UNIVERSITY OF CALIFORNIA, SAN DIEGO

Feedback Communication Systems: Fundamental Limits and Control-Theoretic Approach

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

in

Electrical Engineering (Communication Theory and Systems)

by

Ehsan Ardestanizadeh

Committee in charge:

Professor Young-Han Kim, Chair
Professor Massimo Franceschetti, Co-Chair
Professor Tara Javidi, Co-Chair
Professor Robert Bitmead
Professor Bill Helton
Professor Jack Wolf

2010

Copyright
Ehsan Ardestanizadeh, 2010
All rights reserved.

The dissertation of Ehsan Ardestanizadeh is approved, and it is acceptable in quality and form for publication on microfilm and electronically:

Co-Chair

Chair

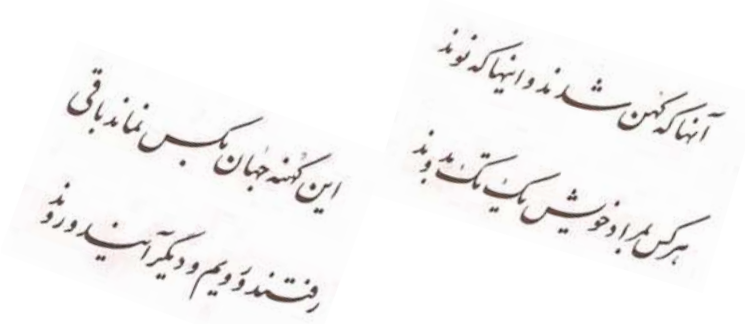
University of California, San Diego

2010

DEDICATION

To my mother and father: Mahdieh and Hossein

EPIGRAPH



In all the eras, old and modern
Everybody runs after his own desires
No one can forever own his possessions
We all have to leave like old ones have left
—Omar Khayam, Persian mathematician and poet, 11th century

TABLE OF CONTENTS

Signature Page iii

Dedication iv

Epigraph v

Table of Contents vi

List of Figures viii

Acknowledgements ix

Vita and Publications xii

Abstract of the Dissertation xiii

Chapter 1 Introduction 1

Chapter 2 Preliminaries 5
- 2.1 Notation 5
- 2.2 Point-to-Point Channels with Feedback 7
  - 2.2.1 Gaussian Channel 8
- 2.3 Estimation and Control 10
  - 2.3.1 Estimation Error Exponent 10
  - 2.3.2 Schalkwijk–Kailath Code 11
  - 2.3.3 Control over the Gaussian Channel 12
- 2.4 Proof of the Lemmas 14
  - 2.4.1 Proof of Lemma 2.3.1 14
  - 2.4.2 Proof of Lemma 2.3.2 17

Chapter 3 Gaussian Multiple Access Channel with Feedback 18
- 3.1 Introduction 19
- 3.2 Problem Setup and the Main Result 21
- 3.3 Proof of the Converse 24
- 3.4 Achievability 35
  - 3.4.1 Code Representation 35
  - 3.4.2 Analysis 37
- 3.5 Discussion 42
- 3.6 Proof of the Lemmas 47
  - 3.6.1 Proof of Lemma 3.3.2 47
  - 3.6.2 Proof of Lemma 3.3.3 48
  - 3.6.3 Proof of Lemma 3.3.6 49

3.6.4 Proof of Lemma 3.3.7 50
3.6.5 Proof of Lemma 3.3.8 54
3.6.6 Proof of Lemma 3.4.5 55
3.6.7 Proof of Lemma 3.5.1 58
3.6.8 Proof of Lemma 3.5.2 60

Chapter 4 Gaussian Broadcast Channel with Feedback 62
4.1 Introduction 63
4.2 Problem Setup 65
4.3 LQG Approach for Gaussian Channel with Feedback . . 67
4.4 LQG Code for Gaussian Broadcast Channel with Feedback 71
4.4.1 Code Design Based on a Control Approach 71
4.4.2 LQG Code Based on the Optimal LQG Control . 74
4.5 Independent Noises: Power Gain 78
4.5.1 Comparison to Gaussian Multiple Access Channel 79
4.5.2 Comparison to Ozarow–Leung Code for $k = 2$ . . 80
4.6 Correlated Noises: Degrees of Freedom Gain 82

