v}_{1,k} \oplus s_{2,k}\mathbf{H}^{N(q-n)}\mathbf{v}_{2,k}\right]. \tag{6.18}$$

Clearly, $K \leq qN$ since received vectors $\tilde{Y}_1, \tilde{Y}_2 \in \mathbb{F}_2^{qN}$. However, since $m \leq n$, a tighter bound to prove is $K \leq mN$. In addition, Lemma 18 implies further that $K \leq \left(\frac{2}{3}\right) qN$ regardless of the values of m, n. To prove the inequalities, the following definition of zero-error linear decoding is provided.

Definition 26 (Encoding and Decoding Matrices)**.** *Encoding vectors* $\{\mathbf{v}_{\ell,k}\}$ *for* $\ell = 1, 2$ *transmitters and* $k \in [K]$ *may be grouped into encoding matrices* $\mathbf{V}_\ell \in \mathbb{F}_2^{qN\times K}$*. For each*

encoding vector $\mathbf{v}_{\ell,k}$ *there exists a corresponding decoding vector* $\mathbf{r}_{\ell,k}$. *The decoding vectors may be grouped as matrices* $\mathbf{R}_\ell \in \mathbf{F}_2^{qN\times K}$.

$$\mathbf{V}_\ell \triangleq \begin{bmatrix} \mathbf{v}_{\ell,1} & \mathbf{v}_{\ell,2} & \dots & \mathbf{v}_{\ell,K} \end{bmatrix}.$$
$$\mathbf{R}_\ell \triangleq \begin{bmatrix} \mathbf{r}_{\ell,1} & \mathbf{r}_{\ell,2} & \dots & \mathbf{r}_{\ell,K} \end{bmatrix}.$$

Definition 27 (Zero-Error Linear Decoding)**.** *Let* $\tilde{Y}_1, \tilde{Y}_2$ *be the output signals received at each receiver respectively. Zero-error linear encoding and decoding over* $\mathbb{F}_2$ *is defined by the following conditions.*

$$\boldsymbol{s}_1 \triangleq \begin{bmatrix} s_{1,1} & s_{1,2} & \dots & s_{1,K} \end{bmatrix}^T.$$
$$\boldsymbol{s}_2 \triangleq \begin{bmatrix} s_{2,1} & s_{2,2} & \dots & s_{2,K} \end{bmatrix}^T.$$
$$\mathbf{R}_1^T\tilde{Y}_1 = \boldsymbol{s}_1 \oplus \boldsymbol{s}_2.$$
$$\mathbf{R}_2^T\tilde{Y}_2 = \boldsymbol{s}_1 \oplus \boldsymbol{s}_2.$$

6.7.1 Proof Of Inequality Eqn. (6.7)

If zero-error linear decoding of K computations is assumed at both receivers according to Definition 27, then the following rank conditions must hold due to the ordinary output equations given in Eqn. (6.11) and Eqn. (6.12) respectively.

$$\mathsf{rank}\left[\mathbf{R}_1^T\mathbf{H}^{N(q-m)}\mathbf{V}_2\right] = K,$$
$$\mathsf{rank}\left[\mathbf{R}_2^T\mathbf{H}^{N(q-m)}\mathbf{V}_1\right] = K.$$

Simplifying the conditions,

$$\begin{aligned}\mathsf{rank}\left[\mathbf{R}_1^T\mathbf{H}^{N(q-m)}\mathbf{V}_2\right] &\le \min\left\{\mathsf{rank}\left[\mathbf{R}_1^T\right], \mathsf{rank}\left[\mathbf{H}^{N(q-m)}\right], \mathsf{rank}\left[\mathbf{V}_2^T\right]\right\}\\ &\le \min\{K, qN, mN\},\\ \mathsf{rank}\left[\mathbf{R}_2^T\mathbf{H}^{N(q-m)}\mathbf{V}_1\right] &\le \min\left\{\mathsf{rank}\left[\mathbf{R}_2^T\right], \mathsf{rank}\left[\mathbf{H}^{N(q-m)}\right], \mathsf{rank}\left[\mathbf{V}_1^T\right]\right\}\\ &\le \min\{K, qN, mN\}.\end{aligned}$$

Therefore, the rank conditions will not hold unless $K \le qN$ and $K \le mN$.

6.7.2 Proof Of Inequality Eqn. (6.8)

To prove $K \le \left(\frac{2}{3}\right)qN$, Lemma 18 and the definitions of alignment sets $\mathcal{A}_1$ and $\mathcal{A}_2$ are necessary. The inequality of Eqn. (6.8) follows from the following lemma.

Lemma 19. *Consider the alignment set* $\mathcal{A}_1 \subseteq [K]$ *from Definition 24 and the alignment set* $\mathcal{A}_2 \subseteq [K]$ *from Definition 25. If zero-error linear decoding of* K *computations is assumed*

at both receivers according to Definition 27, the following set cardinality conditions must be true.

$$|\mathcal{A}_1| + |\mathcal{A}_2| \leq K, \tag{6.19}$$
$$|\mathcal{A}_1| + 2|\mathcal{A}_1^c| \leq qN, \tag{6.20}$$
$$|\mathcal{A}_2| + 2|\mathcal{A}_2^c| \leq qN. \tag{6.21}$$

The first inequality in Eqn. (6.19) follows from Lemma 18 which states that $\mathcal{A}_1 \cap \mathcal{A}_2 = \emptyset$. To see why the second and third inequalities hold, the encoding and decoding may be written in matrix form. In the following notation, assume alignment sets $\mathcal{A}_1$ and $\mathcal{A}_2$ are ordered, and that $\mathbf{V}_{1,\mathcal{A}}$ represents the matrix formed by those columns of $\mathbf{V}_1$ with indices in set $\mathcal{A}$ for an arbitrary set $\mathcal{A} \subseteq [K]$. Similarly, let $\mathbf{V}_{2,\mathcal{A}}$ represent the matrix formed by those columns of $\mathbf{V}_2$ with indices in set $\mathcal{A}$ for an arbitrary set $\mathcal{A} \subseteq [K]$. In addition, define

$$\boldsymbol{\phi}_1 \triangleq \left[\begin{array}{ccc} (\boldsymbol{s}_{1,\mathcal{A}_1} \oplus \boldsymbol{s}_{2,\mathcal{A}_1}) & \boldsymbol{s}_{1,\mathcal{A}_1^c} & \boldsymbol{s}_{2,\mathcal{A}_1^c} \end{array} \right]^T,$$
$$\boldsymbol{\phi}_2 \triangleq \left[\begin{array}{ccc} (\boldsymbol{s}_{1,\mathcal{A}_2} \oplus \boldsymbol{s}_{2,\mathcal{A}_2}) & \boldsymbol{s}_{2,\mathcal{A}_2^c} & \boldsymbol{s}_{1,\mathcal{A}_2^c} \end{array} \right]^T.$$

Based on Equations: (6.15), (6.16), (6.17) and (6.18), define the following matrices.

$$\boldsymbol{\Phi}_1 \triangleq \left[\begin{array}{ccc} \mathbf{H}^{N(q-n)}\mathbf{V}_{1,\mathcal{A}_1} & \mathbf{H}^{N(q-n)}\mathbf{V}_{1,\mathcal{A}_1^c} & \mathbf{H}^{N(q-m)}\mathbf{V}_{2,\mathcal{A}_1^c} \end{array} \right].$$
$$\boldsymbol{\Phi}_2 \triangleq \left[\begin{array}{ccc} \mathbf{H}^{N(q-n)}\mathbf{V}_{2,\mathcal{A}_2} & \mathbf{H}^{N(q-n)}\mathbf{V}_{2,\mathcal{A}_2^c} & \mathbf{H}^{N(q-m)}\mathbf{V}_{1,\mathcal{A}_2^c} \end{array} \right].$$

Then the decoding at both receivers is characterized by the following linear algebra.

$$\mathbf{R}_1^T \tilde{Y}_1 = \mathbf{R}_1^T \boldsymbol{\Phi}_1 \boldsymbol{\phi}_1. \tag{6.22}$$
$$\mathbf{R}_2^T \tilde{Y}_2 = \mathbf{R}_2^T \boldsymbol{\Phi}_2 \boldsymbol{\phi}_2. \tag{6.23}$$

The matrices $\mathbf{R}_1, \mathbf{R}_2 \in \mathbb{F}_2^{qN \times K}$ and the matrices

$$\boldsymbol{\Phi}_1 \in \mathbb{F}_2^{qN \times (|\mathcal{A}_1| + 2|\mathcal{A}_1^c|)},$$
$$\boldsymbol{\Phi}_2 \in \mathbb{F}_2^{qN \times (|\mathcal{A}_2| + 2|\mathcal{A}_2^c|)}.$$

If the columns of $\boldsymbol{\Phi}_1$ are *not* linearly independent, then K computations cannot be recovered at the first receiver, because after column operations, $\boldsymbol{\Phi}_1$ may be reduced to a matrix having at least one column consisting of all zeroes. In this case, $\boldsymbol{\Phi}_1 \boldsymbol{\phi}_1$ will not include at least one source symbol required for K computations. In order for $\boldsymbol{\Phi}_1$ to have linearly independent columns, it must be that $|\mathcal{A}_1| + 2|\mathcal{A}_1^c| \leq qN$. Similarly, in order for $\boldsymbol{\Phi}_2$ to have linearly independent columns, and for the second receiver to recover K computations, $|\mathcal{A}_2| + 2|\mathcal{A}_2^c| \leq qN$. This completes the proof of Lemma 19.

Theorem 8 follows from Lemma 19 since for *any* choice of alignment sets $\mathcal{A}_1 \subseteq [K]$ and $\mathcal{A}_2 \subseteq [K]$, the inequality $3K \leq 2qN$ holds. For the particular choice of alignment sets with balanced cardinalities, i.e., $|\mathcal{A}_1| = |\mathcal{A}_2| = \frac{K}{2}$, the bound $3K \leq 2qN$ holds. For all other choices of alignment sets, the bound is *tighter*. Hence, $3K \leq 2qN$ represents the linear coding upper bound.

□

6.8 Converse Theorems

In order to determine the fundamental limits of computing in a network for either linear or non-linear codes, the entropy of signals must be taken into account. The following basic converse bounds illustrate proof techniques based on Fano's inequality, and simple genie-aided arguments.

Lemma 20 (Basic Cut-Set Bound)**.** *The computation rate is limited by the total entropy of the output signals:*

$$\frac{R_{\text{COMP}}}{q} \leq 1.$$

Proof. For the following steps, we write X_2^n and Y_1^n to mean $\{X_2[i]\}_{i=1}^n$ and $\{Y_1[i]\}_{i=1}^n$ respectively. By applying Fano's inequality,

$$\begin{aligned}
N(R_{\text{COMP}}) &= H(S_1^K \oplus S_2^K), \\
&= I(S_1^K \oplus S_2^K; Y_1^N) + H(S_1^K \oplus S_2^K | Y_1^N), \\
&\leq I(S_1^K \oplus S_2^K; Y_1^N) + N\epsilon_N, \\
&\leq I(S_1^K \oplus S_2^K; Y_1^N, S_2^K) + N\epsilon_N, \\
&= I(S_1^K \oplus S_2^K; Y_1^N | S_2^K, X_2^N) + N\epsilon_N, \\
&\leq H(Y_1^N | S_2^K, X_2^N) + N\epsilon_N, \\
&\leq \sum_i H(Y_{1i} | X_{2i}) + N\epsilon_N.
\end{aligned}$$

If R_{COMP} is achievable, then $\epsilon_N \to 0$ as N tends to infinity. So we get $NR_{\text{COMP}} \leq Nq$. In the above derivations, the fourth step utilizes the fact that S_2^K is independent of $S_1^K \oplus S_2^K$. □

Lemma 21 (Tighter Cut-Set Bound)**.** *For an (m, q, L) network where $L = 2$ users,*

$$\frac{R_{\text{COMP}}}{q} \leq \alpha.$$

Proof. For the following steps, we write X_1^n and Y_1^n to mean $\{X_1[i]\}_{i=1}^n$ and $\{Y_1[i]\}_{i=1}^n$ respectively. By applying Fano's inequality,

$$\begin{aligned}
N(R_{\text{COMP}}) &= H(S_1^K \oplus S_2^K), \\
&= I(S_1^K \oplus S_2^K; Y_1^N) + H(S_1^K \oplus S_2^K | Y_1^N), \\
&\leq I(S_1^K \oplus S_2^K; Y_1^N) + N\epsilon_N, \\
&\leq I(S_1^K \oplus S_2^K; Y_1^N, S_1^K) + N\epsilon_N, \\
&= I(S_1^K \oplus S_2^K; Y_1^N | S_1^K, X_1^N) + N\epsilon_N, \\
&\leq H(Y_1^N | S_1^K, X_1^N) + N\epsilon_N, \\
&\leq \sum_i H(Y_{1i} | X_{1i}) + N\epsilon_N.
\end{aligned}$$

The last inequality yields that $N(R_{\text{COMP}}) \leq Nm$ which completes the proof. □

Lemma 22 (Beyond Cut-Set Bounds [87]). *For an (m, q, L) network where $L = 2$ users,*

$$\frac{R_{\text{COMP}}}{q} \leq \frac{2}{3}.$$

The following proof starts in a novel manner, and was first proven solely by Prof. C. Suh in [87]. The proof is quoted here for the sake of completeness only. For symmetric $L = 2$ user networks, $\mathbf{G}^{q-m}X_\ell$ can be reconstructed from (Y_1, Y_2). Without loss of generality, assume that $\mathbf{G}^{q-m}X_1$ is a function of (Y_1, Y_2). Starting with Fano's inequality, we get

$$\begin{aligned}
&N(3R_{\text{COMP}} - \epsilon_N) \\
&\leq I(S_1^K \oplus S_2^K; Y_1^N) + I(S_1^K \oplus S_2^K; Y_2^N) + I(S_1^K \oplus S_2^K; Y_2^N) \\
&\overset{(a)}{\leq} [H(Y_1^N) - H(Y_1^N|S_1^K \oplus S_2^K)] \\
&\quad + [H(Y_2^N) - H(Y_2^N|S_1^K \oplus S_2^K, Y_1^N)] + I(S_1^K \oplus S_2^K; Y_2^N) \\
&\leq H(Y_1^N) + H(Y_2^N) \\
&\quad - H(Y_1^N, Y_2^N|S_1^K \oplus S_2^K) + I(S_1^K \oplus S_2^K; Y_2^N, S_2^K) \\
&\overset{(b)}{=} H(Y_1^N) + H(Y_2^N) \\
&\quad - H(Y_1^N, Y_2^N|S_1^K \oplus S_2^K) + I(S_1^K \oplus S_2^K; Y_2^N|S_2^K) \\
&\overset{(c)}{=} H(Y_1^N) + H(Y_2^N) \\
&\quad - H(Y_1^N, Y_2^N|S_1^K \oplus S_2^K) + H(\mathbf{T}_{12}X_1^N|S_2^K) \\
&\overset{(d)}{=} H(Y_1^N) + H(Y_2^N) \\
&\quad - H(Y_1^N, Y_2^N, \mathbf{T}_{12}X_1^N|S_1^K \oplus S_2^K) + H(\mathbf{T}_{12}X_1^N|S_2^K) \\
&\leq H(Y_1^N) + H(Y_2^N) \\
&\quad - H(\mathbf{T}_{12}X_1^N|S_1^K \oplus S_2^K) + H(\mathbf{T}_{12}X_1^N|S_2^K) \\
&\overset{(e)}{=} H(Y_1^N) + H(Y_2^N) - H(\mathbf{T}_{12}X_1^N) + H(\mathbf{T}_{12}X_1^N|S_2^K) \\
&\overset{(f)}{\leq} \sum [H(Y_{1i}) + H(Y_{2i})] \\
&\leq 2Nq,
\end{aligned}$$

where (a) follows from the fact that conditioning reduces entropy; (b) follows from the fact that S_2^K is independent of $S_1^K \oplus S_2^K$; (c) follows from the fact that X_2^N is a function of S_2^K and that $\mathbf{T}_{12} \triangleq \mathbf{I}_N \otimes \mathbf{G}^{q-m}$; (d) follows from our hypothesis that $\mathbf{G}^{q-m}X_1$ is a function of (Y_1, Y_2); (e) follows from the fact that X_1^N is a function of S_1^K that is independent of $S_1^K \oplus S_2^K$; (f) follows from the fact that conditioning reduces entropy. This completes the proof.

Table 6.1: COMPUTATION CAPACITY RESULTS FOR (m, q, L) NETWORKS [87]

Network		α $(0, \frac{1}{2})$	α $[\frac{1}{2}, \frac{2}{3}]$	α $(\frac{2}{3}, 1)$	α 1
$(m, q, 2)$	$\frac{C_{\text{COMP}}}{q}$	α	α	$\frac{2}{3}$	1
(m, q, L)	$\frac{C^{\text{LIN}}_{\text{COMP}}}{q}$	α	$\frac{1}{2}$	$\frac{1}{2}$	1
(m, q, ∞)	$\frac{C_{\text{COMP}}}{q}$	α	$\frac{1}{2}$	$\frac{1}{2}$	1

6.9 General L-User Networks

We summarize the contributions for $L = 2$ networks. Computation alignment strategies were introduced for multi-casting modulus functions. Vector and scalar linear coding strategies were both necessary. With even two receivers, a key challenge is to balance shared network resources with receiver demands. A good code allows for *in-network* computation as opposed to recovering all messages at the receivers. The computation capacity was determined for a countably infinite class of $(m, q, L = 2)$ deterministic models. Several network equivalence and decomposition theorems were developed which have a strong potential for inclusion in multi-hop network codes.

In extending to $L > 2$ users, the network equivalences and decompositions still hold. In addition, the linear coding upper bound extends in an intuitive way. The information-theoretic upper bound based on Fano's inequality extends to L-user networks, but yields a gap to the linear coding achievable bound. Table 6.1 summarizes known results for L-user networks as further studied in [87]. In [87], it is shown that if $L \to \infty$, then the asymptotic computation capacity is resolved. For all finite L, the linear coding capacity $C^{\text{LIN}}_{\text{COMP}}$ is known, but a gap to the information-theoretic upper bound exists. It is possible that structured, non-linear codes might outperform vector-space function alignment codes for general (m, q, L) networks where $L > 2$.

Part III

Low-Complexity Source-Channel-Network Coding

Chapter 7

Linear Transform Coding in Networks

7.1 Introduction

The compression and estimation of an observed signal via subspace projections is both a classical and current topic in signal processing and communication. While random subspace projections have received considerable attention in the compressed sensing literature [28], subspace projections optimized for minimal distortion are important for many applications. The Karhunen-Loève transform (KLT) and its empirical form Principal Components Analysis (PCA), are widely studied in computer vision, biology, signal processing, and information theory. Reduced dimensionality representations are useful for source coding, noise filtering, compression, clustering, and data mining. Specific examples include eigenfaces for face recognition, orthogonal decomposition in transform coding, and sparse PCA for gene analysis [89, 44, 25].

In contemporary applications such as wireless sensor networks (WSNs) and distributed databases, data is available and collected in different locations. In a WSN, sensors are usually constrained by limited power and bandwidth resources. This has motivated existing approaches to take into account correlations across high-dimensional sensor data to reduce transmission requirements (see e.g. [36, 83, 92, 94, 31, 95, 30]). Rather than transmitting raw sensor data to a fusion center to approximate a global signal, sensor nodes carry out local data dimensionality reduction to increase bandwidth and energy efficiency.