Chapter 5 Wiretap Channel with Rate-limited Feedback 88
5.1 Introduction 89
5.2 Problem Setup and the Main Result 93
5.3 Proof of the Upper Bound 99
5.4 A Capacity Achieving Code for Degraded Channels . . . 104

Chapter 6 Binary Multiplying Channel 111
6.1 Introduction 112
6.2 Markov Decision Problem Formulation 112
6.3 Directed Information 117
6.4 Schalkwijk Code 118

Bibliography 122

LIST OF FIGURES

Figure 2.1: Point-to-point communication with feedback 7
Figure 2.2: The Gaussian channel with feedback 9
Figure 2.3: Control over the Gaussian channel 13

Figure 3.1: The k-sender Gaussian multiple access channel 19
Figure 3.2: Plot of $\phi(k, P)$ for $k = 5$ 24
Figure 3.3: $C_1(P, \phi)$ (dashed) and $C_2(P, \phi)$ for $P = 2$ and (a) $k = 2$ (b) $k = 5$ (c) $k = 10$ 42
Figure 3.4: $C_1(P, \phi)$ (dashed) and $C_2(P, \phi)$ for $k = 10$ and (a) $P = 2$ (b) $P = 20$ (c) $P = 200$ 43

Figure 4.1: The k-receiver Gaussian broadcast channel with feedback . . . 65
Figure 4.2: Stabilization over the Gaussian channel 68
Figure 4.3: Control over the Gaussian broadcast channel 72

Figure 5.1: The wiretap channel. 90
Figure 5.2: The wiretap channel with secure rate-limited feedback. 91
Figure 5.3: The physically degraded binary symmetric wiretap channel. . . 96
Figure 5.4: Plot of $C_s(R_f)$ for Example 5.2.1. 96
Figure 5.5: The physically degraded Gaussian wiretap channel. 97
Figure 5.6: An example of a degraded wiretap channel whose secrecy capacity is sublinear in the feedback rate. 98
Figure 5.7: Plot of $C_s(R_f)$ for Example 5.2.3. 99
Figure 5.8: The degraded wiretap channel with shared key. 105
Figure 5.9: Structure of the codebook. 106

Figure 6.1: Binary multiplying channel 113

ACKNOWLEDGEMENTS

I have been truly fortunate in the past few years to have had the guidance and support of Professors Massimo Franceschetti, Tara Javidi, and Young-Han Kim. I am honored and privileged to have had the opportunity to work with them and I cannot thank them enough. They have always treated me as a colleague and as a friend and from each I've learned invaluable lessons which I will carry in all my future endeavors. It is with their efforts that I have been able to develop and present this thesis and for that I am eternally grateful. I would also like to acknowledge my PhD committee members, Professor Robert Bitmead, Professor Bill Helton, and especially Professor Jack Wolf whose wisdom has been a great source of inspiration to me.

It was Young-Han's passion and determination for attacking problems that gave me the energy and motivation throughout the challenges of my PhD program. From him, I have learned to strive for clarity and express general ideas in simple, yet precise statements, which is probably the only way to deeply understand and present new ideas in a comprehensible manner. He constructively challenged the depths of my potential and always pushed me to do my best. I will always be indebted to him for his great mentorship.

It is hard to put into words the extent of my appreciation of Tara and Massimo for their patience and support. In the initial stages of my PhD, they always believed in me and gave me the confidence to explore different paths so that I can reach to my present achievements. Their appeal to inter-disciplinary research allowed me to investigate several areas and obtain a broad research vision. I have utmost respect and gratitude for their guidance.

In addition, I would like to thank Professor Paolo Minero, my former colleague at UCSD, for his collaboration and the time he dedicated to help me in different circumstances. I am also thankful to Professor Michele Wigger whom I had the opportunity to collaborate and become good friends with while she was at UCSD as a Postdoc.