In the present paper, we propose a linear transform network (LTN) model to analyze dimensionality reduction for compression-estimation of correlated signals in *multi-hop* networks. In a centralized setting, given a random source signal $\boldsymbol{x}$ with zero-mean and covariance matrix $\boldsymbol{\Sigma_x}$, applying the KLT to $\boldsymbol{x}$ yields uncorrelated components in the eigenvector basis of $\boldsymbol{\Sigma_x}$. The optimal linear least squares k^{th}-order approximation of the source is given by the k components corresponding to the k largest eigenvalues of $\boldsymbol{\Sigma_x}$. In a network setting, multiple correlated signals are observed by different source nodes. The source nodes transmit low-dimensional subspace projections (approximations of the source) to intended receivers via a relay network. The compression-estimation problem is to optimize the subspace projections

computed by all nodes in order to minimize the end-to-end distortion at receiver nodes.

In our model, receivers estimate random vectors based on "one-shot" linear *analog-amplitude* multisensor observations. The restriction to "one-shot", zero-delay encoding of each vector of source observations separately is interesting due to severe complexity limitations in many applications (e.g. sensor networks). Linear coding depends on first-order and second-order statistics and is robust to uncertainty in the precise probabilistic distribution of the sources. Under the assumption of ideal channels between nodes, our task is to optimize signal subspaces given limited bandwidth in terms of the number of real-valued messages communicated. Our results extend previous work on distributed estimation in this case [36, 83, 92, 94]. For the case of dimensionality-reduction with noisy channel communication (see e.g. [83]), the task is to optimize signal subspaces subject to channel noise and power constraints.

For noisy networks, the general communication problem is often referred to as the *joint source-channel-network coding problem* in the information-theoretic literature and is a famously open problem. Beyond the zero-delay, linear dimensionality-reduction considered here, end-to-end performance in networks could be improved by (i), non-linear strategies and (ii), allowing a longer coding horizon. Partial progress includes non-linear low-delay mappings for only simple network scenarios [78, 86, 46]. For the case of an infinite coding horizon, separation theorems for decomposing the joint communication problem have been analyzed by [77, 50, 34].

7.1.1 Related Work

Directly related to our work in networks is the *distributed* KLT problem. Distributed linear transforms were introduced by Gastpar et al. for the compression of jointly Gaussian sources using iterative methods [36][35]. Simultaneous work by Zhang et al. for multi-sensor data fusion also resulted in iterative procedures [94]. An alternate proof based on innovations for second order random variables with arbitrary distributions was given by [70]. The problem was extended for non-Gaussian sources, including channel fading and noise effects to model the non-ideal link from sensors to decoder by Schizas et al. [83]. Roy and Vetterli provide an *asymptotic* distortion analysis of the distributed KLT, in the case when the dimension of the source and observation vectors approaches infinity [80]. Finally, Xiao et al. analyze linear transforms for distributed *coherent* estimation [92].

Much of the estimation-theoretic literature deals with *single-hop* networks; each sensor relays information directly to a fusion center. In *multi-hop* networks, linear operations are performed by successive relays to aggregate, compress, and redistribute correlated signals. The LTN model relates to recent work on routing and *network coding* (Ahlswede et al. [3]). In pure routing solutions, intermediate nodes either forward or drop packets. The corresponding analogy in the LTN model is to constrain transforms to be essentially identity transforms. However, network coding (over finite fields) has shown that mixing of data at intermediate nodes achieves higher rates in the multicast setting (see [59] regarding the sufficiency of linear codes and [49] for multicast code construction). Similarly in the LTN model,

linear combining of subspace projections (over the real field) at intermediate nodes improves decoding performance. Lastly, the max-flow min-cut theorem of Ford-Fulkerson [32] provides the basis for cut-set lower bounds in networks.

The LTN model is partially related to the formulation of Koetter and Kschischang [52] modeling information transmission as the injection of a basis for a vector space into the network, and subspace codes [85]. If arbitrary data exchange is permitted between network nodes, the compression-estimation problem is related to estimation in graphical models (e.g. decomposable PCA [90], and tree-based transforms (tree-KLT) [84]). Other related work involving signal projections in networks includes joint source-channel communication in sensor networks [11], random projections in a gossip framework[73], and distributed compressed sensing [13].

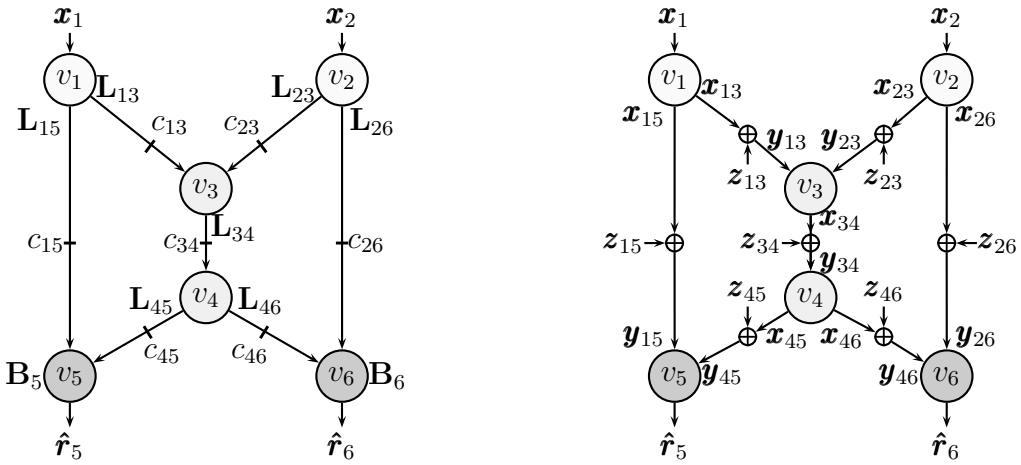
7.1.2 Summary of Main Results

We cast the network compression-estimation problem as a statistical signal processing and constrained optimization problem. For most networks, the optimization is non-convex. Therefore, our main results are divided into two categories: (i) Iterative solutions for linear transform coding over acyclic networks; (ii) Cut-set bounds based on convex relaxations and cut-set bounds based on information theory.

- Section 7.3 reviews linear signal processing in networks. Section 7.4 outlines an iterative optimization for compression-estimation matrices in ideal networks under a local convergence criterion.
- Section 7.7 analyzes an iterative optimization method involving constrained quadratic programs for noisy networks with power allocation over subspaces.
- Section 8.1 introduces cut-set lower bounds to benchmark the minimum mean square error (MSE) for linear coding based on convex relaxations such as a semi-definite program (SDP) relaxation.
- Section 8.5 describes cut-set lower bounds for any coding strategy in networks based on information-theoretic principles of source-channel separation. The lower bounds are plotted for a distributed noisy network.
- Sections 7.4-8.1 provide examples illustrating the tradeoffs between compression and estimation; upper and lower bounds are illustrated for an aggregation (tree) network, butterfly network, and distributed noisy network.

7.1.3 Notation

Boldface upper case letters denote matrices, boldface lower case letters denote column vectors, and calligraphic upper case letters denote sets. The ℓ^2-norm of a vector $\boldsymbol{x} \in \mathbb{R}^n$ is



(a) Linear Transform Network (b) Signal Flow on Graph

Figure 7.1: (*a*) Linear transform network model. (*b*) Signal flow graph representation.

defined as $\|\boldsymbol{x}\|_2 \triangleq \sqrt{\sum_{i=1}^{n} |x_i|^2}$. The weighted ℓ^2-norm $\|\boldsymbol{x}\|_{\mathbf{W}} \triangleq \|\mathbf{W}\boldsymbol{x}\|_2$ where $\mathbf{W}$ is a positive semi-definite matrix (written $\mathbf{W} \succeq \mathbf{0}$). Let $(\cdot)^T$, $(\cdot)^{-1}$, and $\mathrm{tr}(\cdot)$ denote matrix transpose, inverse, and trace respectively. Let $\mathbf{A} \otimes \mathbf{B}$ denote the Kronecker matrix product of two matrices. The matrix $\mathbf{I}_\ell$ denotes the $\ell \times \ell$ identity. For $\ell \geq k$, the notation $\mathbf{T}_{k:\ell} \triangleq \mathbf{T}_k \mathbf{T}_{k+1} \cdots \mathbf{T}_\ell$ denotes the product of $(\ell - k + 1)$ matrices. A matrix $\mathbf{X} \in \mathbb{R}^{m \times n}$ is written in vector form $\mathrm{vec}(\mathbf{X}) \in \mathbb{R}^{mn}$ by stacking its columns; i.e. $\mathrm{vec}(\mathbf{X}) = [\boldsymbol{x}_1; \boldsymbol{x}_2; \ \ldots \ ; \boldsymbol{x}_n]$ where $\boldsymbol{x}_j$ is the j-th column of $\mathbf{X}$. For random vectors, $E[\cdot]$ denotes the expectation, and $\boldsymbol{\Sigma}_{\boldsymbol{x}} \triangleq E[\boldsymbol{x}\boldsymbol{x}^T]$ denotes the covariance matrix of the zero-mean random vector $\boldsymbol{x}$.

7.2 Network Model

Fig. 7.1 serves as an extended example of an LTN graph. The network is comprised of two sources, two relays, and two receiver nodes.

Definition 28 (Relay Network)**.** *Consider a relay network modeled by a directed acyclic graph (DAG) $G = (\mathcal{V}, \mathcal{E})$ and a set of weights $\mathcal{C}$. The set $\mathcal{V} = \{v_1, v_2, \ldots, v_{|\mathcal{V}|}\}$ is the vertex/node set, $\mathcal{E} \subset \{1, \ldots, |\mathcal{V}|\} \times \{1, \ldots, |\mathcal{V}|\}$ is the edge set, and $\mathcal{C} = \{c_{ij} \in \mathbb{Z}^+ : (i,j) \in \mathcal{E}\}$ is the set of weights. Each edge $(i,j) \in \mathcal{E}$ represents a communication link with integer bandwidth c_{ij} from node v_i to v_j. The in-degree and out-degree of a node v_i are computed as*

$$d_i^- = \sum_{q:(q,i)\in\mathcal{E}} c_{qi}, \tag{7.1}$$

$$d_i^+ = \sum_{l:(i,l)\in\mathcal{E}} c_{il}. \tag{7.2}$$

As an example, the graph in Fig. 7.1 consists of nodes $\mathcal{V} = \{v_1, v_2, \ldots, v_6\}$. Integer bandwidths c_{ij} for each communication link (i, j) are marked.

Definition 29 (Source and Receiver Nodes)**.** *Given a relay network $G = (\mathcal{V}, \mathcal{E})$, the set of source nodes $\mathcal{S} \subset \mathcal{V}$ is defined as $\mathcal{S} = \{v_i \in \mathcal{V} \mid d_i^- = 0\}$. We assume a labeling of nodes in $\mathcal{V}$ so that $\mathcal{S} = \{v_1, v_2, \ldots, v_{|\mathcal{S}|}\}$, i.e. the first $|\mathcal{S}|$ nodes are source nodes. The set of receiver nodes $\mathcal{T} \subset \mathcal{V}$ is defined as $\mathcal{T} = \{v_i \in \mathcal{V} \mid d_i^+ = 0\}$.*[1] *Let $\kappa \triangleq |\mathcal{V}| - |\mathcal{T}|$. We assume a labeling of nodes in $\mathcal{V}$ so that $\mathcal{T} = \{v_{\kappa+1}, v_{\kappa+2}, \ldots, v_{|\mathcal{V}|}\}$, i.e. the last $|\mathcal{T}|$ nodes are receiver nodes.*

In Fig. 7.1, $\mathcal{S} = \{v_1, v_2\}$ and $\mathcal{T} = \{v_5, v_6\}$.

7.2.1 Source Model

Definition 30 (Basic Source Model)**.** *Given a relay network $G = (\mathcal{V}, \mathcal{E})$ with source and receiver nodes $(\mathcal{S}, \mathcal{T})$, the source nodes $\mathcal{S} = \{v_i\}_{i=1}^{|\mathcal{S}|}$ observe random signals $\mathcal{X} = \{\boldsymbol{x}_i\}_{i=1}^{|\mathcal{S}|}$. The random vectors $\boldsymbol{x}_i \in \mathbb{R}^{n_i}$ are assumed zero-mean with covariance $\boldsymbol{\Sigma}_{ii}$, and cross-covariances $\boldsymbol{\Sigma}_{ij} \in \mathbb{R}^{n_i \times n_j}$. Let $n \triangleq \sum_i n_i$. The distributed network sources may be grouped into an n-dimensional random vector $\boldsymbol{x} = [\boldsymbol{x}_1; \boldsymbol{x}_2; \ \ldots \ ; \boldsymbol{x}_{|\mathcal{S}|}]$ with known second-order statistics $\boldsymbol{\Sigma}_{\boldsymbol{x}} \in \mathbb{R}^{n \times n}$,*

$$\boldsymbol{\Sigma}_{\boldsymbol{x}} = \begin{bmatrix} \boldsymbol{\Sigma}_{11} & \boldsymbol{\Sigma}_{12} & \cdots & \boldsymbol{\Sigma}_{1|\mathcal{S}|} \\ \boldsymbol{\Sigma}_{21} & \boldsymbol{\Sigma}_{22} & \cdots & \boldsymbol{\Sigma}_{2|\mathcal{S}|} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{\Sigma}_{|\mathcal{S}|1} & \boldsymbol{\Sigma}_{|\mathcal{S}|2} & \cdots & \boldsymbol{\Sigma}_{|\mathcal{S}||\mathcal{S}|} \end{bmatrix}. \tag{7.3}$$

More generally, each source node $v_i \in \mathcal{S}$ emits independent and identically distributed (*i.i.d.*) source vectors $\{\boldsymbol{x}_i[t]\}_{t>0}$ for t a discrete time index; however, in the analysis of zero-delay linear coding, we do not write the time indices explicitly.

Remark 20. *A common linear signal-plus-noise model for sensor networks is of the form $\boldsymbol{x}_i = \mathbf{H}_i \boldsymbol{x} + \boldsymbol{n}_i$; however, neither a linear source model nor the specific distribution of $\boldsymbol{x}_i$ is assumed here.* A priori *knowledge of second-order statistics may be obtained during a training phase via sample estimation.*

In Fig. 7.1, two source nodes $\mathcal{S} = \{v_1, v_2\}$ observe the corresponding random signals in $\mathcal{X} = \{\boldsymbol{x}_1, \boldsymbol{x}_2\}$.

7.2.2 Communication Model

Definition 31 (Communication Model)**.** *Given a relay network $G = (\mathcal{V}, \mathcal{E})$ with weight-set $\mathcal{C}$, each edge $(i, j) \in \mathcal{E}$ represents a communication link of bandwidth c_{ij} from v_i to v_j. The*

[1] For networks of interest in this paper, an arbitrary DAG G may be augmented with auxiliary nodes to ensure that source nodes have in-degree $d_i^- = 0$ and receiver nodes have out-degree $d_i^+ = 0$.

bandwidth is the dimension of the vector channel. We denote signals exiting $v_i \in \mathcal{V}$ *along edge* $(i,j) \in \mathcal{E}$ *by* $\boldsymbol{x}_{ij} \in \mathbb{R}^{c_{ij}}$ *and signals entering node* v_j *along edge* $(i,j) \in \mathcal{E}$ *by* $\boldsymbol{y}_{ij} \in \mathbb{R}^{c_{ij}}$. *If communication is noiseless,* $\boldsymbol{y}_{ij} = \boldsymbol{x}_{ij}$. *For all relay nodes and receiver nodes, we further define* $\boldsymbol{y}_j \in \mathbb{R}^{d_j^-}$ *to be the concatenation of all signals* $\boldsymbol{y}_{ij}$ *incident to node* v_j *along edges* $(i,j) \in \mathcal{E}$.

A noisy communication link $(i,j) \in \mathcal{E}$ *is modeled as:* $\boldsymbol{y}_{ij} = \boldsymbol{x}_{ij} + \boldsymbol{z}_{ij}$. *The channel noise* $\boldsymbol{z}_{ij} \in \mathbb{R}^{c_{ij}}$ *is a Gaussian random vector with zero-mean and covariance* $\boldsymbol{\Sigma}_{\boldsymbol{z}_{ij}}$. *The channel input is power constrained so that* $E[\|\boldsymbol{x}_{ij}\|_2^2] \leq P_{ij}$. *The power constraints for a network are given by set* $\mathcal{P} = \{P_{ij} \in \mathbb{R}^+ : (i,j) \in \mathcal{E}\}$. *The signal-to-noise ratio (SNR) along a link is*

$$SNR_{ij} = \frac{E\left[\|\boldsymbol{x}_{ij}\|_2^2\right]}{E\left[\|\boldsymbol{z}_{ij}\|_2^2\right]}. \tag{7.4}$$

Fig. 7.1(b) illustrates the signal flow of an LTN graph.

7.2.3 Linear Encoding over Graph G

Source and relay nodes encode random vector signals by applying reduced-dimension linear transforms.

Definition 32 (Linear Encoding)**.** *Given a relay network* $G = (\mathcal{V}, \mathcal{E})$, *weight-set* $\mathcal{C}$, *source and receiver nodes* $(\mathcal{S}, \mathcal{T})$, *sources* $\mathcal{X}$, *and the communication model of Definition 31, the linear encoding matrices for* G *are denoted by set* $\mathcal{L}_G = \{\mathbf{L}_{ij} : (i,j) \in \mathcal{E}\}$. *Each* $\mathbf{L}_{ij}$ *represents the linear transform applied by node* v_i *in communication with node* v_j. *For* $v_i \in \mathcal{S}$, *transform* $\mathbf{L}_{ij}$ *is of size* $c_{ij} \times n_i$ *and represents the encoding* $\boldsymbol{x}_{ij} = \mathbf{L}_{ij}\boldsymbol{x}_i$. *For a relay* v_i, *transform* $\mathbf{L}_{ij}$ *is of size* $c_{ij} \times d_i^-$, *and* $\boldsymbol{x}_{ij} = \mathbf{L}_{ij}\boldsymbol{y}_i$. *The* compression ratio *along edge* $(i,j) \in \mathcal{E}$ *is*

$$\alpha_{ij} = \begin{cases} \dfrac{c_{ij}}{n_i} & \text{if } v_i \in \mathcal{S}, \quad (7.5a) \\ \dfrac{c_{ij}}{d_i^-} & \text{if } v_i \in \mathcal{V} \setminus \mathcal{S}. \quad (7.5b) \end{cases}$$

In Fig. 7.1, the linear encoding matrices for source node v_1 and v_2 are $\{\mathbf{L}_{15}, \mathbf{L}_{13}\}$ and $\{\mathbf{L}_{26}, \mathbf{L}_{23}\}$ respectively. The linear encoding matrices for the relays are $\mathbf{L}_{34}$, $\mathbf{L}_{45}$, $\mathbf{L}_{46}$. The output signals of source node v_1 are $\boldsymbol{x}_{15} = \mathbf{L}_{15}\boldsymbol{x}_1$ and $\boldsymbol{x}_{13} = \mathbf{L}_{13}\boldsymbol{x}_1$. Similarly, the output signal of relay v_3 is

$$\boldsymbol{x}_{34} = \mathbf{L}_{34}\boldsymbol{y}_3 = \mathbf{L}_{34}\begin{bmatrix} \boldsymbol{y}_{13} \\ \boldsymbol{y}_{23} \end{bmatrix}. \tag{7.6}$$

7.2.4 Linear Estimation over G

Definition 33 (Linear Estimation)**.** *Given relay network* $G = (\mathcal{V}, \mathcal{E})$, *weight-set* $\mathcal{C}$, *source and receiver nodes* $(\mathcal{S}, \mathcal{T})$, *sources* $\mathcal{X}$, *and the communication model of Def. 31, the set of*

linear decoding matrices is denoted $\mathcal{B}_G = \{\mathbf{B}_i\}_{i:v_i\in\mathcal{T}}$. *Each receiver* $v_i \in \mathcal{T}$ *estimates a (zero-mean) random vector* $\boldsymbol{r}_i \in \mathbb{R}^{r_i}$ *which is correlated with the sources in* $\mathcal{X}$. *We assume that the second-order statistics* $\boldsymbol{\Sigma}_{\boldsymbol{r}_i}$, $\boldsymbol{\Sigma}_{\boldsymbol{r}_i\boldsymbol{x}}$ *are known. Receiver* $v_i \in \mathcal{T}$ *applies a linear estimator given by matrix* $\mathbf{B}_i \in \mathbb{R}^{r_i\times d_i^-}$ *to estimate* $\boldsymbol{r}_i$ *given its observations and computes* $\hat{\boldsymbol{r}}_i = \mathbf{B}_i\boldsymbol{y}_i$. *The linear least squares estimate (LLSE) of* $\boldsymbol{r}_i$ *is denoted by* $\hat{\boldsymbol{r}}_i$.

In Fig. 7.1, receiver v_5 reconstructs $\boldsymbol{r}_5$ while receiver v_6 reconstructs $\boldsymbol{r}_6$. The LLSE signals $\hat{\boldsymbol{r}}_5$ and $\hat{\boldsymbol{r}}_6$ are computed as

$$\hat{\boldsymbol{r}}_5 = \mathbf{B}_5\boldsymbol{y}_5 = \mathbf{B}_5\begin{bmatrix}\boldsymbol{y}_{15}\\ \boldsymbol{y}_{45}\end{bmatrix}, \tag{7.7}$$

$$\hat{\boldsymbol{r}}_6 = \mathbf{B}_6\boldsymbol{y}_6 = \mathbf{B}_6\begin{bmatrix}\boldsymbol{y}_{26}\\ \boldsymbol{y}_{46}\end{bmatrix}. \tag{7.8}$$

Definition 34 (Distortion Metric)**.** *Let* $\boldsymbol{x}$ *and* $\boldsymbol{y}$ *be two real vectors of the same dimension. The MSE distortion metric is defined as*

$$d_{mse}(\boldsymbol{x},\boldsymbol{y}) \triangleq \|\boldsymbol{x}-\boldsymbol{y}\|_2^2. \tag{7.9}$$

7.2.5 Compression-Estimation in Networks

Definition 35 (Linear Transform Network $\mathcal{N}$)**.** *An LTN model* $\mathcal{N}$ *is a communication network modeled by DAG* $G = (\mathcal{V},\mathcal{E})$, *weight-set* $\mathcal{C}$, *source and receiver nodes* $(\mathcal{S},\mathcal{T})$, *sources* $\mathcal{X}$, *sets* $\mathcal{L}_G$, *and* $\mathcal{B}_G$ *from Definitions 28-33. Second-order source statistics are given by* $\boldsymbol{\Sigma}_{\boldsymbol{x}}$ *(Definition 30). The operational meaning of compression-estimation matrices in* $\mathcal{L}_G$ *and* $\mathcal{B}_G$ *is in terms of signal flows on* G *(Definition 31). The desired reconstruction vectors* $\{\boldsymbol{r}_i\}_{i:v_i\in\mathcal{T}}$ *have known second-order statistics* $\boldsymbol{\Sigma}_{\boldsymbol{r}_i}$ *and* $\boldsymbol{\Sigma}_{\boldsymbol{r}_i\boldsymbol{x}}$. *The set* $\{\hat{\boldsymbol{r}}_i\}_{i:v_i\in\mathcal{T}}$ *denotes the LLSE estimates formed at receivers (Definition 33). For noisy networks, noise variables along link* $(i,j)\in\mathcal{E}$ *have known covariances* $\boldsymbol{\Sigma}_{\boldsymbol{z}_{ij}}$. *Power constraints are given by set* $\mathcal{P}$ *in Definition 31.*

Given an LTN graph $\mathcal{N}$, the task is to design a *network transform code*: the compression-estimation matrices in $\mathcal{L}_G$ and $\mathcal{B}_G$ to minimize the end-to-end weighted MSE distortion. Let positive weights $\{w_i\}_{i:v_i\in\mathcal{T}}$ represent the relative importance of reconstructing a signal at receiver $v_i \in \mathcal{T}$. Using indexing term $\kappa \triangleq |\mathcal{V}|-|\mathcal{T}|$ for receiver nodes, we concatenate vectors $\boldsymbol{r}_i$ as $\boldsymbol{r} = \left[\boldsymbol{r}_{\kappa+1};\boldsymbol{r}_{\kappa+2};\ \ldots\ ;\boldsymbol{r}_{|\mathcal{V}|}\right]$ and LLSE estimates $\hat{\boldsymbol{r}}_i$ as $\hat{\boldsymbol{r}} = \left[\hat{\boldsymbol{r}}_{\kappa+1};\hat{\boldsymbol{r}}_{\kappa+2};\ \ldots\ ;\hat{\boldsymbol{r}}_{|\mathcal{V}|}\right]$. The average weighted MSE written via a weighted ℓ^2-norm is

$$\begin{aligned} D_{MSE,\mathbf{W}} &\triangleq E\left[\sum_{i:v_i\in\mathcal{T}} d_{mse}(\sqrt{w_i}\boldsymbol{r}_i,\sqrt{w_i}\hat{\boldsymbol{r}}_i)\right],\\ &= E\Big[\big\|\boldsymbol{r}-\hat{\boldsymbol{r}}\big\|_{\mathbf{W}}^2\Big], \end{aligned} \tag{7.10}$$

where $\mathbf{W}$ contains diagonal blocks $\mathbf{W}_i = \sqrt{w_i}\,\mathbf{I}$.

Remark 21. *The distortion $D_{MSE,\mathbf{W}}$ is a function of the compression matrices in $\mathcal{L}_G$ and the estimation matrices in $\mathcal{B}_G$. In most network topologies, the weighted MSE distortion is non-convex over the set of feasible matrices. Even in the particular case of distributed compression [36], currently the optimal linear transforms are not solvable in closed form.*

7.3 Linear Processing of Network Signals

The linear processing and filtering of source signals by an LTN graph $\mathcal{N}$ is modeled compactly as a linear system with inputs, outputs, and memory elements. At each time step, LTN nodes transmit random signals through edges/channels of the graph.

7.3.1 Linear System

Consider edge $(i,j) \in \mathcal{E}$ as a memory element storing random vector $\boldsymbol{y}_{ij}$. Let $c \triangleq (\sum_{(i,j)\in\mathcal{E}} c_{ij})$ and $d \triangleq (\sum_{i:v_i\in\mathcal{T}} d_i^-)$. The network $\mathcal{N}$ is modeled as a linear system with the following signals: (i) input sources $\{\boldsymbol{x}_i\}_{i:v_i\in\mathcal{S}}$ concatenated as global source vector $\boldsymbol{x} \in \mathbb{R}^n$; (ii) input noise variables $\{\boldsymbol{z}_{ij}\}_{(i,j)\in\mathcal{E}}$ concatenated as global noise vector $\boldsymbol{z} \in \mathbb{R}^c$; (iii) memory elements $\{\boldsymbol{y}_{ij}\}_{(i,j)\in\mathcal{E}}$ concatenated as global state vector $\boldsymbol{\mu}[t] \in \mathbb{R}^c$ at time t; (iv) output vectors $\{\boldsymbol{y}_i\}_{i:v_i\in\mathcal{T}}$ concatenated as $\boldsymbol{y} \in \mathbb{R}^d$.

7.3.1.1 State-space Equations

The linear system[2] is described by the following state-space equations for $i : v_i \in \mathcal{T}$,

$$\boldsymbol{\mu}[t+1] = \mathbf{F}\boldsymbol{\mu}[t] + \mathbf{E}\boldsymbol{x}[t] + \tilde{\mathbf{E}}\boldsymbol{z}[t], \tag{7.11}$$

$$\boldsymbol{y}_i[t] = \mathbf{C}_i\boldsymbol{\mu}[t] + \mathbf{D}_i\boldsymbol{x}[t] + \tilde{\mathbf{D}}_i\boldsymbol{z}[t]. \tag{7.12}$$

The matrix $\mathbf{F} \in \mathbb{R}^{c\times c}$ is the state-evolution matrix common to all receivers, $\mathbf{E} \in \mathbb{R}^{c\times n}$ is the source-network connectivity matrix, and $\tilde{\mathbf{E}} \in \mathbb{R}^{c\times c}$ is the noise-to-network connectivity matrix. The matrices $\mathbf{C}_i \in \mathbb{R}^{d_i^-\times c}$, $\mathbf{D}_i \in \mathbb{R}^{d_i^-\times n}$, and $\tilde{\mathbf{D}}_i \in \mathbb{R}^{d_i^-\times c}$ represent how each receiver's output is related to the state, source, and noise vectors respectively. For networks considered in this paper, $\mathbf{D}_i = \mathbf{0}$ and $\tilde{\mathbf{D}}_i = \mathbf{0}$.

7.3.1.2 Linear Transfer Function

A standard result in linear system theory yields the transfer function (assuming a unity indeterminate delay operator) for each receiver $v_i \in \mathcal{T}$,

$$\boldsymbol{y}_i = \mathbf{C}_i\left(\mathbf{I}-\mathbf{F}\right)^{-1}\left(\mathbf{E}\boldsymbol{x} + \tilde{\mathbf{E}}\boldsymbol{z}\right), \tag{7.13}$$

$$= \mathbf{G}_i\boldsymbol{x} + \tilde{\mathbf{G}}_i\boldsymbol{z}, \tag{7.14}$$

[2]When discussing zero-delay linear coding, the time indices on vectors $\boldsymbol{x}$, $\boldsymbol{z}$, and $\boldsymbol{y}_i$ are omitted for greater clarity of presentation.

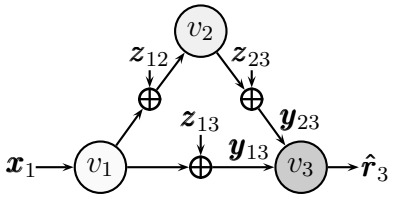


Figure 7.2: Input and output signals for a noisy relay network.

where $\mathbf{G}_i \triangleq \mathbf{C}_i (\mathbf{I} - \mathbf{F})^{-1} \mathbf{E}$ and $\tilde{\mathbf{G}}_i \triangleq \mathbf{C}_i (\mathbf{I} - \mathbf{F})^{-1} \tilde{\mathbf{E}}$. For acyclic graphs, $\mathbf{F}$ is a nilpotent matrix and $(\mathbf{I} - \mathbf{F})^{-1} = \mathbf{I} + \sum_{k=1}^{\gamma} \mathbf{F}^{\gamma}$ for finite integer γ. Using indexing term κ, the observation vectors collected by receivers are concatenated as $\boldsymbol{y} = \left[\boldsymbol{y}_{\kappa+1};\ \boldsymbol{y}_{\kappa+2};\ \ldots\ ;\ \boldsymbol{y}_{|\mathcal{V}|}\right]$. Let

$$\mathbf{T} \triangleq \left[\mathbf{G}_{\kappa+1};\ \mathbf{G}_{\kappa+2};\ \ldots\ ;\ \mathbf{G}_{|\mathcal{V}|}\right], \tag{7.15}$$

and let $\tilde{\mathbf{T}}$ be defined similarly with respect to matrices $\tilde{\mathbf{G}}_i$. Then the complete linear transfer function of the network $\mathcal{N}$ is $\boldsymbol{y} = \mathbf{T}\boldsymbol{x} + \tilde{\mathbf{T}}\boldsymbol{z}$. Analog processing of signals without error control implies noise propagation; the additive noise $\boldsymbol{z}$ is also linearly filtered by the network via $\tilde{\mathbf{T}}$.

Example 10. *Fig. 7.2 is the LTN graph of a noisy relay network. Let state* $\boldsymbol{\mu} = [\boldsymbol{y}_{12};\ \boldsymbol{y}_{13};\ \boldsymbol{y}_{23}]$, $\boldsymbol{z} = [\boldsymbol{z}_{12};\ \boldsymbol{z}_{13};\ \boldsymbol{z}_{23}]$, *and output* $\boldsymbol{y}_3 = [\boldsymbol{y}_{13};\ \boldsymbol{y}_{23}]$. *The linear system representation is given as follows,*

$$\boldsymbol{\mu}[t+1] = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{L}_{23} & \mathbf{0} & \mathbf{0} \end{bmatrix} \boldsymbol{\mu}[t] + \begin{bmatrix} \mathbf{L}_{12} \\ \mathbf{L}_{13} \\ \mathbf{0} \end{bmatrix} \boldsymbol{x}_1[t] + \mathbf{I}_c \boldsymbol{z}[t],$$
$$\boldsymbol{y}_3[t] = \begin{bmatrix} \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix} \boldsymbol{\mu}[t].$$

By evaluating Eqn. (7.14),

$$\boldsymbol{y}_3[t] = \begin{bmatrix} \mathbf{L}_{13} \\ \mathbf{L}_{23}\mathbf{L}_{12} \end{bmatrix} \boldsymbol{x}_1[t] + \begin{bmatrix} \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{L}_{23} & \mathbf{0} & \mathbf{I} \end{bmatrix} \boldsymbol{z}[t].$$

Dropping the time indices and writing $\boldsymbol{x} = \boldsymbol{x}_1$ *in addition to* $\boldsymbol{y} = \boldsymbol{y}_3$, *the linear transfer function of the noisy relay network is of the following form:* $\boldsymbol{y} = \mathbf{T}\boldsymbol{x} + \tilde{\mathbf{T}}\boldsymbol{z}$.

7.3.2 Layered Networks

Definition 36 (Layered DAG Network)**.** *A layering of a DAG* $G = (\mathcal{V}, \mathcal{E})$ *is a partition of* $\mathcal{V}$ *into disjoint subsets* $\mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_{p+1}$ *such that if directed edge* $(u, v) \in \mathcal{E}$, *where* $u \in \mathcal{V}_j$ *and* $v \in \mathcal{V}_k$, *then* $j > k$. *A DAG layering (non-unique) is polynomial-time computable [45].*

Given a layered partition $\{\mathcal{V}_\ell\}_{\ell=1}^{p+1}$ of an LTN graph, source nodes $v_i \in \mathcal{S}$ with in-degree $d_i^- = 0$ may be placed in partition $\mathcal{V}_{p+1}$. Similarly, receivers $v_i \in \mathcal{T}$ with out-degree $d_i^+ = 0$ may be placed in partition $\mathcal{V}_1$. The transfer function $\mathbf{T}$ in Eqn. (7.15) may be factored into a product of matrices,

$$\mathbf{T} = \mathbf{T}_{1:p} \triangleq \mathbf{T}_1 \mathbf{T}_2 \cdots \mathbf{T}_p, \tag{7.16}$$

where $\mathbf{T}_\ell$ for $1 \leq \ell \leq p$ is the linear transformation of signals between nodes in partition $\mathcal{V}_{\ell+1}$ and $\mathcal{V}_\ell$ (note the reverse ordering of the $\mathbf{T}_\ell$ with respect to the partitions $\mathcal{V}_\ell$). If an edge exists between nodes in non-consecutive partitions, an identity transform is inserted to replicate signals between multiple layers. Due to the linearity of transforms, for any layered partition $\{\mathcal{V}_\ell\}_{\ell=1}^{p+1}$ of $\mathcal{V}$, the layered transforms $\{\mathbf{T}_\ell\}_{\ell=1}^{p}$ can be constructed. The $\{\mathbf{T}_\ell\}_{\ell=1}^{p}$ are structured matrices comprised of sub-blocks $\mathbf{L}_{ij}$, identity matrices, and/or zero matrices. The block structure is determined by the network topology.

Example 11. *For the multiple unicast network of Fig. 7.1, a valid layered partition of $\mathcal{V}$ is $\mathcal{V}_1 = \{v_5, v_6\}$, $\mathcal{V}_2 = \{v_4\}$, $\mathcal{V}_3 = \{v_3\}$, and $\mathcal{V}_4 = \{v_1, v_2\}$. Let $\boldsymbol{x} = [\boldsymbol{x}_1;\ \boldsymbol{x}_2]$, $\boldsymbol{y} = [\boldsymbol{y}_5;\ \boldsymbol{y}_6] = [\boldsymbol{y}_{15};\ \boldsymbol{y}_{45};\ \boldsymbol{y}_{46};\ \boldsymbol{y}_{26}]$, and let $\mathbf{L}_{34}$ be partitioned as $\mathbf{L}_{34} = [\mathbf{L}'_{34}\ \ \mathbf{L}''_{34}]$. According to the layering, the transfer matrix $\mathbf{T}$ is factored in product form $\mathbf{T} = \mathbf{T}_1\mathbf{T}_2\mathbf{T}_3$,*

$$\mathbf{T} = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{L}_{45} & \mathbf{0} \\ \mathbf{0} & \mathbf{L}_{46} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix} \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{L}'_{34} & \mathbf{L}''_{34} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix} \begin{bmatrix} \mathbf{L}_{15} & \mathbf{0} \\ \mathbf{L}_{13} & \mathbf{0} \\ \mathbf{0} & \mathbf{L}_{23} \\ \mathbf{0} & \mathbf{L}_{26} \end{bmatrix}.$$

Example 12. *Consider the setting of Example 10 for the relay network shown in Fig. 7.2. A valid layered partition of $\mathcal{V}$ is $\mathcal{V}_1 = \{v_3\}$, $\mathcal{V}_2 = \{v_2\}$, $\mathcal{V}_3 = \{v_1\}$. According to the layering, the transfer matrix $\mathbf{T}$ may be written in product form $\mathbf{T} = \mathbf{T}_1\mathbf{T}_2$,*

$$\mathbf{T} = \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{L}_{23} \end{bmatrix} \begin{bmatrix} \mathbf{L}_{13} \\ \mathbf{L}_{12} \end{bmatrix}.$$

7.4 Convex Optimization of Compression-Estimation Matrices

Our optimization method proceeds iteratively over network layers. To simplify the optimization, we first assume ideal channels (high-SNR communication) for which $\boldsymbol{y}_{ij} = \boldsymbol{x}_{ij}$. Then the linear operation of the network $\mathcal{N}$ is $\boldsymbol{y} = \mathbf{T}\boldsymbol{x}$ with $\boldsymbol{z} = \mathbf{0}$. Linear transform coding is constrained according to bandwidth compression ratios α_{ij}.

7.4.1 MSE Distortion at Receivers

According to the linear system equations, Eqns. (7.11)-(7.14), each receiver $v_i \in \mathcal{T}$ receives filtered source observations $\boldsymbol{y}_i = \mathbf{G}_i\boldsymbol{x}$. Receiver v_i applies a linear estimator $\mathbf{B}_i$ to estimate signal $\boldsymbol{r}_i$. The MSE cost of estimation is

$$\begin{aligned} D_i &= E\Big[\big\|\boldsymbol{r}_i - \mathbf{B}_i\mathbf{G}_i\boldsymbol{x}\big\|_2^2\Big] \\ &= \mathrm{tr}\big(\boldsymbol{\Sigma}_{\boldsymbol{r}_i}\big) - 2\mathrm{tr}\big(\mathbf{B}_i\mathbf{G}_i\boldsymbol{\Sigma}_{\boldsymbol{x}\boldsymbol{r}_i}\big) + \mathrm{tr}\big(\mathbf{B}_i\mathbf{G}_i\boldsymbol{\Sigma}_{\boldsymbol{x}}\mathbf{G}_i^T\mathbf{B}_i^T\big). \end{aligned} \tag{7.17}$$

Setting the matrix derivative with respect to $\mathbf{B}_i$ in Eqn. (7.17) to zero yields: $-2\boldsymbol{\Sigma}_{\boldsymbol{r}_i\boldsymbol{x}}\mathbf{G}_i^T + 2\mathbf{B}_i\mathbf{G}_i\boldsymbol{\Sigma}_{\boldsymbol{x}}\mathbf{G}_i^T = 0$. For a fixed transfer function $\mathbf{G}_i$, the optimal LLSE matrix $\mathbf{B}_i^{opt}$ is

$$\mathbf{B}_i^{opt} = \boldsymbol{\Sigma}_{\boldsymbol{r}_i\boldsymbol{x}}\mathbf{G}_i^T\left[\mathbf{G}_i\boldsymbol{\Sigma}_{\boldsymbol{x}}\mathbf{G}_i^T\right]^{-1}. \tag{7.18}$$

If $\mathbf{G}_i$ in Eqn. (7.18) is singular, the inverse may be replaced with a pseudo-inverse operation to compute $\mathbf{B}_i^{opt}$.