I am also grateful to my former and current colleagues Rathinakumar Appuswamy, Abhijeet Bhorkar, Kaushik Chakraborty, Chiao-Yi Chen, Lorenzo

Coviello, Avinash Jain, Halyun Jeong, Nikhil Karamchandani, Somsak Kittipiyakul, Sung Hoon Lim, Mohammad Naghshvar, Jennifer Price, Anand Sarwate, Ofer Shayevitz, Mohammad Taghavi, Lele Wang, and Yu Xiang for discussing various research problems, giving me constructive feedback on my work, and their warm friendship. Additionally, I would like to acknowledge Vahid Ataie, Reza Hemmati, Iman Novin, Kambiz Samadi, Ahsan Samiee, and Shervin Sharifi my friends at UCSD who helped me in several instances during the past few years.

Finally, I am truly indebted to my family especially my sister Elham, my caring significant other Setareh Setayesh, and my close friend Hamid Ahmadian for their love and support in all these years that were spent towards this thesis.

The following co-authored material has been used in the this dissertation. Chapter 2, in part, includes the material in E. Ardestanizadeh and M. Franceschetti. "Control-theoretic approach to communication with feedback: fundamental limits and code design," arXiv:1006.5265, Jun 2010, submitted for publication in *IEEE Transactions on Automatic Control*. The dissertation author was the primary investigator and author of this paper.

Chapter 3, in part, is a reprint of the material in E. Ardestanizadeh, M. A. Wigger, T. Javidi, and Y.-H. Kim. "Linear sum capacity for Gaussian multiple access channel with feedback," arXiv:1002.1781, Feb 2010, submitted for publication in *IEEE Transactions on Information Theory*. The dissertation author was the primary investigator and author of this paper.

Chapter 4, in part, is a reprint of the material in E. Ardestanizadeh, P. Minero, and M. Franceschetti, "LQG control approach to Gaussian broadcast channels with feedback," 2010, in preparation for submission to *IEEE Transactions on Information Theory*. The dissertation author was the primary investigator and author of this paper.

Chapter 5, in part, is a reprint of the material in E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5353–5361, December 2009. The dissertation author was the primary investigator and author of this paper.

Chapter 6 is based on a research project in collaboration with Professors T. Javidi and Y.-H. Kim. The dissertation author was the primary investigator.

VITA

2004	B. S. in Electrical Engineering, Sharif University of Technology
2007	M. S. in Electrical Engineering and Computer Science, University of California, San Diego
2010	Ph. D. in Electrical and Computer Engineering, University of California, San Diego

PUBLICATIONS

E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *IEEE Transactions on Information Theory*, vol. 55, no. 12, December 2009.

E. Ardestanizadeh, M. A. Wigger, T. Javidi, and Y.-H Kim. "Linear sum capacity for Gaussian multiple access channel with feedback," arXiv:1002.1781, February 2010, submitted for publication in *IEEE Transactions on Information Theory*.

E. Ardestanizadeh and M. Franceschetti. "Control-theoretic approach to communication with feedback: fundamental limits and code design," arXiv:1006.5265, June 2010, submitted for publication in *IEEE Transactions on Automatic Control*.

ABSTRACT OF THE DISSERTATION

Feedback Communication Systems:
Fundamental Limits and Control-Theoretic Approach

by

Ehsan Ardestanizadeh

Doctor of Philosophy in Electrical Engineering (Communication Theory and Systems)

University of California, San Diego, 2010

Professor Young-Han Kim, Chair
Professor Massimo Franceschetti, Co-Chair
Professor Tara Javidi, Co-Chair

Feedback links from the receivers to the transmitters are natural resources in many real-world communication networks which are utilized to send back information about the decoding process as well as the channel dynamics. However, the theoretical understanding of the role of feedback in communication systems is yet far from being complete. In this thesis, we apply techniques from information theory, estimation and control, and optimization theory to investigate the benefits of feedback in improving fundamental limits on information flow in communication networks. We focus on three network models: Gaussian multiple access channels,