Let $\mathbf{B}$ denote a block diagonal global matrix containing individual decoding matrices $\{\mathbf{B}_i\}_{i:v_i\in\mathcal{T}}$ on the diagonal. For an LTN graph $\mathcal{N}$ with encoding transfer function $\mathbf{T} = \mathbf{T}_{1:p}$, we write the linear decoding operation of all receivers as $\hat{\boldsymbol{r}} = \mathbf{B}\boldsymbol{y}$ where $\boldsymbol{y} = \mathbf{T}_{1:p}\boldsymbol{x}$ are the observations received. The weighted MSE cost in Eqn. (7.10) for reconstructing signals $\{\boldsymbol{r}_i\}_{i:v_i\in\mathcal{T}}$ at all receivers is written as

$$\begin{aligned} D_{MSE,\mathbf{W}} &= E\left[\|\boldsymbol{r} - \hat{\boldsymbol{r}}\|_{\mathbf{W}}^2\right] \\ &= E\left[\|\boldsymbol{r} - \mathbf{B}\mathbf{T}_{1:p}\boldsymbol{x}\|_{\mathbf{W}}^2\right] \\ &= \mathrm{tr}\left(\mathbf{W}\boldsymbol{\Sigma}_{\boldsymbol{r}}\mathbf{W}^T\right) - 2\mathrm{tr}\left(\mathbf{W}\mathbf{B}\mathbf{T}_{1:p}\boldsymbol{\Sigma}_{\boldsymbol{x}\boldsymbol{r}}\mathbf{W}^T\right) \\ &\quad + \mathrm{tr}\left(\mathbf{W}\mathbf{B}\mathbf{T}_{1:p}\boldsymbol{\Sigma}_{\boldsymbol{x}}\mathbf{T}_{1:p}^T\mathbf{B}^T\mathbf{W}^T\right). \end{aligned} \tag{7.19}$$

By construction of the weighting matrix $\mathbf{W}$, the MSE in Eqn. (7.19) is a weighted sum of individual distortions at receivers, i.e. $D_{MSE,\mathbf{W}} = \sum_{i:v_i\in\mathcal{T}} w_i\, D_i$.

7.4.2 Computing Encoding Transforms $\mathbf{T}_i$

The optimization of the network transfer function $\mathbf{T} = \mathbf{T}_{1:p}$ is more complex due to block constraints imposed by the network topology on matrices $\{\mathbf{T}_i\}_{i=1}^p$. In order to solve for a particular linear transform $\mathbf{T}_i$, we assume all linear transforms $\mathbf{T}_j$, $j \neq i$ and the receivers' decoding transform $\mathbf{B}$ are fixed. Then the optimal $\mathbf{T}_i$ is the solution to a constrained quadratic program. To derive this, we utilize the following identities in which $\boldsymbol{x} = \mathrm{vec}(\mathbf{X})$:

$$\mathrm{tr}\big(\mathbf{A}^T\mathbf{X}\big) = \mathrm{vec}(\mathbf{A})^T\boldsymbol{x}, \tag{7.20}$$

$$\mathrm{tr}\big(\mathbf{X}^T\mathbf{A}_1\mathbf{X}\mathbf{A}_2\big) = \boldsymbol{x}^T(\mathbf{A}_2 \otimes \mathbf{A}_1)\boldsymbol{x}. \tag{7.21}$$

We write the network's linear transfer function as $\mathbf{T} = \mathbf{T}_{1:p} = \mathbf{T}_{1:i-1}\mathbf{T}_i\mathbf{T}_{i+1:p}$ and define the following matrices

$$\mathbf{J}_i \triangleq \mathbf{T}_{i+1:p}\boldsymbol{\Sigma}_{\boldsymbol{xr}}\mathbf{W}^T\mathbf{W}\mathbf{B}\mathbf{T}_{1:i-1}, \tag{7.22}$$

$$\mathbf{J}'_i \triangleq (\mathbf{T}_{1:i-1})^T\mathbf{B}^T\mathbf{W}^T\mathbf{W}\mathbf{B}\mathbf{T}_{1:i-1}, \tag{7.23}$$

$$\mathbf{J}''_i \triangleq \mathbf{T}_{i+1:p}\boldsymbol{\Sigma}_{\boldsymbol{x}}(\mathbf{T}_{i+1:p})^T. \tag{7.24}$$

To write $D_{MSE,\mathbf{W}}$ in terms of the matrix variable $\mathbf{T}_i$, we also define the following,

$$p_i \triangleq \mathrm{tr}\big(\mathbf{W}\boldsymbol{\Sigma}_{\boldsymbol{r}}\mathbf{W}^T\big), \tag{7.25}$$

$$\boldsymbol{p}_i \triangleq -2\mathrm{vec}\big(\mathbf{J}_i^T\big), \tag{7.26}$$

$$\mathbf{P}_i \triangleq \mathbf{J}''_i \otimes \mathbf{J}'_i, \tag{7.27}$$

where p_i, $\boldsymbol{p}_i$, and $\mathbf{P}_i$ are a scalar, vector, and positive semi-definite matrix respectively. The following lemma expresses $D_{MSE,\mathbf{W}}$ as a function of the unknown matrix variable $\mathbf{T}_i$.

Lemma 23. *Let transforms $\mathbf{T}_j$, $j \neq i$, and $\mathbf{B}$ be fixed. Let $\mathbf{J}_i$, $\mathbf{J}'_i$, $\mathbf{J}''_i$ be defined in Eqns. (7.22)-(7.24), and p_i, $\boldsymbol{p}_i$, and $\mathbf{P}_i$ be defined in Eqns. (7.25)-(7.27). Then the weighted MSE distortion $D_{MSE,\mathbf{W}}$ of Eqn. (7.19) is a quadratic function of $\boldsymbol{t}_i = vec(\mathbf{T}_i)$,*

$$D_{MSE,\mathbf{W}} = \boldsymbol{t}_i^T\mathbf{P}_i\boldsymbol{t}_i + \boldsymbol{p}_i^T\boldsymbol{t}_i + p_i. \tag{7.28}$$

Proof. Substituting the expressions for $\mathbf{J}_i$, $\mathbf{J}'_i$, $\mathbf{J}''_i$ in Eqns. (7.22)-(7.24) into Eqn. (7.19) produces the intermediate equation: $D_{MSE,\mathbf{W}} = \mathrm{tr}\big(\mathbf{T}_i^T\mathbf{J}'_i\mathbf{T}_i\mathbf{J}''_i\big) - 2\mathrm{tr}\big(\mathbf{J}_i\mathbf{T}_i\big) + p_i$. Directly applying the vector-matrix identities of Eqns. (7.20)-(7.21) results in Eqn. (7.28). □

7.4.3 Quadratic Program with Convex Constraints

Due to Lemma 23, the weighted MSE is a quadratic function of $\boldsymbol{t}_i = \mathrm{vec}(\mathbf{T}_i)$ if all other network matrices are fixed. The optimal $\mathbf{T}_i$ must satisfy block constraints determined by network topology. The block constraints are *linear equality constraints* of the form $\boldsymbol{\Phi}_i\boldsymbol{t}_i = \boldsymbol{\phi}_i$. For example, if $\mathbf{T}_i$ contains an identity sub-block, this is enforced by setting entries in $\boldsymbol{t}_i$ to zero and one accordingly, via linear equality constraints.

Theorem 9 (Optimal Encoding)**.** *Let encoding matrices $\mathbf{T}_j$, $j \neq i$ and decoding matrix $\mathbf{B}$ be fixed. Let $\boldsymbol{t}_i = vec(\mathbf{T}_i)$. The optimal encoding transform $\boldsymbol{t}_i$ is given by the following constrained quadratic program (QP) [15, Def. 4.34]*

$$\begin{aligned} \arg\min_{\boldsymbol{t}_i} \quad & \boldsymbol{t}_i^T\mathbf{P}_i\boldsymbol{t}_i + \boldsymbol{p}_i^T\boldsymbol{t}_i + p_i \\ s.\ t. \quad & \boldsymbol{\Phi}_i\boldsymbol{t}_i = \boldsymbol{\phi}_i, \end{aligned} \tag{7.29}$$

Algorithm 1 IDEAL-COMPRESSION-ESTIMATION($\mathcal{N}$, $\mathbf{W}$, ϵ)

Identify compression matrices $\{\mathbf{T}_i\}_{i=1}^p$ and corresponding linear equalities $\{\mathbf{\Phi}_i, \boldsymbol{\phi}_i\}_{i=1}^p$ for network $\mathcal{N}$. Identify estimation matrices $\{\mathbf{B}_i\}_{i:v_i \in \mathcal{T}}$. [Sec. 7.3, Sec. 7.4.3]
Initialize $\{\mathbf{T}_i^{(0)}\}_{i=1}^p$ randomly to feasible matrices.
Set $n = 1$, $D_{MSE,\mathbf{W}}(0) = \infty$.
repeat
  Compute $\{\mathbf{B}_i^{(n)}\}_{i:v_i \in \mathcal{T}}$ given $\{\mathbf{T}_k^{(n-1)}\}_{k=1}^p$. [Eqn. (7.18)]
  for $i = 1 : p$ **do**
    Compute $\mathbf{T}_i^{(n)}$ given $\{\mathbf{\Phi}_i, \boldsymbol{\phi}_i\}$, $\{\mathbf{B}_k^{(n)}\}_{k:v_k \in \mathcal{T}}$, $\{\mathbf{T}_k^{(n)}\}_{k=1}^{(i-1)}$, $\{\mathbf{T}_k^{(n-1)}\}_{k=i+1}^p$. [Theorem 9]
  end for
  Compute $D_{MSE,\mathbf{W}}(n)$. [Eqn. (7.19)]
  Set $\Delta_{MSE,\mathbf{W}} = D_{MSE,\mathbf{W}}(n) - D_{MSE,\mathbf{W}}(n-1)$.
  Set $n = n + 1$.
until $\Delta_{MSE,\mathbf{W}} \leq \epsilon$ or $n \geq N_{max}$.
return $\{\mathbf{T}_i^{(n)}\}_{i=1}^p$, $\{\mathbf{B}_i^{(n)}\}_{i:v_i \in \mathcal{T}}$.

where $(\mathbf{\Phi}_i, \boldsymbol{\phi}_i)$ *represent linear equality constraints on elements of* $\mathbf{T}_i$*. The solution to the above optimization for* $\boldsymbol{t}_i$ *is obtained by solving a corresponding linear system*

$$\begin{bmatrix} 2\mathbf{P}_i & \mathbf{\Phi}_i^T \\ \mathbf{\Phi}_i & \mathbf{0} \end{bmatrix} \begin{bmatrix} \boldsymbol{t}_i \\ \boldsymbol{\lambda} \end{bmatrix} = \begin{bmatrix} -\boldsymbol{p}_i \\ \boldsymbol{\phi}_i \end{bmatrix}. \tag{7.30}$$

If the constraints determined by the pair $(\mathbf{\Phi}_i, \boldsymbol{\phi}_i)$ *are feasible, the linear system of Eqn. (7.30) is guaranteed to have either one or infinitely many solutions.*

Proof. The QP of Eqn. (7.29) follows from Lemma 23 with additional linear equality constraints placed on $\boldsymbol{t}_i$. The closed form solution to the QP is derived using Lagrange dual multipliers for the linear constraints, and the Karush-Kuhn-Tucker (KKT) conditions. Let $f(\boldsymbol{t}_i, \boldsymbol{\lambda})$ represent the Lagrangian formed with dual vector variable $\boldsymbol{\lambda}$ for the constraints,

$$f(\boldsymbol{t}_i, \boldsymbol{\lambda}) = \boldsymbol{t}_i^T \mathbf{P}_i \boldsymbol{t}_i + \boldsymbol{p}_i^T \boldsymbol{t}_i + p_i + \boldsymbol{\lambda}^T (\mathbf{\Phi}_i \boldsymbol{t}_i - \boldsymbol{\phi}_i), \tag{7.31}$$

$$\nabla_{\boldsymbol{t}_i} f(\boldsymbol{t}_i, \boldsymbol{\lambda}) = 2\mathbf{P}_i \boldsymbol{t}_i + \boldsymbol{p}_i + \mathbf{\Phi}_i^T \boldsymbol{\lambda}, \tag{7.32}$$

$$\nabla_{\boldsymbol{\lambda}} f(\boldsymbol{t}_i, \boldsymbol{\lambda}) = \mathbf{\Phi}_i \boldsymbol{t}_i - \boldsymbol{\phi}_i. \tag{7.33}$$

Setting $\nabla_{\boldsymbol{t}_i} f(\boldsymbol{t}_i, \boldsymbol{\lambda}) = \mathbf{0}$ and $\nabla_{\boldsymbol{\lambda}} f(\boldsymbol{t}_i, \boldsymbol{\lambda}) = \mathbf{0}$ yields the linear system of Eqn. (7.30), the solutions to which are $\boldsymbol{t}_i$ and dual vector $\boldsymbol{\lambda}$. Since the MSE distortion is bounded by a minimum of zero error, the linear system has a unique solution if $\mathbf{P}_i$ is full rank, or infinitely many solutions of equivalent objective value if $\mathbf{P}_i$ is singular. □

Remark 22. *Beyond linear constraints, several other convex constraints on matrix variables could be applied within the quadratic program. For example, the* ℓ_1*-norm of a vector* $\boldsymbol{x} \in \mathbb{R}^n$ *defined by* $\|\boldsymbol{x}\|_1 \triangleq \sum_i |x_i|$ *is often used in compressed sensing to enforce* sparsity.

7.5 Iterative Algorithm

Algorithm 1 defines an iterative method to optimize all encoding matrices $\{\mathbf{T}_i\}_{i=1}^p$ and the global decoding matrix $\mathbf{B}$ for an LTN graph. The iterative algorithm begins with the random initialization of the encoding matrices $\{\mathbf{T}_i\}_{i=1}^p$ subject to size specifications and linear equality constraints given by $\{\mathbf{\Phi}_i\}_{i=1}^p$ and $\{\boldsymbol{\phi}_i\}_{i=1}^p$. The iterative method proceeds by solving for the optimal $\mathbf{B}$ transform first. Similarly, with $\mathbf{T}_j, j \neq i$ and $\mathbf{B}$ fixed, the optimal $\mathbf{T}_i$ is computed using Theorem 9. The iterative method proceeds for $n \leq N_{max}$ iterations or until the difference in error $\Delta_{MSE,\mathbf{W}}$ is less than a prescribed tolerance ϵ.

7.5.1 Convergence to Stationary Points

A key property of Algorithm 1 is the convergence to a stationary point (either local minimum or saddle-point) of the weighted MSE.

Theorem 10 (Local Convergence)**.** *Denote the network's linear transfer function after the n-th outer-loop iteration in Algorithm 1 by $\mathbf{T}^{(n)}$, and the block-diagonal global decoding transform by $\mathbf{B}^{(n)}$ which contains matrices $\{\mathbf{B}_i^{(n)}\}_{i:v_i\in\mathcal{T}}$ on the diagonal. Let $\hat{\boldsymbol{r}}^{(n)} = \mathbf{B}^{(n)}\mathbf{T}^{(n)}\boldsymbol{x}$ denote the estimate of desired signal $\boldsymbol{r}$. Then*

$$E\left[\left\|\boldsymbol{r}-\hat{\boldsymbol{r}}^{(n)}\right\|_{\mathbf{W}}^2\right] \geq E\left[\left\|\boldsymbol{r}-\hat{\boldsymbol{r}}^{(n+1)}\right\|_{\mathbf{W}}^2\right], \tag{7.34}$$

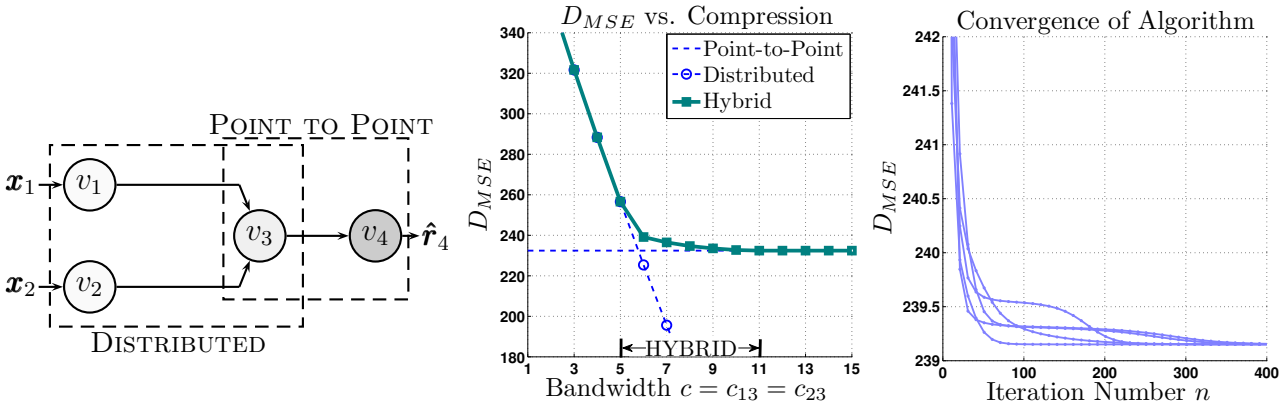
i.e., the weighted MSE distortion is a nonincreasing function of the iteration number n.

Proof. In Step 5 of Algorithm 1, with matrices $\{\mathbf{T}_k^{(n-1)}\}_{k=1}^p$ fixed, the optimal transform $\mathbf{B}^{(n)}$ is determined to minimize $D_{MSE,\mathbf{W}}$. The current transform $\mathbf{B}^{(n-1)}$ is feasible within the optimization space which implies that the MSE distortion cannot increase. In Step 7 of the inner loop, with matrices $\mathbf{B}^{(n)}$, $\{\mathbf{T}_k^{(n)}\}_{k=1}^{(i-1)}$, and $\{\mathbf{T}_k^{(n-1)}\}_{k=i+1}^p$ fixed, Theorem 9 computes the optimal transform $\mathbf{T}_i^{(n)}$ to minimize $D_{MSE,\mathbf{W}}$. A similar argument shows that the error term cannot increase. The distortion sequence $\{D_{MSE,\mathbf{W}}(n)\}$ is nonincreasing and nonnegative; hence $\lim_{n\to\infty} D_{MSE,\mathbf{W}}(n) = \inf\{D_{MSE,\mathbf{W}}(n)\}$ by monotone convergence. □

Remark 23. *The local convergence in Theorem 10 is affected by several factors: (i) The covariance structure $\mathbf{\Sigma}_{\boldsymbol{x}}$ of the source; (ii) The DAG structure of G; (iii) The schedule of iterative optimization of local matrices and factorization of $\mathbf{T}$ into the $\mathbf{T}_i$; (iv) The random initialization of $\{\mathbf{T}_i\}_{i=1}^p$. In practice, multiple executions of Algorithm 1 increase the probability of converging to a global minimum.*

7.6 Example: A Multi-Hop Network

Consider the noiseless multi-hop network of Fig. 7.3 in which a relay aggregates, compresses and/or forwards its observations to a receiver. The network is a hybrid combination of a distributed and point-to-point network.



(a) LTN Block Diagram (b) Distortion vs. Compression (c) Convergence

Figure 7.3: (*a*) Block diagram of the "hybrid network" example. (*b*) The end-to-end distortion vs. compression for varying bandwidth $c = c_{13} = c_{23}$. (*c*) Convergence of $D_{MSE}(n)$ for five different initializations of the iterative algorithm for the operating point $c = 6, c_{34} = 11$.

Example 13 ("Hybrid Network"). *High-dimensional, correlated signals* $\boldsymbol{x}_1 \in \mathbb{R}^{n_1}$ *and* $\boldsymbol{x}_2 \in \mathbb{R}^{n_2}$ *are observed at nodes* v_1 *and* v_2 *where* $n_1 = n_2 = 15$ *dimensions. The covariance* $\boldsymbol{\Sigma}_{\boldsymbol{x}}$ *of the global source* $\boldsymbol{x} = [\boldsymbol{x}_1;\ \boldsymbol{x}_2]$ *was generated as follows for the experiment, ensuring* $\boldsymbol{\Sigma}_{\boldsymbol{x}} \succ \mathbf{0}$. *The diagonal entries* (i,i) *of* $\boldsymbol{\Sigma}_{\boldsymbol{x}}$ *were selected as* $15 + 2U_{ii}$, *and off-diagonal entries* (i,j) *for* $j > i$ *were selected as* $1 + 2U_{ij}$ *where* U_{ii} *and* U_{ij} *are i.i.d. uniform random variables over the interval* $[0,1]$.

The linear transfer function is factored in the form $\mathbf{T} = \mathbf{T}_1\mathbf{T}_2$ *where* $\mathbf{T}_1 = \mathbf{L}_{34}$ *and*

$$\mathbf{T}_2 = \begin{bmatrix} \mathbf{L}_{13} & \mathbf{0} \\ \mathbf{0} & \mathbf{L}_{23} \end{bmatrix}.$$

The target reconstruction at v_4 *is the entire signal* $\boldsymbol{r}_4 = \boldsymbol{x}$. *The bandwidth* $c_{34} = 11$, *while bandwidth* $c = c_{13} = c_{23}$ *is varied for the experiment. Depending on the amount of bandwidth* c, *the network operates in one of three modes (distributed, hybrid, or point-to-point) as described in Example 13. Fig. 7.3(b) plots the sum distortion vs. compression performance, and Fig. 7.3(c) plots the convergence of Algorithm 1 for the operating point* $c = 6$, $c_{34} = 11$.

7.7 Analysis of Noisy Networks

We now analyze communication for networks with non-ideal channels: $\boldsymbol{y}_{ij} = \boldsymbol{x}_{ij} + \boldsymbol{z}_{ij}$. Edges (i,j) represent vector Gaussian channels. Network communication is limited according to both bandwidth compression ratios α_{ij} and signal-to-noise ratios SNR_{ij}. We simplify optimization of subspaces by restricting attention to single-layer multi-source, multi-receiver networks for which $\mathcal{V} = \mathcal{S} \cup \mathcal{T}$. In this case, the linear transfer function is $\boldsymbol{y} = \mathbf{T}\boldsymbol{x} + \boldsymbol{z}$, i.e. the noise is additive but not filtered over multiple network layers.

Table 7.1: A "HYBRID" LINEAR TRANSFORM NETWORK

Network Modes	*Bandwidth*
Distributed	$c \leq \lfloor \frac{c_{34}}{2} \rfloor$
Hybrid	$\lceil \frac{c_{34}}{2} \rceil < c < c_{34}$
Point to Point	$c_{34} \leq c$

7.7.1 MSE Distortion at Receivers

Each receiver $v_i \in \mathcal{T}$ receives observations $\boldsymbol{y}_i = \mathbf{G}_i\boldsymbol{x} + \boldsymbol{z}_i$ where $\boldsymbol{z}_i$ is the noise to v_i. The MSE distortion for reconstructing $\boldsymbol{r}_i$ at receiver v_i is given by,

$$\begin{aligned}\tilde{D}_i = \mathrm{tr}\big(\boldsymbol{\Sigma}_{\boldsymbol{r}}\big) - 2\mathrm{tr}\big(\mathbf{B}_i\mathbf{G}_i\boldsymbol{\Sigma}_{\boldsymbol{x}\boldsymbol{r}_i}\big) + \mathrm{tr}\big(\mathbf{B}_i\boldsymbol{\Sigma}_{\boldsymbol{z}_i}\mathbf{B}_i^T\big) \\ + \mathrm{tr}\big(\mathbf{B}_i\mathbf{G}_i\boldsymbol{\Sigma}_{\boldsymbol{x}}\mathbf{G}_i^T\mathbf{B}_i^T\big).\end{aligned} \tag{7.35}$$

Setting the matrix derivative with respect to $\mathbf{B}_i$ in Eqn. (7.35) to zero yields the optimal linear transform $\mathbf{B}_i$ (cf. Eqn. (7.18)),

$$\mathbf{B}_i^{opt} = \boldsymbol{\Sigma}_{\boldsymbol{r}_i\boldsymbol{x}}\mathbf{G}_i^T\Big[\mathbf{G}_i\boldsymbol{\Sigma}_{\boldsymbol{x}}\mathbf{G}_i^T + \boldsymbol{\Sigma}_{\boldsymbol{z}_i}\Big]^{-1}. \tag{7.36}$$

Combining the LLSE estimates as $\hat{\boldsymbol{r}} = \mathbf{B}\boldsymbol{y}$, where $\boldsymbol{y} = \mathbf{T}\boldsymbol{x} + \boldsymbol{z}$, the weighted MSE for all receivers is given by

$$\begin{aligned}\tilde{D}_{MSE,\mathbf{W}} &= E\Big[\big\|\boldsymbol{r} - \hat{\boldsymbol{r}}\big\|_{\mathbf{W}}^2\Big] \\ &= E\Big[\big\|\boldsymbol{r} - \mathbf{B}(\mathbf{T}\boldsymbol{x} + \boldsymbol{z})\big\|_{\mathbf{W}}^2\Big] \\ &= \mathrm{tr}\big(\mathbf{W}\mathbf{B}\mathbf{T}\boldsymbol{\Sigma}_{\boldsymbol{x}}\mathbf{T}^T\mathbf{B}^T\mathbf{W}^T\big) - 2\mathrm{tr}\big(\mathbf{W}\mathbf{B}\mathbf{T}\boldsymbol{\Sigma}_{\boldsymbol{x}\boldsymbol{r}}\mathbf{W}^T\big) \\ &\quad + \mathrm{tr}\big(\mathbf{W}\boldsymbol{\Sigma}_{\boldsymbol{r}}\mathbf{W}^T\big) + \mathrm{tr}\big(\mathbf{W}\mathbf{B}\boldsymbol{\Sigma}_{\boldsymbol{z}}\mathbf{B}^T\mathbf{W}^T\big).\end{aligned} \tag{7.37}$$

By construction of the weighting matrix $\mathbf{W}$, the MSE in Eqn. (7.37) is a weighted sum of individual distortions at receivers, i.e. $\tilde{D}_{MSE,\mathbf{W}} = \sum_i w_i\,\tilde{D}_i$.

7.7.2 Computing Encoding Transform T

For noisy networks, power constraints on channel inputs limit the amount of amplification of transmitted signals. For single-layer networks, let $v_i \in \mathcal{S}$ be a source node with observed signal $\boldsymbol{x}_i$. A power constraint on the input to channel $(i,j) \in \mathcal{E}$ is given by

$$E[\|\boldsymbol{x}_{ij}\|_2^2] = E[\|\mathbf{L}_{ij}\boldsymbol{x}_i\|_2^2] = \mathrm{tr}\big(\mathbf{L}_{ij}\boldsymbol{\Sigma}_{\boldsymbol{x}_i}\mathbf{L}_{ij}^T\big) \leq P_{ij}. \tag{7.38}$$

The power constraint in Eqn. (7.38) is a quadratic function of the entries of the global linear transform $\mathbf{T}$. More precisely, let $\boldsymbol{\ell}_{ij} = \mathrm{vec}(\mathbf{L}_{ij})$ and $\boldsymbol{t} = \mathrm{vec}(\mathbf{T})$. Since $\boldsymbol{t}$ contains all variables

Algorithm 2 NOISY-COMPRESSION-ESTIMATION$(\mathcal{N}, \mathbf{W}, \epsilon)$

1: Identify compression matrix $\mathbf{T}$ and corresponding linear equality constraints $(\boldsymbol{\Phi}, \boldsymbol{\phi})$, and quadratic power constraints $\{(\boldsymbol{\Gamma}_{ij}, P_{ij})\}_{(i,j)\in\mathcal{E}}$. Identify estimation matrices $\{\mathbf{B}_i\}_{i:v_i\in\mathcal{T}}$. [Sec. 7.3, Sec. 7.7.2]
2: Initialize $\mathbf{T}^{(0)}$ randomly to a feasible matrix.
3: Set $n = 1$, $\tilde{D}_{MSE,\mathbf{W}}(0) = \infty$.
4: **repeat**
5: Compute $\{\mathbf{B}_i^{(n)}\}_{i:v_i\in\mathcal{T}}$ given $\mathbf{T}^{(n-1)}$. [Eqn. (7.36)]
6: Compute $\mathbf{T}^{(n)}$ given $\{\mathbf{B}_i^{(n)}\}_{i:v_i\in\mathcal{T}}$, $(\boldsymbol{\Phi}, \boldsymbol{\phi})$, $\{(\boldsymbol{\Gamma}_{ij}, P_{ij})\}_{(i,j)\in\mathcal{E}}$. [Theorem 11]
7: Compute $\tilde{D}_{MSE,\mathbf{W}}(n)$. [Eqn. (7.37)]
8: Set $\tilde{\Delta}_{MSE,\mathbf{W}} = \tilde{D}_{MSE,\mathbf{W}}(n) - \tilde{D}_{MSE,\mathbf{W}}(n-1)$.
9: Set $n = n + 1$.
10: **until** $\tilde{\Delta}_{MSE,\mathbf{W}} \leq \epsilon$ or $n \geq N_{max}$.
11: **return** $\mathbf{T}^{(n)}$ and $\{\mathbf{B}_i^{(n)}\}_{i:v_i\in\mathcal{T}}$.

of $\boldsymbol{\ell}_{ij}$, we may write $\boldsymbol{\ell}_{ij} = \mathbf{J}_{ij}\boldsymbol{t}$ where $\mathbf{J}_{ij}$ selects variables from $\boldsymbol{t}$. Using the matrix-vector identities of Eqn. (7.21), the power constraint in Eqn. (7.38) can be written as

$$\begin{aligned}\operatorname{tr}\left(\mathbf{L}_{ij}\boldsymbol{\Sigma}_{\boldsymbol{x}_i}\mathbf{L}_{ij}^T\right) &= \boldsymbol{\ell}_{ij}^T\left(\boldsymbol{\Sigma}_{\boldsymbol{x}_i}\otimes\mathbf{I}\right)\boldsymbol{\ell}_{ij} \\ &= \boldsymbol{t}^T\mathbf{J}_{ij}^T\left(\boldsymbol{\Sigma}_{\boldsymbol{x}_i}\otimes\mathbf{I}\right)\mathbf{J}_{ij}\boldsymbol{t}. \end{aligned} \tag{7.39}$$

Letting $\boldsymbol{\Gamma}_{ij} \triangleq \mathbf{J}_{ij}^T\left(\boldsymbol{\Sigma}_{\boldsymbol{x}_i}\otimes\mathbf{I}\right)\mathbf{J}_{ij}$, the quadratic constraint is $\boldsymbol{t}^T\boldsymbol{\Gamma}_{ij}\boldsymbol{t} \leq P_{ij}$. The matrix $\boldsymbol{\Gamma}_{ij}$ is a symmetric, positive semi-definite matrix. Thus a power constraint is a quadratic, convex constraint.

7.7.3 Quadratic Program with Convex Constraints

As in Section 7.4.2, we use the vector form $\boldsymbol{t} = \operatorname{vec}(\mathbf{T})$ to enforce linear equality constraints $\boldsymbol{\Phi}\boldsymbol{t} = \boldsymbol{\phi}$. For noisy networks, we include power constraints $\boldsymbol{t}^T\boldsymbol{\Gamma}_{ij}\boldsymbol{t} \leq P_{ij}$ for each channel $(i,j) \in \mathcal{E}$. For a fixed global decoding transform $\mathbf{B}$, the distortion $\tilde{D}_{MSE,\mathbf{W}}$ of Eqn. (7.37) is again a quadratic function of $\boldsymbol{t}$. Using the compact notation

$$p \triangleq \operatorname{tr}\left(\mathbf{W}\boldsymbol{\Sigma}_{\boldsymbol{r}}\mathbf{W}^T\right) + \operatorname{tr}\left(\mathbf{W}\mathbf{B}\boldsymbol{\Sigma}_{\boldsymbol{z}}\mathbf{B}^T\mathbf{W}^T\right), \tag{7.40}$$

$$\boldsymbol{p} \triangleq -2\operatorname{vec}\left(\mathbf{B}^T\mathbf{W}^T\mathbf{W}\boldsymbol{\Sigma}_{\boldsymbol{rx}}\right), \tag{7.41}$$

$$\mathbf{P} \triangleq \boldsymbol{\Sigma}_{\boldsymbol{x}}\otimes\mathbf{B}^T\mathbf{W}^T\mathbf{W}\mathbf{B}, \tag{7.42}$$

a derivation identical to that of Lemma 23 yields $\tilde{D}_{MSE,\mathbf{W}} = \boldsymbol{t}^T\mathbf{P}\boldsymbol{t} + \boldsymbol{p}^T\boldsymbol{t} + p$. The optimal encoding transform $\mathbf{T}$ for single-layer noisy networks is solvable via a quadratic program with quadratic constraints (QCQP), following the development of Eqns. (7.40)-(7.42), and the power constraints given in Eqns. (7.38)-(7.39); cf. Theorem 9.

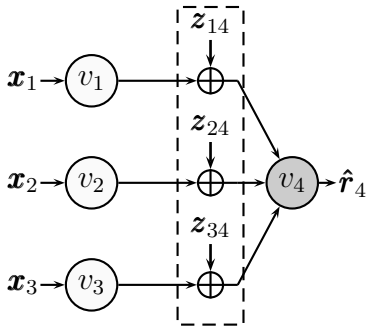


Figure 7.4: Block diagram of a distributed network with noise and power constraints.

Theorem 11 (Optimal Encoding $\mathbf{T}$ for Noisy LTN)**.** *Let $\mathcal{N}$ be a single-layer LTN, $\mathbf{B}$ be the fixed decoding transform, and $\boldsymbol{t} = vec(\mathbf{T})$ be the encoding transform. The optimal encoding $\boldsymbol{t}$ is the solution to the following quadratic program with quadratic constraints (QCQP):*

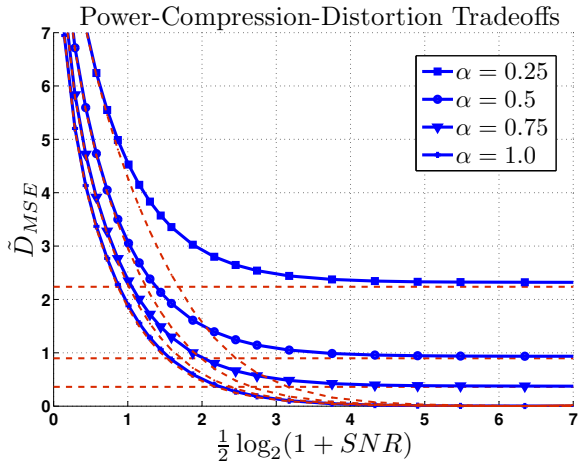
$$\begin{aligned} \arg\min_{\boldsymbol{t}} \quad & \boldsymbol{t}^T \mathbf{P} \boldsymbol{t} + \boldsymbol{p}^T \boldsymbol{t} + p \\ s.\ t. \quad & \boldsymbol{\Phi} \boldsymbol{t} = \boldsymbol{\phi}, \\ & \boldsymbol{t}^T \boldsymbol{\Gamma}_{ij} \boldsymbol{t} \leq P_{ij}, \quad (i,j) \in \mathcal{E}, \end{aligned} \tag{7.43}$$

where $(\boldsymbol{\Phi}, \boldsymbol{\phi})$ represent linear equality constraints (dictated by network topology), and where $\{(\boldsymbol{\Gamma}_{ij}, P_{ij})\}_{(i,j)\in\mathcal{E}}$ represent quadratic power constraints on variables of $\mathbf{T}$.

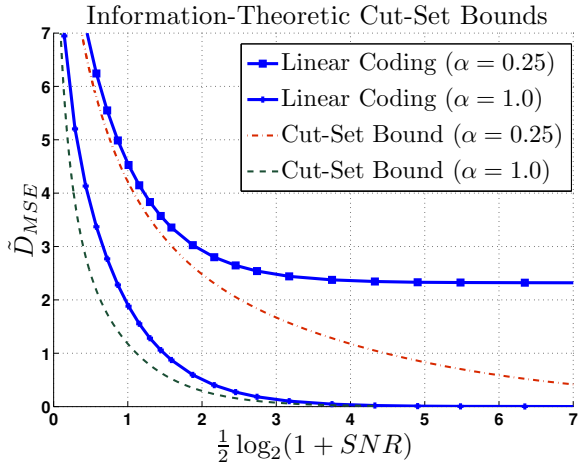
Remark 24. *A quadratic program with linear and convex quadratic constraints is solvable efficiently via standard convex program solvers; the time complexity depends polynomially on the number of matrix variables and constraints.*

7.7.4 Iterative Algorithm and Convergence

Algorithm 2 defines an iterative algorithm for single-layer, noise/power limited networks. In addition to subspace selection, the amount of power per subspace is determined iteratively. The iterative method alternates between optimizing the global decoding transform $\mathbf{B}$ and the global encoding transform $\mathbf{T}$, ensuring that network topology and power constraints are satisfied. As in Theorem 10, the weighted MSE distortion is a nonincreasing function of the iteration number, i.e. $\tilde{D}_{MSE,\mathbf{W}}(n) \geq \tilde{D}_{MSE,\mathbf{W}}(n+1)$. While convergence to a stationary point is guaranteed, the optimization space is highly complex– a globally optimal solution is not guaranteed.



(a) Compression-Estimation Tradeoffs



(b) Cut-Set Lower Bounds (Information Theory)

Figure 7.5: (a) Power-compression-distortion "spectra" of a distributed noisy network for varying compression ratios α and SNR levels. Unmarked, red, dashed lines represent cut-set lower bounds for linear coding based on convex relaxations. (b) For $\alpha \in \{0.25, 1.0\}$, the results due to low-complexity linear transforms are measured with respect to information-theoretic cut-set bounds.

7.8 Example: A Distributed Noisy Network

Fig. 7.4 diagrams a classic example of a distributed network with multiple source (sensor) nodes transmitting signal projections to a central decoder. Each source node is power constrained and must transmit a compressed description of its observed signal over a noisy vector channel.