Gaussian broadcast channels, and wiretap channels. First, combining the Lagrange duality technique and tools from information theory we derive an upper bound on the sum rate achievable by linear codes for the Gaussian multiple access channel. This upper bound is further shown to coincide with the known lower bound, hence establishing the linear sum capacity. Next, we study the application of the tools from classic linear quadratic Gaussian (LQG) control in designing codes for feedback communications. For the Gaussian broadcast channel, we construct a linear code based on the LQG optimal control, which achieves the best known lower bound on the sum rate. In addition, depending on the spatial correlation of the noise across different receivers, it is shown that in the high signal-to-noise ratio regime, the sum rate achieved by this code can increase linearly with the number of receivers. Third, we consider the wiretap channel with an eavesdropper and study the benefits of a rate-limited feedback link. We propose a new technique based on which we derive an upper bound on the maximum rate of reliable and secure communication. For the special case in which the eavesdropper's signal is a degraded version of the legitimate receiver's signal, this upper bound matches the known lower bound establishing the secrecy capacity. Finally, we present results for the binary multiplying channel, one of the simplest two-way channels for which the capacity region is not known. We apply tools from stochastic control to establish sufficient conditions for optimality, and use the concept of directed information to analyze the performance of coding schemes.

Chapter 1

Introduction

Significant growth of the communication networks has increased the demand for new systems architecture that utilize the available spectrum more efficiently, and interaction between the receivers and the transmitters through feedback links is one way to achieve this goal. However, despite many advancements in information theory, the fundamental limits of such benefit is still not well-understood. In this thesis, we strive to take steps towards the understanding of the role of feedback in improving spectral efficiency.

The study of feedback systems naturally falls at the intersection between communication and control theories. However, the information-theoretic approach and the control-theoretic one have often evolved in isolation, separated by different objectives. Information theory studies how feedback can improve the process of reliable information transmission while the problems considering stabilization of dynamical systems in the presence of feedback is mainly studied in control theory. In this thesis, we attempt one step at bridging the gap, showing how tools from control theory developed to study stabilization problems can be applied to design efficient codes for communication in the presence of feedback. In addition, we also discuss applications of dynamic programing and stochastic control in establishing sufficient conditions for optimality of interactive communication codes.

Feedback plays two pivotal roles in the current communication systems: it provides 1) information about the channel dynamics and 2) information about the decoding process. Having access to the channel state information (CSI), the

transmitters can opportunistically take advantage of the time-varying nature of the channel and transmit at a higher rate whenever the channel is good. This technique, which is implemented at the physical layer, is called *water-filling* and can improve the rate of the communication when the CSI is available at the transmitters. The second role of providing information about the status of the decoding is currently implemented in the upper layers only in a primitive form as acknowledgment (ACK) or automatic repeat request (ARQ).

We assume that the transmitters know the CSI and focus on the second role of feedback addressing the following question: What are the fundamental gains, in terms of throughput, due to the transmitters' knowledge about the receivers' signals in communication networks? Towards this end, a causal noiseless feedback model is assumed throughout. While positive results for this idealistic feedback model will lead to new systems architecture, negative results will prevent over-engineering the feedback and allow us to focus on alternative ways for improving throughput in the networks.

We propose novel approaches and present new results for three network models: 1) Gaussian multiple access channel with feedback, 2) Gaussian broadcast channel with feedback, and 3) wiretap channel with secure rate-limited feedback. The thesis is organized as follows. Chapter 2 presents the notation and the basic definitions for point-to-point (P2P) channels with feedback. We also introduce estimation and control theoretic approaches in this chapter, which will be used later in Chapter 4.

In Chapter 3, we consider the k-sender ($k \geq 2$) Gaussian multiple access channel (MAC) with feedback which models the uplink channel in the communication systems. It is known that the capacity region of the Gaussian MAC, which characterizes the optimal trade-off between communication rates, is enlarged by introducing feedback links as they allow separately located transmitters to cooperate. However, the characterization of the capacity region for $k > 2$ is still an important open problem in network information theory. Our main contribution is an upper bound on the sum capacity achieved by the class of linear feedback codes. This upper bound is derived combining techniques from information the-

ory and convex optimization. Moreover, we show that the upper bound coincides with an existing lower bound and hence we characterize the linear sum capacity. Furthermore, we discuss the application of Hirschfeld–Gebelein–Réyni maximal correlation in deriving upper bounds on the sum rate achieved by general feedback codes.

In Chapter 4, we consider the k-receiver ($k \geq 2$) Gaussian broadcast channel (BC) with feedback which models the downlink channel in communication systems. We construct a code for this channel and characterize the set of achievable rates using the theory of linear quadratic Gaussian control. This code achieves the best known lower bound on the sum capacity of the Gaussian BC with feedback. Next, we study the effect of feedback in increasing the degrees of freedom, which is the ratio between the sum capacity with feedback and without feedback in the high signal-to-noise regime. Interestingly, it is shown that depending on the rank of the covariance matrix of the noise among the receivers, the degrees of freedom can be k. This suggests that the channel can be decomposed into k interference-free parallel channels.