Example 14 (Distributed LTN). *In Fig. 7.4, the global source* $\boldsymbol{x} = [\boldsymbol{x}_1;\ \boldsymbol{x}_2;\ \boldsymbol{x}_3]$ *is chosen to be a* jointly Gaussian *vector with* $n = 12$ *dimensions, and* $n_i = 4$ *for each of* $|\mathcal{S}| = 3$ *source nodes. Here, we specify the exact distribution of* $\boldsymbol{x}$ *in order to provide information-theoretic*

lower bounds. We set the covariance of $\boldsymbol{x}$ *to be Gauss-Markov with* $\rho = 0.8$,

$$\boldsymbol{\Sigma}_{\boldsymbol{x}} = \begin{bmatrix} 1 & \rho & \rho^2 & \dots & \rho^{11} \\ \rho & 1 & \rho & \dots & \rho^{10} \\ \rho^2 & \rho & 1 & \dots & \rho^9 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \rho^{11} & \rho^{10} & \rho^9 & \dots & 1 \end{bmatrix}.$$

The network structure is specified by bandwidths $c_{14} = c_{24} = c_{34} = c$. *The global encoding transform* $\mathbf{T}$ *is block-diagonal with matrices* $\mathbf{L}_{14}$, $\mathbf{L}_{24}$, *and* $\mathbf{L}_{34}$ *on the diagonal. The compression ratio is varied equally for each source node,* $\alpha = \frac{c}{n_i}$ *where* $n_i = 4$. *The noise variables* $\boldsymbol{z}_{ij}$ *are i.i.d. Gaussian random vectors with zero-mean and identity covariances. The power constraints are set as* $P_1 = P_2 = P_3 = c(SNR)$, *where* $SNR_{ij} = SNR$ *for all links. The goal of destination* v_4 *is to reconstruct the entire source* $\boldsymbol{r}_4 = \boldsymbol{x}$. *Fig. 7.5(a) plots the performance of LTN optimization for varying* α *and* SNR *ratios as well as cut-set lower bounds for linear coding based on convex relaxations. Cut-set lower bounds for linear coding for this example are explained further in Section 8.4.1. Fig. 7.5(b) plots cut-set bounds based on information theory which are explained further in Sections 8.5 and 8.5.5. In the high-SNR setting, information-theoretic coding strategies are capable of zero-distortion; however, in the low-SNR setting, linear coding achieves a competitive MSE performance while maintaining zero-delay and low-complexity.*

Remark 25 (Comparison with [36, 83])**.** *For this example, as the* $SNR \to \infty$, *the error* $\tilde{D}_{MSE}$ *approaches the error associated to the distributed KLT [36] where channel noise was not considered. In [83], the authors model the effects of channel noise; however, they do not provide cut-set lower bounds. In addition, the iterative optimization of the present paper optimizes all compression matrices simultaneously per iteration and allows arbitrary convex constraints, as opposed to the schemes in both [36, 83] which optimize the encoding matrix of each user separately per iteration.*

Chapter 8

Cut-Set Bounds

8.1 Cutting a Graph

In this section, we derive lower bounds on the minimum MSE distortion possible for linear compression and estimation of correlated signals in the LTN model. Our main technique is to relax an arbitrary acyclic graph along all possible graph cuts to point-to-point networks with side information. The cut-set bounds provide a performance benchmark for the iterative methods of Sections 7.4-7.7.

8.1.1 Point-to-Point Network with Side Information

Consider the point-to-point network of Fig. 8.1. Source node v_1 compresses source $\boldsymbol{x} \in \mathbb{R}^n$ via a linear transform $\mathbf{L}_{12}$. The signal $\boldsymbol{x}_{12} \in \mathbb{R}^{c_{12}}$ is transmitted where $\boldsymbol{x}_{12} = \mathbf{L}_{12}\boldsymbol{x}$ and $E[\|\boldsymbol{x}_{12}\|_2^2] \leq P$. Receiver v_2 computes a linear estimate of desired signal $\boldsymbol{r} \in \mathbb{R}^r$ using observations $\boldsymbol{y}_{12} = \boldsymbol{x}_{12} + \boldsymbol{z}$ and side information $\boldsymbol{s} \in \mathbb{R}^s$ as follows,

$$\hat{\boldsymbol{r}} = \mathbf{B}\begin{bmatrix}\boldsymbol{y}_{12}\\ \boldsymbol{s}\end{bmatrix} = \begin{bmatrix}\mathbf{B}_{11} & \mathbf{B}_{12}\end{bmatrix}\begin{bmatrix}\boldsymbol{y}_{12}\\ \boldsymbol{s}\end{bmatrix}. \tag{8.1}$$

The decoding transform $\mathbf{B}$ is here partitioned into two sub-matrices $\mathbf{B}_{11}$ and $\mathbf{B}_{12}$. We will find it convenient to define the following random vectors,

$$\boldsymbol{\xi} \triangleq \boldsymbol{x} - \boldsymbol{\Sigma}_{\boldsymbol{xs}}\boldsymbol{\Sigma}_{\boldsymbol{s}}^{-1}\boldsymbol{s}, \tag{8.2}$$

$$\boldsymbol{\nu} \triangleq \boldsymbol{r} - \boldsymbol{\Sigma}_{\boldsymbol{rs}}\boldsymbol{\Sigma}_{\boldsymbol{s}}^{-1}\boldsymbol{s}. \tag{8.3}$$

Signals $\boldsymbol{\xi}$ and $\boldsymbol{\nu}$ are innovation vectors. For example, $\boldsymbol{\xi}$ is the difference between $\boldsymbol{x}$ and the linear least squares estimate of $\boldsymbol{x}$ given $\boldsymbol{s}$ which is equivalent to $\boldsymbol{\Sigma}_{\boldsymbol{xs}}\boldsymbol{\Sigma}_{\boldsymbol{s}}^{-1}\boldsymbol{s}$.

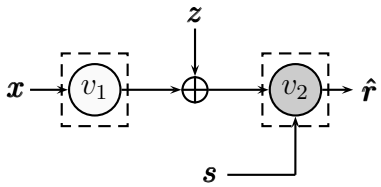


Figure 8.1: A point-to-point network with a power-constrained transmitter, additive channel noise, and side information available at the receiver.

8.2 Case I: Relaxation to Ideal Vector Channel

In the ideal case, $P = \infty$ or $\boldsymbol{z} = 0$. The weighted, linear minimum MSE distortion of the point-to-point network with side information is obtained by solving

$$\begin{aligned} D^*_{ideal} &= \min_{\mathbf{L}_{12},\mathbf{B}} \quad E\Big[\big\|\boldsymbol{r}-\hat{\boldsymbol{r}}\big\|^2_{\mathbf{W}}\Big], \\ &= \min_{\mathbf{L}_{12},\mathbf{B}_{11},\mathbf{B}_{12}} E\Big[\big\|\boldsymbol{r}-(\mathbf{B}_{11}\mathbf{L}_{12}\boldsymbol{x}+\mathbf{B}_{12}\boldsymbol{s})\big\|^2_{\mathbf{W}}\Big]. \end{aligned} \tag{8.4}$$

The following theorem specifies the solution to Eqn. (8.4).

Theorem 12 (Ideal Network Relaxation)**.** *Let $\boldsymbol{x} \in \mathbb{R}^n$, $\boldsymbol{s} \in \mathbb{R}^s$, and $\boldsymbol{r} \in \mathbb{R}^r$ be zero-mean random vectors with given full-rank covariance matrices $\boldsymbol{\Sigma}_{\boldsymbol{x}}$, $\boldsymbol{\Sigma}_{\boldsymbol{s}}$, $\boldsymbol{\Sigma}_{\boldsymbol{r}}$ and cross-covariances $\boldsymbol{\Sigma}_{\boldsymbol{rx}}$, $\boldsymbol{\Sigma}_{\boldsymbol{rs}}$, $\boldsymbol{\Sigma}_{\boldsymbol{xs}}$. Let $\boldsymbol{\xi}$ and $\boldsymbol{\nu}$ be the innovations defined in Eqn (8.2) and Eqn. (8.3) respectively. The solution to the minimization of Eqn. (8.4) over matrices $\mathbf{L}_{12} \in \mathbb{R}^{c_{12}\times n}$, $\mathbf{B}_{11} \in \mathbb{R}^{r\times c_{12}}$, and $\mathbf{B}_{12} \in \mathbb{R}^{r\times s}$ is obtained in closed form as*

$$D^*_{ideal} = tr\big(\boldsymbol{\Sigma}_{\boldsymbol{\nu}}\mathbf{W}^T\mathbf{W}\big) - \sum_{j=1}^{c_{12}} \lambda_j, \tag{8.5}$$

where $\{\lambda_j\}_{j=1}^{c_{12}}$ are the c_{12} largest eigenvalues of the matrix $\mathbf{W}\boldsymbol{\Sigma}_{\boldsymbol{\nu\xi}}\boldsymbol{\Sigma}_{\boldsymbol{\xi}}^{-1}\boldsymbol{\Sigma}_{\boldsymbol{\xi\nu}}\mathbf{W}^T$.

Proof. The optimization in Eqn. (8.4) is simplified by first determining the LMMSE optimal $\mathbf{B}_{12}$ transform in terms of $\mathbf{B}_{11}$ and $\mathbf{L}_{12}$: $\mathbf{B}_{12}^{opt} = \boldsymbol{\Sigma}_{\boldsymbol{rs}}\boldsymbol{\Sigma}_{\boldsymbol{s}}^{-1} - \mathbf{B}_{11}\mathbf{L}_{12}\boldsymbol{\Sigma}_{\boldsymbol{xs}}\boldsymbol{\Sigma}_{\boldsymbol{s}}^{-1}$. Plugging $\mathbf{B}_{12}^{opt}$ into Eqn. (8.4) yields a minimization over $\mathbf{B}_{11}$ and $\mathbf{L}_{12}$ only. By grouping and rearranging variables in terms of innovation vectors $\boldsymbol{\xi}$ and $\boldsymbol{\nu}$,

$$D^*_{ideal} = \min_{\mathbf{L}_{12},\mathbf{B}_{11}} E\Big[\big\|\boldsymbol{\nu}-\mathbf{B}_{11}\mathbf{L}_{12}\boldsymbol{\xi}\big\|^2_{\mathbf{W}}\Big]. \tag{8.6}$$

The optimization of Eqn. (8.6) is that of an equivalent point-to-point network with input signal $\boldsymbol{\xi}$ and desired reconstruction $\boldsymbol{\nu}$, without side information. Eqn. (8.6) is in standard form and solvable using canonical correlation analysis as detailed in [17, p. 368]. The optimal value D^*_{ideal} is given in Eqn. (8.5) in terms of the eigenvalues of $\mathbf{W}\boldsymbol{\Sigma}_{\boldsymbol{\nu\xi}}\boldsymbol{\Sigma}_{\boldsymbol{\xi}}^{-1}\boldsymbol{\Sigma}_{\boldsymbol{\xi\nu}}\mathbf{W}^T$. □

8.3 Case II: Semi-Definite Programming Relaxation

In the case of additive noise $\boldsymbol{z}$ (here with assumed covariance $\boldsymbol{\Sigma}_{\boldsymbol{z}} = \mathbf{I}$ for compactness) and a power-constrained input to the vector channel, the weighted, linear minimum MSE distortion is obtained by solving

$$\begin{aligned} D^*_{noisy} = \min_{\mathbf{L}_{12},\mathbf{B}_{11},\mathbf{B}_{12}} & E\Big[\big\|\boldsymbol{r} - (\mathbf{B}_{11}(\mathbf{L}_{12}\boldsymbol{x} + \boldsymbol{z}) + \mathbf{B}_{12}\boldsymbol{s})\big\|^2_{\mathbf{W}}\Big], \\ \text{s.t.} \quad & \text{tr}[\mathbf{L}_{12}\boldsymbol{\Sigma}_{\boldsymbol{x}}\mathbf{L}_{12}^T] \leq P. \end{aligned} \tag{8.7}$$

Again, by solving for the optimal LMMSE matrix $\mathbf{B}_{12}$ and grouping terms in the resulting optimization according to innovation vectors $\boldsymbol{\xi}$ and $\boldsymbol{\nu}$,

$$\begin{aligned} D^*_{noisy} = \min_{\mathbf{L}_{12},\mathbf{B}_{11}} & E\Big[\big\|\boldsymbol{\nu} - (\mathbf{B}_{11}(\mathbf{L}_{12}\boldsymbol{\xi} + \boldsymbol{z}))\big\|^2_{\mathbf{W}}\Big], \\ \text{s.t.} \quad & \text{tr}[\mathbf{L}_{12}\boldsymbol{\Sigma}_{\boldsymbol{x}}\mathbf{L}_{12}^T] \leq P. \end{aligned} \tag{8.8}$$

Remark 26. *The exact solution to Eqn. (8.8) involves handling a quadratic power constraint and a rank constraint due to the reduced-dimensionality of* $\mathbf{L}_{12}$*. In [83, Theorem 4], a related optimization problem was solved via a Lagrangian relaxation. For our problem, we take a simpler approach using a semi-definite programming (SDP) relaxation. We first note that* $D^*_{noisy} \geq D^*_{ideal}$*. In the high-SNR regime, the two distortion values are asymptotically equivalent. Therefore, we compute a good approximation for the distortion* D^*_{noisy} *in the low-SNR regime via the following SDP relaxation.*

Theorem 13 (SDP Relaxation)**.** *Consider random vectors* $\boldsymbol{x}$*,* $\boldsymbol{s}$*,* $\boldsymbol{r}$*,* $\boldsymbol{\xi}$*,* $\boldsymbol{\nu}$*, and matrices* $\mathbf{L}_{12}$*,* $\mathbf{B}_{11}$ *as defined in Theorem 12. In addition, let random vector* $\boldsymbol{z}$ *have zero-mean and covariance* $\boldsymbol{\Sigma}_{\boldsymbol{z}} = \mathbf{I}$*. Let* $\boldsymbol{\Psi} \triangleq \mathbf{L}_{12}^T\mathbf{L}_{12}$ *and* $\boldsymbol{\Phi} \in \mathbb{R}^{r\times r}$ *be an arbitrary positive semi-definite matrix where* r *is the dimension of random vector* $\boldsymbol{r}$*. The following lower bound applies,*

$$\begin{aligned} D^*_{noisy} \geq \min_{\boldsymbol{\Phi},\boldsymbol{\Psi}} \quad & tr[\boldsymbol{\Phi}] + tr\big[\mathbf{W}\big[\boldsymbol{\Sigma}_{\boldsymbol{\nu}} - \boldsymbol{\Sigma}_{\boldsymbol{\nu\xi}}\boldsymbol{\Sigma}_{\boldsymbol{\xi}}^{-1}\boldsymbol{\Sigma}_{\boldsymbol{\xi\nu}}\big]\mathbf{W}^T\big], \\ s.t. \quad & tr[\boldsymbol{\Sigma}_{\boldsymbol{x}}\boldsymbol{\Psi}] \leq P, \quad \boldsymbol{\Psi} \succeq \mathbf{0}, \\ & \begin{bmatrix} \boldsymbol{\Phi} & \mathbf{W}\boldsymbol{\Sigma}_{\boldsymbol{\nu\xi}}\boldsymbol{\Sigma}_{\boldsymbol{\xi}}^{-1} \\ \boldsymbol{\Sigma}_{\boldsymbol{\xi}}^{-1}\boldsymbol{\Sigma}_{\boldsymbol{\xi\nu}}\mathbf{W}^T & \boldsymbol{\Sigma}_{\boldsymbol{\xi}}^{-1} + \boldsymbol{\Psi} \end{bmatrix} \succeq \mathbf{0}. \end{aligned} \tag{8.9}$$

The proof of Theorem 13 is based on a rank relaxation as detailed in the Appendix. The power constraint is still enforced in Eqn. (8.9). In the low-SNR regime, power allocation over subspaces dominates the error performance. If we denote the solution to the SDP of Theorem 13 as D^*_{sdp}, we arrive at the following characterization,

$$D^*_{noisy} \geq \max\{D^*_{ideal}, D^*_{sdp}\}. \tag{8.10}$$

8.4 Cut-Set Lower Bounds for Linear Coding

Consider an LTN graph $\mathcal{N}$ with source nodes $\mathcal{S} \subset \mathcal{V}$ and receivers $\mathcal{T} \subset \mathcal{V}$. We assume that $\mathcal{S} \cap \mathcal{T} = \emptyset$, i.e. the set of sources and receivers are disjoint. The total bandwidth and total power across a *cut* $\mathcal{F} \subset \mathcal{V}$ are defined respectively as

$$C(\mathcal{F}) = \sum_{\substack{jk \in \mathcal{E} \\ j \in \mathcal{F},\ k \in \mathcal{F}^c}} c_{jk}, \tag{8.11}$$

$$P(\mathcal{F}) = \sum_{\substack{jk \in \mathcal{E} \\ j \in \mathcal{F},\ k \in \mathcal{F}^c}} P_{jk}, \tag{8.12}$$

where the edge set $\mathcal{E}$ and bandwidths c_{jk} were defined in Section 7.2. The edges of the graph are directed, hence the bandwidth across a cut accounts for the c_{ij} only for those edges directed from node v_i to v_j. In the following theorem, the notation $\boldsymbol{x}_{\mathcal{F}}$ denotes the concatenation of vectors $\boldsymbol{x}_i : v_i \in \mathcal{F}$. The set $\mathcal{F}^c$ denotes the complement of $\mathcal{F}$ in $\mathcal{V}$.

Definition 37. $D^*_{ideal}\left[\boldsymbol{x}, \boldsymbol{r} \middle| \boldsymbol{s}; c, \mathbf{W}\right]$ *represents the distortion* D^*_{ideal} *computed with the weighted norm via* $\mathbf{W}$ *for the ideal point-to-point network with input* $\boldsymbol{x}$*, bandwidth* c*, reconstruction vector* $\boldsymbol{r}$*, and side information to receiver* $\boldsymbol{s}$*. Similarly,* $D^*_{noisy}\left[\boldsymbol{x}, \boldsymbol{r} \middle| \boldsymbol{s}; c, P, \mathbf{W}\right]$ *represents the distortion* D^*_{noisy} *for a noisy point-to-point network with channel-input power constraint* P *and noise vector* $\boldsymbol{z}$ *with zero-mean with identity covariance.*

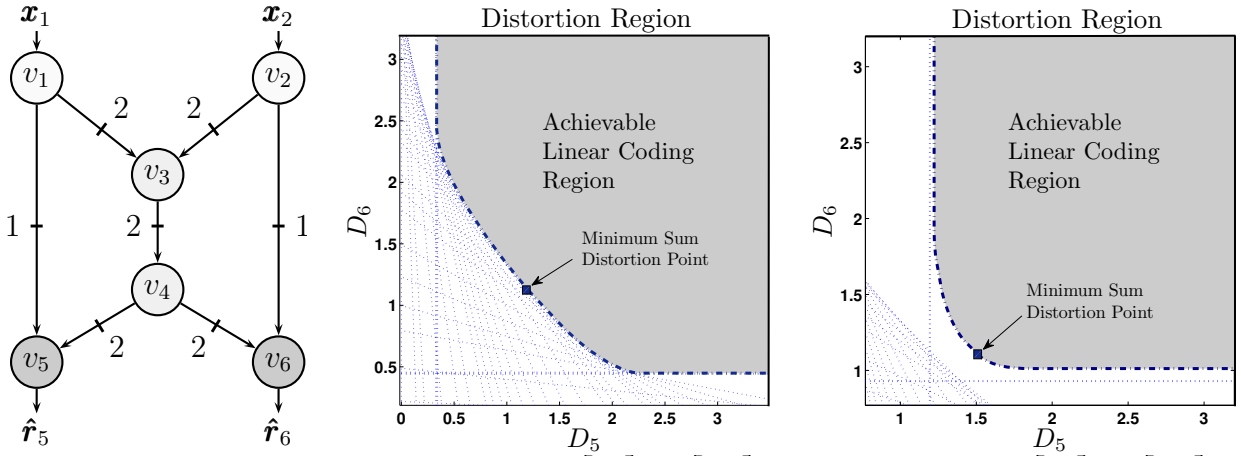
Theorem 14 (Cut-Set Lower Bounds)**.** *Let* $\mathcal{N}$ *be an arbitrary LTN graph with source nodes* $\mathcal{S}$ *and receivers* $\mathcal{T}$*. Let* $\mathcal{F} \subset \mathcal{V}$ *be a cut of the graph. For ideal channel communication,*

$$E\left[\left\|\boldsymbol{r}_{\mathcal{F}^c} - \hat{\boldsymbol{r}}_{\mathcal{F}^c}\right\|^2_{\mathbf{W}}\right] \geq D^*_{ideal}\left[\boldsymbol{x}_{\mathcal{F}}, \boldsymbol{r}_{\mathcal{F}^c} \middle| \boldsymbol{x}_{\mathcal{F}^c}; C(\mathcal{F}), \mathbf{W}\right]. \tag{8.13}$$

In the case of noisy channel communication over network $\mathcal{N}$ *with additive channel noise* $\boldsymbol{z}_{ij}$ *(assumed zero-mean, identity covariance),*

$$E\left[\left\|\boldsymbol{r}_{\mathcal{F}^c} - \hat{\boldsymbol{r}}_{\mathcal{F}^c}\right\|^2_{\mathbf{W}}\right] \geq D^*_{noisy}\left[\boldsymbol{x}_{\mathcal{F}}, \boldsymbol{r}_{\mathcal{F}^c} \middle| \boldsymbol{x}_{\mathcal{F}^c}; C(\mathcal{F}), P(\mathcal{F}), \mathbf{W}\right]. \tag{8.14}$$

Proof. The LTN graph is partitioned into two sets $\mathcal{F}$ and $\mathcal{F}^c$. The source nodes $v_i \in \mathcal{F}$ are merged as one source "super" node, and the receivers $v_i \in \mathcal{F}^c$ are merged into one receiver "super" node. The maximum bandwidth and maximum power between the source and receiver are $C(\mathcal{F})$ and $P(\mathcal{F})$ respectively. The random vector $\boldsymbol{x}_{\mathcal{F}^c}$ represents those signals with channels to the receiver super node, not accounted for in the cut $\mathcal{F}$; hence, this information is given as side information (a relaxation) to the receiver. The relaxed network after the merging process is the point-to-point network of Fig. 8.1 with noise $\boldsymbol{z}$ of dimension equal to the bandwidth $C(\mathcal{F})$ of the cut, and provides a lower bound on the MSE distortion $E\left[\left\|\boldsymbol{r}_{\mathcal{F}^c} - \hat{\boldsymbol{r}}_{\mathcal{F}^c}\right\|^2_{\mathbf{W}}\right]$ at receivers $v_i \in \mathcal{F}^c$. □



(a) LTN Block Diagram (b) Estimate: $\begin{bmatrix}\boldsymbol{r}_5\\ \boldsymbol{r}_6\end{bmatrix} = \begin{bmatrix}\boldsymbol{x}_1\\ \boldsymbol{x}_2\end{bmatrix}$ (c) Estimate: $\begin{bmatrix}\boldsymbol{r}_5\\ \boldsymbol{r}_6\end{bmatrix} = \begin{bmatrix}\boldsymbol{x}_2\\ \boldsymbol{x}_1\end{bmatrix}$

Figure 8.2: (a) Block diagram of a multi-source, multi-destination ideal network with labeled bandwidths c_{ij}. (b) The distortion region assuming that node v_5 reconstructs $\boldsymbol{x}_1$, and node v_6 reconstructs $\boldsymbol{x}_2$. (c) The distortion region assuming that node v_5 reconstructs $\boldsymbol{x}_2$, and node v_6 reconstructs $\boldsymbol{x}_1$.

Remark 27. *The total number of distinct cuts $\mathcal{F}$ separating sources and receivers is $(2^{|\mathcal{S}|}-1)(2^{|\mathcal{T}|}-1)$. For a particular cut, there exists a continuum of lower bounds for multi-receiver networks depending on the choice of weighting $\mathbf{W}$.*

8.4.1 Example: Cut-Set Lower Bounds for Linear Coding

In Fig. 7.5(a), cut-set lower bounds for linear coding are illustrated based on Theorem 14 for a distributed noisy network. The bounds are depicted for the cut that separates all sources from the receiver. Due to our approximation method in Eqn. (8.10) based on the SDP relaxation, the lower bounds show tight agreement in the low-SNR and high-SNR asymptotic regimes.

8.5 Cut-Set Lower Bound From Information Theory

For the point-to-point communication scenario illustrated in Fig. 8.1, the optimal performance can be determined precisely. Consider an ℓ-length sequence $\{(\boldsymbol{x}[t],\boldsymbol{s}[t])\}_{t=1}^{\ell}$ of jointly *i.i.d.* random vectors. The source node v_1 has access to the source sequence $\{\boldsymbol{x}[t]\}_{t=1}^{\ell}$. We will assume throughout that $\boldsymbol{r}$ (respectively $\boldsymbol{r}[t]$) is a deterministic function of $(\boldsymbol{x},\boldsymbol{s})$ (respectively $(\boldsymbol{x}[t],\boldsymbol{s}[t])$). The goal of receiver v_2 is to minimize the *average* MSE distortion $D_\ell = E\left[\frac{1}{\ell}\sum_{t=1}^{\ell}\|\boldsymbol{r}[t]-\hat{\boldsymbol{r}}[t]\|_2^2\right]$ where the reconstruction sequence $\{\hat{\boldsymbol{r}}[t]\}_{t=1}^{\ell}$ is generated based on access to side information $\{\boldsymbol{s}[t]\}_{t=1}^{\ell}$ and the sequence of channel output vectors. We study the performance in the limit as $\ell\to\infty$ and denote $D \triangleq D_\infty$.

8.5.1 Source-Channel Separation

We establish a lower bound by combining the data processing inequality with the definitions of Wyner-Ziv rate-distortion function and channel capacity. Specifically, by straightforward extension of [91], the minimum rate $R(D)$ required to reconstruct $\{\boldsymbol{r}[t]\}_{t=1}^{\infty}$ at distortion D is given by $R(D) = \min I(\boldsymbol{x};\boldsymbol{u}|\boldsymbol{s})$ where the minimization is over all "auxiliary" random vectors $\boldsymbol{u}$ for which $p(\boldsymbol{u},\boldsymbol{x},\boldsymbol{s}) = p(\boldsymbol{u}|\boldsymbol{x})p(\boldsymbol{x},\boldsymbol{s})$ and for which $E[\|\boldsymbol{r} - E[\boldsymbol{r}|\boldsymbol{u},\boldsymbol{s}]\|_2^2] \leq D$. Furthermore, by definition of the channel capacity $C(P)$ between v_1 and v_2, $C(P) = \max_{p(\boldsymbol{x}_{12}):E\left[\|\boldsymbol{x}_{12}\|_2^2\right]\leq P} I(\boldsymbol{x}_{12};\boldsymbol{y}_{12})$.[1] Source-channel separation applies to the scenario of Fig. 8.1, and in a nearly identical proof as detailed in [37, Thm. 1.10],

$$R(D) \leq C(P). \tag{8.15}$$

8.5.2 $R(D)$ for Jointly Gaussian Sources

If $\{(\boldsymbol{r}[t],\boldsymbol{x}[t],\boldsymbol{s}[t])\}$ form an *i.i.d.* sequence of jointly Gaussian random vectors, then $R(D)$ is equal to the conditional rate-distortion function [36, Appendix II],

$$R_c(D) = \min_{p(\hat{\boldsymbol{r}}|\boldsymbol{x},\boldsymbol{s}):E\left[\|\boldsymbol{r}-\hat{\boldsymbol{r}}\|_2^2\right]\leq D} I(\boldsymbol{x};\hat{\boldsymbol{r}}|\boldsymbol{s}). \tag{8.16}$$

8.5.3 Capacity of the Vector AWGN Channel

If the channel noise $\boldsymbol{z}$ is a Gaussian random vector with zero mean and covariance $\boldsymbol{\Sigma}_{\boldsymbol{z}} = \mathbf{I}$, the capacity of the channel in Fig. 8.1 with bandwidth c_{12} and power constraint P is

$$C(P) = \frac{c_{12}}{2}\log_2\left[1 + \frac{P}{c_{12}}\right]. \tag{8.17}$$

8.5.4 Lower Bound

We utilize Eqn. (8.15) to obtain an information-theoretic lower bound to the distortion achievable in any network of the type considered in this paper. An arbitrary graph is reduced via graph cuts to point-to-point networks. The following theorem collects the known information-theoretic results discussed.

Theorem 15 (Cut-Set Bounds: Information Theory)**.** *Let $\mathcal{N}$ be an arbitrary LTN graph with vector AWGN channels. Consider a cut $\mathcal{F} \subset \mathcal{V}$ separating the graph into a point-to-point network with bandwidth $C(\mathcal{F})$ and power $P(\mathcal{F})$. Let $R(D^*_{opt})$ be the rate-distortion function for the source $\boldsymbol{x}_{\mathcal{F}}$ with side information $\boldsymbol{x}_{\mathcal{F}^c}$ and reconstruction $\boldsymbol{r}_{\mathcal{F}^c}$.*[2] *Then*

$$R(D^*_{opt}) \leq \frac{C(\mathcal{F})}{2}\log_2\left[1 + \frac{P(\mathcal{F})}{C(\mathcal{F})}\right]. \tag{8.18}$$

[1] The notation in information theory vs. signal processing differs. The term $I(\boldsymbol{x}_{12};\boldsymbol{y}_{12})$ denotes the mutual information between random vectors whereas the term $p(\boldsymbol{x}_{12})$ indicates a probability distribution.

[2] We assume that $\boldsymbol{r}_{\mathcal{F}^c}$ is a deterministic function of the global source $\boldsymbol{x}$.

8.5.5 Example: Cut-Set Lower Bound From Information Theory

For the noisy network in Example 14, consider cut $\mathcal{F} = \{v_1, v_2, v_3\}$. The source signal $\boldsymbol{x}_{\mathcal{F}} = \boldsymbol{x} = [\boldsymbol{x}_1; \boldsymbol{x}_2; \boldsymbol{x}_3]$ is jointly Gaussian, the side information is absent, and $\boldsymbol{r}_{\mathcal{F}^c} = \boldsymbol{x}$. Denote the eigenvalues of the source $\boldsymbol{x}_{\mathcal{F}}$ as $\{\lambda_{\boldsymbol{x},i}\}_{i=1}^n$. Evaluating Eqn. (8.16) as in [36, Appendix II], optimal source coding corresponds to reverse water-filling over the eigenvalues (see also [21, Chap. 10]),

$$R_c(D^*_{opt}) = \sum_{i=1}^{n} \max\left\{\frac{1}{2}\log_2 \frac{\lambda_{\boldsymbol{x},i}}{D_i}, 0\right\},$$

$$\text{where } D_i = \begin{cases} \theta & \text{if } \theta < \lambda_{\boldsymbol{x},i} \\ \lambda_{\boldsymbol{x},i} & \text{if } \theta \geq \lambda_{\boldsymbol{x},i} \end{cases}$$

and where θ is chosen such that $\sum_{i=1}^n D_i = D^*_{opt}$. The lower bound of Eqn. (8.18) is plotted in Fig. 7.5(b) for two different bandwidth compression ratios.

8.6 Example: Multi-Source, Multi-Receiver Network

Example 15 (Multiple Unicast)**.** *In Fig. 8.2, the global source* $\boldsymbol{x} = [\boldsymbol{x}_1;\ \boldsymbol{x}_2]$ *where* $\boldsymbol{x}_1 \in \mathbb{R}^4$ *and* $\boldsymbol{x}_2 \in \mathbb{R}^4$*. The correlation structure of* $\boldsymbol{x}$ *is given by the following matrices,*

$$\left[\begin{array}{c|c} \boldsymbol{\Sigma}_{11} & \boldsymbol{\Sigma}_{12} \\ \hline \boldsymbol{\Sigma}_{21} & \boldsymbol{\Sigma}_{22} \end{array}\right] = \left[\begin{array}{cccc:cccc} 2.4 & 1.1 & 0.4 & 0.0 & 0.1 & 0.1 & 0.0 & 0.1 \\ 1.1 & 1.7 & 0.8 & 0.4 & 0.0 & 0.2 & 0.2 & 0.1 \\ 0.4 & 0.8 & 1.2 & 0.0 & 0.2 & 0.6 & 0.1 & 0.3 \\ 0.0 & 0.4 & 0.0 & 0.8 & 0.3 & 0.0 & 0.1 & 0.0 \\ \hdashline 0.1 & 0.0 & 0.2 & 0.3 & 1.1 & 0.1 & 0.2 & 0.0 \\ 0.1 & 0.2 & 0.6 & 0.0 & 0.1 & 1.2 & 0.2 & 0.1 \\ 0.0 & 0.2 & 0.1 & 0.1 & 0.2 & 0.2 & 1.0 & 0.6 \\ 0.1 & 0.1 & 0.3 & 0.0 & 0.0 & 0.1 & 0.6 & 1.2 \end{array}\right]. \tag{8.20}$$

Although the network is symmetric, the source covariance matrix given in Eqn. (8.20) includes cross-correlations which cause the distortion plots to appear asymmetric. The network structure is specified by bandwidths c_{ij} *as labeled in Fig. 8.2(a). The factorization of the global linear transform* $\mathbf{T}$ *was given in Example 11 of Section 7.4.*

The distortion region for the network in the case when node v_5 *estimates* $\boldsymbol{r}_5 = \boldsymbol{x}_1$*, and node* v_6 *estimates* $\boldsymbol{r}_6 = \boldsymbol{x}_2$ *is given in Fig. 8.2(b). A direct link exists from each source to receiver. However, if the desired reconstruction at the receivers is switched as in Fig. 8.2(c), the channel from* v_3 *to* v_4 *must be shared fully and becomes a bottleneck. The cut-set bounds of interest are shown in dotted lines. The shaded region depicts the points achievable via the iterative method of Section 7.4. In Fig. 8.2(c), the upper and lower bounds are not tight everywhere–even if one receiver is completely ignored, the resulting problem is still a distributed compression problem for which tight bounds are not known. The achievable*

Table 8.1: Comparison of Reduced-Dimension Linear Transforms

Design Method	*Fig.* 5(*b*) $D_5 + D_6$	*Fig.* 5(*c*) $D_5 + D_6$
Random Projections	4.3170	6.3471
Routing and Network Coding	2.7029	3.8170
Iterative QP Optimization	2.3258	2.6165
⟨*Lower Bound*⟩	2.3243	2.3243

curve was generated by taking the convex hull of 32 *points corresponding to weighting ratios* $\frac{w_5}{w_6} \in [\frac{1}{100}, 100]$.

In Table 8.1, we compare the results of linear transform design methods for the minimum sum distortion point (weighting ratio $\frac{w_5}{w_6} = 1$*).*

- Random Projections– *Each entry for all compression matrices is selected from the standard normal distribution. The sum distortion* $D_5 + D_6$ *is averaged over* 10^2 *random compression matrices selected for all nodes.*

- Routing and Network Coding (Ad-Hoc)– *For the scenario in Fig. 8.2(b), nodes* v_1 *and* v_2 *project their signal onto the principal eigenvectors of* $\mathbf{\Sigma}_{11}$ *and* $\mathbf{\Sigma}_{22}$ *respectively. Routing permits each receiver to receive the best two eigenvector projections from its corresponding source, as well as an extra projection from the other source. For Fig. 8.2(c), using a simple "network coding" strategy of adding signals at* v_3*, one receiver is able to receive its best two eigenvector projections, but the other receiver can only receive one best eigenvector projection.*

- Iterative QP Optimization– *Linear transforms are designed using the iterative method of Section 7.4.*

- Lower Bound– *The minimum sum distortion possible due to the cut-set lower bound of Theorem 14.*

8.6.1 Concluding Remarks

The linear transform network (LTN) was proposed to model the aggregation, compression, and estimation of correlated random signals in directed, acyclic graphs. For both noiseless and noisy LTN graphs, a new iterative algorithm was introduced for the joint optimization of reduced-dimension network matrices. Cut-set lower bounds were introduced for zero-delay linear coding based on convex relaxations. Cut-set lower bounds for optimal coding were introduced based on information-theoretic principles. The compression-estimation tradeoffs were analyzed for several example networks. A future challenge remains to compute tighter

lower bounds and relaxations for non-convex network optimization problems. Reduced-dimension linear transforms have potential applications in data fusion and sensor networks. The idea of exploiting correlations between network signals to reduce data transmission, and the idea of approximate reconstruction as opposed to exact recovery at receivers may lead to further advances in networking.