In Chapter 5, we consider the wiretap channel (WC), where a message is required to be transmitted reliably while being secret from an eavesdropper. We consider a secure rate-limited feedback and introduce a new technique to derive an upper bound on the secrecy capacity, the maximum data rate of reliable and secure communication. This upper bound is shown to be tight for the class of physically degraded wiretap channels, where the eavesdropper observes the legitimate receiver's signal through an additional noisy channel independent of the main channel.

Finally, Chapter 6 discusses the binary multiplying channel (BMC), a simple two-way channel introduced by Shannon and Blackwell, for which the capacity region is not known. Two-way channels model the communication scenario between two users, where each user wishes to convey its message to the other one by interactive exchange of information over a channel, and generalize P2P channels with feedback discussed in Chapter 2 by letting each user be both a sender and a receiver. Here, the main question is how each user has to cooperate and at the

same time compete for transmission of its own message. For the BMC, we analyze the performance of a code by Schalkwijk using an alternative approach based on directed information. In addition, based on the classic results from stochastic control, we present a sufficient condition for optimality of the codes over the BMC.

Chapter 2

Preliminaries

2.1 Notation

We closely follow the notation in [1].

Sets, Scalars, and Vectors

We use lower case letters $x, y, \ldots$ to denote constants and values of random variables. We use $x^j = (x_1, x_2, \ldots, x_j)$ to denote a j-sequence/vector. Sometimes we write $\mathbf{x}, \mathbf{y}, \ldots$ for constant (column) vectors with specified dimension and x_j for the j-th component of $\mathbf{x}$. Let $x(i)$ be a vector indexed by time i and $x_j(i)$ be the j-th component of $x(i)$. The sequence of these vectors will be then written as $\mathbf{x}^n = (\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(n))$.

Calligraphic letters $\mathcal{X}, \mathcal{Y}, \ldots$ will be used for finite sets, and $|\mathcal{X}|$ denotes the cardinality of the finite set $\mathcal{X}$. The following notation for common sets will be used: $\mathbb{R}^d$ is the d-dimensional real Euclidean space and $\mathbb{C}^d$ is the d-dimensional complex Euclidean space. Script letters $\mathscr{C}$, $\mathscr{R}$, $\mathscr{P}$, ... will be used for subsets of $\mathbb{R}^d$ or $\mathbb{C}^d$. For a pair of integers $i \leq j$, we define $[i : j] = \{i, i+1, \ldots, j\}$. For a pair of real numbers $b > a$, $[a, b]$ denotes a continuous interval.

Matrices

We use upper case letters $A, B, G, \ldots$ to denote matrices. The entry in the i-th row and j-th column of a matrix A is written as A_{ij}. Similarly, $(A_k)_{ij}$ denotes

the (i, j)-th element of a sequence of matrices indexed by k. The transpose and complex transpose of a matrix A is denoted by A^T and A', respectively.

Random Variables and Vectors

We use upper case letters $X, Y, \ldots$ to denote random variables. The random variables may take values from finite sets $\mathcal{X}, \mathcal{Y}, \ldots$, from the real line $\mathbb{R}$, or from the complex plane $\mathbb{C}$. The probability of the event $\{X \in \mathcal{A}\}$ is denoted by $\mathsf{P}\{X \in \mathcal{A}\}$.

In accordance with the notation for constant vectors, we use the notation $X^j = (X_1, X_2, \ldots, X_j)$ to denote a j-sequence/vector of random variables. The subset of random variables with indices from $\mathcal{J} \subset [1 : n]$ is denoted by $X(\mathcal{J}) = (X_j : j \in \mathcal{J})$. Similarly, given k random vectors $(X_1^n, X_2^n, \ldots, X_k^n)$, $X^n(\mathcal{J}) = (X_j^n : j \in \mathcal{J}) = (X_1(J), X_2(J), \ldots, X_n(J))$. The notation $\{X_i\} := \{X_1, X_2, \ldots\}$ refers to a discrete-time random process.