8.7 Proof of Theorem 13

Starting from the optimization in Eqn. (8.8), the LLSE optimal matrix

$$\mathbf{B}_{11}^{opt} = \mathbf{\Sigma}_{\boldsymbol{\nu\xi}}\mathbf{L}_{12}^T(\mathbf{L}_{12}\mathbf{\Sigma}_{\boldsymbol{\xi}}\mathbf{L}_{12}^T + \mathbf{I})^{-1},$$

assuming $\mathbf{\Sigma}_{\boldsymbol{z}} = \mathbf{I}$. Substituting this expression and simplifying the objective function in Eqn. (8.8),

$$\begin{aligned} D_{noisy}^* = \min_{\mathbf{L}_{12}} \quad & \mathrm{tr}\left[\mathbf{W}\mathbf{\Sigma}_{\boldsymbol{\nu}}\mathbf{W}^T\right] \\ & + \mathrm{tr}\left[\mathbf{W}\mathbf{\Sigma}_{\boldsymbol{\nu\xi}}\mathbf{L}_{12}^T\left[\mathbf{L}_{12}\mathbf{\Sigma}_{\boldsymbol{\xi}}\mathbf{L}_{12}^T + \mathbf{I}\right]^{-1}\mathbf{L}_{12}\mathbf{\Sigma}_{\boldsymbol{\xi\nu}}\mathbf{W}^T\right] \\ \text{s.t.} \quad & \mathrm{tr}\left[\mathbf{L}_{12}\mathbf{\Sigma}_{\boldsymbol{x}}\mathbf{L}_{12}^T\right] \leq P. \end{aligned} \tag{8.21}$$

Applying the Woodbury (matrix-inversion) identity [15, C.4.3] to the objective function,

$$\begin{aligned} D_{noisy}^* = \min_{\mathbf{L}_{12}} \quad & \mathrm{tr}\left[\mathbf{W}\mathbf{\Sigma}_{\boldsymbol{\nu}}\mathbf{W}^T\right] - \mathrm{tr}\left[\mathbf{W}\mathbf{\Sigma}_{\boldsymbol{\nu\xi}}\mathbf{\Sigma}_{\boldsymbol{\xi}}^{-1}\mathbf{\Sigma}_{\boldsymbol{\xi\nu}}\mathbf{W}^T\right] \\ & + \mathrm{tr}\left[\mathbf{W}\mathbf{\Sigma}_{\boldsymbol{\nu\xi}}\mathbf{\Sigma}_{\boldsymbol{\xi}}^{-1}\left[\mathbf{\Sigma}_{\boldsymbol{\xi}}^{-1} + \mathbf{L}_{12}^T\mathbf{L}_{12}\right]^{-1}\mathbf{\Sigma}_{\boldsymbol{\xi}}^{-1}\mathbf{\Sigma}_{\boldsymbol{\xi\nu}}\mathbf{W}^T\right] \\ \text{s.t.} \quad & \mathrm{tr}\left[\mathbf{L}_{12}\mathbf{\Sigma}_{\boldsymbol{x}}\mathbf{L}_{12}^T\right] \leq P. \end{aligned} \tag{8.22}$$

Introducing a positive semi-definite matrix $\mathbf{\Phi}$ such that

$$\mathbf{\Phi} \succeq \mathbf{W}\mathbf{\Sigma}_{\boldsymbol{\nu\xi}}\mathbf{\Sigma}_{\boldsymbol{\xi}}^{-1}\left[\mathbf{\Sigma}_{\boldsymbol{\xi}}^{-1} + \mathbf{L}_{12}^T\mathbf{L}_{12}\right]^{-1}\mathbf{\Sigma}_{\boldsymbol{\xi}}^{-1}\mathbf{\Sigma}_{\boldsymbol{\xi\nu}}\mathbf{W}^T,$$

written equivalently in Schur-complement form [15, A.5.5], and setting $\mathbf{\Psi} = \mathbf{L}_{12}^T\mathbf{L}_{12} \in \mathbb{R}^{n\times n}$ as a rank c_{12} matrix,

$$\begin{aligned} D_{noisy}^* = \min_{\mathbf{\Phi},\mathbf{\Psi}} \quad & \mathrm{tr}\left[\mathbf{\Phi}\right] + \mathrm{tr}\left[\mathbf{W}\left[\mathbf{\Sigma}_{\boldsymbol{\nu}} - \mathbf{\Sigma}_{\boldsymbol{\nu\xi}}\mathbf{\Sigma}_{\boldsymbol{\xi}}^{-1}\mathbf{\Sigma}_{\boldsymbol{\xi\nu}}\right]\mathbf{W}^T\right], \\ \text{s.t.} \quad & \mathrm{tr}\left[\mathbf{\Sigma}_{\boldsymbol{x}}\mathbf{\Psi}\right] \leq P, \quad \mathbf{\Psi} \succeq \mathbf{0}, \quad \mathrm{rank}\left[\mathbf{\Psi}\right] = c_{12}, \\ & \begin{bmatrix} \mathbf{\Phi} & \mathbf{W}\mathbf{\Sigma}_{\boldsymbol{\nu\xi}}\mathbf{\Sigma}_{\boldsymbol{\xi}}^{-1} \\ \mathbf{\Sigma}_{\boldsymbol{\xi}}^{-1}\mathbf{\Sigma}_{\boldsymbol{\xi\nu}}\mathbf{W}^T & \mathbf{\Sigma}_{\boldsymbol{\xi}}^{-1} + \mathbf{\Psi} \end{bmatrix} \succeq \mathbf{0}. \end{aligned} \tag{8.23}$$

Dropping the rank constraint yields the relaxation of Eqn. (8.9).

Bibliography

[1] E. Abbe. Randomness and dependencies extraction via polarization. In *Proc. of the Information Theory and Applications (ITA) Workshop*, San Diego, California, February 2011.

[2] E. Abbe and E. Telatar. Polar codes for the m-user multiple access channel. *IEEE Transactions on Information Theory*, 58(8):5437 –5448, August 2012. ISSN 0018-9448. doi: 10.1109/TIT.2012.2201374.

[3] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Network information flow. *IEEE Tran. on Info. Theory*, 46(4), July 2000.

[4] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund. Nested polar codes for wiretap and relay channels. *IEEE Communications Letters*, 14(8):752–754, August 2010. ISSN 1089-7798.

[5] R. Appuswamy, M. Franceschetti, N. Karamchandani, and K. Zeger. Network coding for computing: Cut-set bounds. *IEEE Transactions on Information Theory*, 57:1015–1030, February 2011.

[6] E. Arıkan. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Transactions on Information Theory*, 55(7):3051–3073, July 2009.

[7] E. Arıkan. Source polarization. In *Proc. of the IEEE International Symposium on Information Theory*, June 2010.

[8] E. Arıkan. Polar coding for the slepian-wolf problem based on monotone chain rules. In *Proc. of the International Symposium on Information Theory*, July 2012.

[9] E. Arıkan and E. Telatar. On the rate of channel polarization. In *Proc. of the IEEE International Symposium on Information Theory*, Seoul, South Korea, July 2009.

[10] Salman Avestimehr, Suhas Diggavi, and David Tse. Wireless network information flow: A deterministic approach. *IEEE Transactions on Information Theory*, 57(4):1872–1905, April 2011.

[11] W. Bajwa, J. Haupt, A. Sayeed, and R. Nowak. Joint source-channel communication for distributed estimation in sensor networks. *IEEE Tran. Info. Theory*, 53:3629–3653, October 2007.

[12] Z. Bar-Yossef, Y. Birk, T. S. Jayram, and T. Kol. Index coding with side information. *IEEE Transactions on Information Theory*, 57(3):1479–1494, 2011.

[13] D. Baron, M. B. Wakin, M. F. Duarte, S. Sarvotham, and R. G. Baraniuk. Distributed compressed sensing. Available at: http://dsp.rice.edu/cs.

[14] R. Blasco-Serrano, R. Thobaben, M. Andersson, V. Rathi, and M. Skoglund. Polar codes for cooperative relaying. *IEEE Transactions on Communications*, 60(11):3263–3273, November 2012. ISSN 0090-6778.

[15] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, Cambridge, 2004.

[16] A. Braunstein, F. Kayhan, G. Montorsi, and R. Zecchina. Encoding for the blackwell channel with reinforced belief propagation. In *Proc. of the IEEE International Symposium on Information Theory*, Nice, France, 2007.

[17] D. R. Brillinger. *Time Series: Data Analysis and Theory*. Holden-Day, San Francisco, 1981.

[18] Viveck R. Cadambe and Syed A. Jafar. Interference alignment and the degree of freedom for the K user interference channel. *IEEE Transactions on Information Theory*, 54(8): 3425–3441, August 2008.

[19] T. P. Coleman, M. Effros, E. Martinian, and M. Medard. Rate-splitting for the deterministic broadcast channel. In *Proc. of the IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005.

[20] T. P. Coleman, E. Martinian, M. Effros, and M. Medard. Interference management via capacity-achieving codes for the deterministic broadcast channel. In *Proc. IEEE Information Theory Workshop*, pages 23–27, September 2005.

[21] Thomas Cover and Joy Thomas. *Elements of Information Theory*. Wiley-Interscience, New York, 1991.

[22] Thomas M. Cover. Broadcast channels. *IEEE Transactions on Information Theory*, 18 (1):2–14, January 1972.

[23] Thomas M. Cover. Comments on broadcast channels. *IEEE Transactions on Information Theory*, 44(6):2524–2530, October 1998.

[24] E. Şaşoğlu, E. Telatar, and E. Arıkan. Polarization for arbitrary discrete memoryless channels. *CoRR*, abs/0908.0302, 2009.

[25] A. d'Aspremont, L. El Ghaoui, M. I. Jordan, and G. R. Lanckriet. A direct formulation for sparse pca using semidefinite programming. *SIAM Review*, (49):434–448, 2007.

[26] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. Wainwright, and K. Ramchandran. Network coding for distributed storage systems. *IEEE Transactions on Information Theory*, 56 (9):4539–4551, September 2010.

[27] A. G. Dimakis, Kannan Ramchandran, Yunnan Wu, and Changho Suh. A survey on network codes for distributed storage. *Proceedings of the IEEE*, 99:476–489, March 2011.

[28] David Donoho. Compressed sensing. *IEEE Tran. on Info. Theory*, 52(4):1289–1306, April 2006.

[29] Randall Dougherty, Christopher Freiling, and Kenneth Zeger. Insufficiency of linear coding in network information flow. *IEEE Transactions on Information Theory*, 51(8): 2745–2759, August 2005.

[30] J. Fang and H. Li. Joint dimension assignment and compression for distributed multi-sensor estimation. *IEEE Signal Processing Letters*, 15:174–177, Jan. 2008.

[31] Jun Fang and Hongbin Li. Optimal/near-optimal dimensionality reduction for distributed estimation in homogeneous and certain inhomogeneous scenarios. *IEEE Transactions on Signal Processing*, 58(8):4339–4353, Aug. 2010.

[32] L.R. Ford and D.R. Fulkerson. Maximal flow through a network. *Canadian Journal of Mathematics*, 8:399–404, 1956.

[33] Abbas El Gamal and Young-Han Kim. *Network Information Theory*. Cambridge University Press, New York, 2011.

[34] M. Gastpar. On source-channel communication in networks. In Piyush Gupta, Gerhard Kramer, and Adriaan van Wijngarden, editors, *Advances in Network Information Theory*, DIMACS, pages 217–237. March 2003.

[35] M. Gastpar, P. L. Dragotti, and M. Vetterli. The distributed karhunen-loève transform. In *Proc. IEEE Workshop on Multimedia Signal Processing*, pages 57–60, St. Thomas, Virgin Islands, USA, Dec. 2002.

[36] M. Gastpar, P. L. Dragotti, and M. Vetterli. The distributed karhunen loève transform. *IEEE Tran. Info. Theory*, 52:5177–5196, 2006.

[37] Michael Gastpar. *To Code or Not To Code*. PhD thesis, EPFL, 2002.

[38] Arvind Giridhar and P. R. Kumar. Computing and communicating functions over sensor networks. *IEEE Journal on Selected Areas in Communications*, 23(4):755–764, April 2005.

[39] N. Goela and M. Gastpar. Reduced-dimension linear transform coding of correlated signals in networks. *IEEE Transactions on Signal Processing*, (6):3174–3187.

[40] N. Goela, E. Abbe, and M. Gastpar. Polar codes for the deterministic broadcast channel. In *Proc. International Zurich Seminar on Communications*, pages 51–54, Zurich, Switzerland, February 2012.

[41] N. Goela, C. Suh, and M. Gastpar. Network coding with computation alignment. In *IEEE Information Theory Workshop (ITW)*, pages 507–511, 2012.

[42] N. Goela, E. Abbe, and M. Gastpar. Polar codes for broadcast channels. *CoRR*, abs/1301.6150, 2013.

[43] A.A. Gohari and V. Anantharam. Evaluation of marton's inner bound for the general broadcast channel. *IEEE Transactions on Information Theory*, 58(2):608–619, February 2012. ISSN 0018-9448.

[44] V. Goyal. Theoretical foundations of transform coding. *IEEE Signal Processing Magazine*, 18(5), 2001.

[45] Patrick Healy and Nikola S. Nikolov. How to layer a directed acyclic graph. In *Revised Papers from the 9th International Symposium on Graph Drawing*, Graph Drawing, pages 16–30, 2002.

[46] F. Hekland, P. A. Floor, and T. A. Ramstad. Shannon-kotel'nikov mappings in joint source-channel coding. *IEEE Transactions on Communications*, 57(1):94–105, Jan. 2009.

[47] Tracey Ho, Muriel Medard, Ralf Koetter, David R. Karger, Michelle Effros, Jun Shi, and Ben Leong. A random linear network coding approach to multicast. *IEEE Transactions on Information Theory*, 52(10):4413–4430, October 2006.

[48] Eran Hof, Igal Sason, and Shlomo Shamai. Polar coding for reliable communications over parallel channels. *CoRR*, abs/1005.2770, 2010.

[49] S. Jaggi, P. Sanders, P.A. Chou, M. Effros, S. Egner, K. Jain, and L.M.G.M.M. Tolhuizen. Polynomial time algorithms for multicast network code construction. *IEEE Tran. Info. Theory*, 51:1973–1982, 2005.

[50] S. Jalali and M. Effros. On the separation of lossy source-network coding and channel coding in wireline networks. In *Proc. IEEE International Symposium on Information Theory*, pages 500–504, June 2010.

[51] M. Karzand. Polar codes for degraded relay channels. In *Proc. International Zurich Seminar on Communications*, pages 59–62, Zurich, Switzerland, February 2012.

[52] R. Koetter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, Aug. 2008.

[53] Ralf Koetter and Muriel Medard. An algebraic approach to network coding. *IEEE/ACM Transactions on Networking*, 11:782–795, October 2003.

[54] S. B. Korada and R. L. Urbanke. Polar codes are optimal for lossy source coding. *IEEE Transactions on Information Theory*, 56(4):1751–1768, 2010.

[55] Satish B. Korada. *Polar Codes for Channel and Source Coding*. PhD thesis, EPFL, 2009.

[56] S.B. Korada, E. Şaşoğlu, and R. Urbanke. Polar codes: Characterization of exponent, bounds, and constructions. *IEEE Transactions on Information Theory*, 56(12):6253–6264, December 2010. ISSN 0018-9448.

[57] O.O. Koyluoglu and H. El Gamal. Polar coding for secure transmission and key agreement. *IEEE Transactions on Information Forensics and Security*, 7(5):1472–1483, October 2012. ISSN 1556-6013.

[58] Gerhard Kramer and Serap A. Savari. Edge-cut bounds on network coding rates. *J. Network Syst. Management*, 14(1):49–67, 2006.

[59] S.-Y. R. Li, R. W. Yeung, and N. Cai. Linear network coding. *IEEE Trans. Inform. Theory*, 49(2):371–381, February 2003.

[60] M. A. Maddah-Ali, S. A. Motahari, and Amir K. Khandani. Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis. *IEEE Transactions on Information Theory*, 54(8):3457–3470, August 2008.

[61] H. Mahdavifar and A. Vardy. Achieving the secrecy capacity of wiretap channels using polar codes. *IEEE Transactions on Information Theory*, 57(10):6428–6443, October 2011. ISSN 0018-9448.

[62] K. Marton. The capacity region of deterministic broadcast channels. In *Proc. of the IEEE International Symposium on Information Theory*, Paris-Cachan, 1977.

[63] K. Marton. A coding theorem for the discrete memoryless broadcast channel. *IEEE Transactions on Information Theory*, 25:306–311, May 1979.

[64] R. Mori and T. Tanaka. Channel polarization on q-ary discrete memoryless channels by arbitrary kernels. In *Proc. IEEE International Symposium on Information Theory*, pages 894–898, June 2010.

[65] C. Nair. Capacity regions of two new classes of two-receiver broadcast channels. *IEEE Transactions on Information Theory*, 56(9):4207–4214, September 2010. ISSN 0018-9448. doi: 10.1109/TIT.2010.2054310.

[66] C. Nair and A. El Gamal. An outer bound to the capacity region of the broadcast channel. *IEEE Transactions on Information Theory*, 53:350–355, January 2007.

[67] Bobak Nazer and Michael Gastpar. Computation over multiple-access channels. *IEEE Trans. Inform. Theory*, 53(10):3498–3516, October 2007.

[68] Bobak Nazer and Michael Gastpar. Compute-and-forward: Harnessing interference through structured codes. *IEEE Transactions on Information Theory*, 57:6463–6486, October 2011.

[69] Urs Niesen, Bobak Nazer, and Phil Whiting. Computation alignment: Capacity approximation without noise accumulation. *arXiv:1108.6312*, August 2011.

[70] H. I. Nurdin, R. R. Mazumdar, and A. Bagchi. Reduced-dimension linear transform coding of distributed correlated signals with incomplete observations. *IEEE Transactions on Information Theory*, 55(6):2848–2858, June 2009.

[71] W. Park and A. Barg. Polar codes for q-ary channels, $q = 2^r$. *IEEE Transactions on Information Theory*, 59(2):955–969, February 2013. ISSN 0018-9448.

[72] M. S. Pinsker. Capacity of noiseless broadcast channels. *Probl. Inform. Transm.*, pages 97–102, June 1978.

[73] M. Rabbat, J. Haupt, A. Singh, and R. Nowak. Decentralized compression and predistribution via randomized gossiping. In *IPSN 2006, Nashville, TN*.

[74] B. Rai and B. Dey. On network coding for sum-networks. *IEEE Transactions on Information Theory*, 58:50–63, January 2012.

[75] A. Ramamoorthy. Communicating the sum of sources over a network. *Proceedings of the IEEE International Symposium on Information Theory*, pages 1646–1650, July 2008.

[76] A. Ramamoorthy and M. Langberg. Communicating the sum of sources over a network. *arXiv:1001.5319*, January 2010.

[77] A. Ramamoorthy, K. Jain, P. A. Chou, and M. Effros. Separating distributed source coding from network coding. *IEEE Transactions on Information Theory*, 52(6):2785–2795, June 2006.

[78] T. Ramstad. Shannon mappings for robust communication. *Telektronikk*, 98(1):114–128, 2002.

[79] S. El Rouayheb, A. Sprintson, and C. Georghiades. On the index coding problem and its relation to network coding and matroid theory. *IEEE Transactions on Information Theory*, 56(7):3187–3195, 2010.

[80] O. Roy and M. Vetterli. Dimensionality reduction for distributed estimation in the infinite dimensional regime. *IEEE Tran. Info. Theory*, 54(4):1655–1669, April 2008.

[81] A.G. Sahebi and S.S. Pradhan. Multilevel polarization of polar codes over arbitrary discrete memoryless channels. In *49th Annual Allerton Conference on Communication, Control, and Computing*, pages 1718–1725, September 2011.

[82] E. Şaşoğlu. Polarization and polar codes. *Foundations and Trends in Comm. and Information Theory*, 8(4):259–381, 2012.

[83] I. D. Schizas, G. B. Giannakis, and Z. Q. Luo. Distributed estimation using reduced-dimensionality sensor observations. *IEEE Tran. Signal Processing*, 55(8):4284–4299, August 2007.

[84] Godwin Shen, Sunil K. Narang, and Antonio Ortega. Adaptive distributed transforms for irregularly sampled wireless sensor networks. In *Proc. Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, April 2009.

[85] D. Silva, F. R. Kschischang, and R. Koetter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(2):3951–3967, Sept. 2008.

[86] M. Skoglund, N. Phamdo, and F. Alajaji. Hybrid digital-analog source-channel coding for bandwidth compression/expansion. *IEEE Transactions on Information Theory*, 52 (8):3757–3763, Aug. 2006.

[87] C. Suh, N. Goela, and M. Gastpar. Computation in multicast networks: Function alignment and converse theorems. *CoRR*, abs/1209.3358, 2012.

[88] Ido Tal and Alexander Vardy. How to construct polar codes. *CoRR*, abs/1105.6164, 2011.

[89] M. Turk and A. Pentland. Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, 3(1):71–86, 1991.

[90] Ami Wiesel and Alfred O. Hero III. Decomposable principal component analysis. *IEEE Transactions on Signal Processing*, 57(11):4369–4377, Nov. 2009.

[91] Aaron D. Wyner and Jacob Ziv. The rate-distortion function for source coding with side information at the decoder. *IEEE Transactions on Information Theory*, 22(1):1–10, January 1976.

[92] Jinjun Xiao, Shuguang Cui, Zhi-Quan Luo, and Andrea J. Goldsmith. Linear coherent decentralized estimation. *IEEE Transactions on Signal Processing*, 56(2):757–770, 2008.

[93] W. Yu and M. Aleksic. Coding for the blackwell channel: A survey propagation approach. In *Proc. of the IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005.

[94] K. Zhang. *Best Linear Unbiased Estimation Fusion with Constraints*. PhD thesis, Univ. of New Orleans, New Orleans, LA, 2003.

[95] Y. Zhu, E. Song, J. Zhou, and Z. You. Optimal dimensionality reduction of sensor data in multisensor estimation fusion. *IEEE Transactions on Signal Processing*, 53(5): 1631–1639, May 2005.