Sometimes we write $\mathbf{X}, \mathbf{Y}, \ldots$ for random (column) vectors with specified dimensions and X_j for the j-th component of $\mathbf{X}$. Let $\mathbf{X}(i)$ be a random vector indexed by time i and $X_j(i)$ be the j-th component of $\mathbf{X}(i)$. The sequence of these vectors will be then written as $\mathbf{X}^n = (\mathbf{X}(1), \mathbf{X}(2), \ldots, \mathbf{X}(n))$.

Given a random variable X, the expected value of its function $g(X)$ is denoted by $\mathsf{E}_X(g(X))$ or $\mathsf{E}(g(X))$ in short. The conditional expectation of X given Y is denoted by $\mathsf{E}(X|Y)$. We use $\mathrm{Var}(X) = \mathsf{E}[(X - E(X))^2]$ to denote the variance of X and $\mathrm{Var}(X|Y) = \mathsf{E}[(X - E(X|Y))^2|Y]$ to denote the conditional variance of X given Y. For random vectors $\mathbf{X} = X^n$ and $\mathbf{Y} = Y^k$, $K_X = \mathsf{E}(X - \mathsf{E}\,X)(X - \mathsf{E}\,X)'$ denotes the covariance matrix of X, $K_{XY} = \mathsf{E}(X - \mathsf{E}\,X)(Y - \mathsf{E}\,Y)'$ denotes the cross-covariance matrix of (X, Y), and $K_{X|Y} = \mathsf{E}(X - \mathsf{E}(X|Y))(X - \mathsf{E}(X|Y))' = K_{X - \mathsf{E}(X|Y)}$ denotes the covariance matrix of the minimum mean square error (MMSE) for estimating X given Y.

Information Measures

We use $H(X)$ to denote the entropy of a discrete random variable X, and $h(X)$ to denote the differential entropy if X is continuous. The mutual information between two random variables X and Y is denoted by $I(X; Y)$.

2.2 Point-to-Point Channels with Feedback

We review the basic definitions for point-to-point (P2P) communication with feedback, which are immediately extended to multi-user networks discussed in subsequent chapters.

Consider the feedback communication problem depicted in Figure 2.1. We assume a discrete memoryless channel $(\mathcal{X}, p(y|x), \mathcal{Y})$ model that consists of a finite input set $\mathcal{X}$, a finite output set $\mathcal{Y}$, and a collection of conditional pmfs $p(y|x)$ on Y for every $x \in \mathcal{X}$. The sender wishes to reliably communicate a discrete message $M \in \mathcal{M}$ at a rate R bits per transmission to the receiver. Toward this end, the sender encodes the message into a codeword X^n and transmits it over the channel in n time instances (or channel uses). Upon receiving the noisy sequence Y^n, the receiver decodes it to obtain the estimate $\hat{M}$.

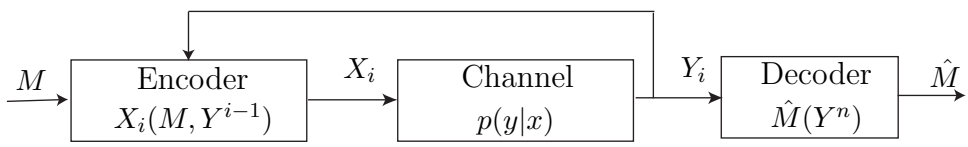


Figure 2.1: Point-to-point communication with feedback

We assume that the output symbols are causally and noiselessly fed back to the sender and the transmitted symbol X_i at each time $i \in [1:n] := \{1, \ldots, n\}$ can depend on both the previous noisy channel output sequence $Y^{i-1} := (Y_1, \ldots, Y_{i-1})$ and the message M.

Definition 2.2.1. *A $(2^{nR}, n)$ code for the DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ consists of*

1. *a discrete message set $\mathcal{M} = [1 : 2^{nR}] := \{1, \ldots, 2^{\lceil nR \rceil}\}$,*
2. *an encoder which assigns a symbol $x_i(m, y^{i-1}) \in \mathcal{X}$ to every message $m \in [1 : 2^{nR}]$ and past received output sequence $y^{i-1} \in \mathcal{Y}^{i-1}$ for $i \in [1 : n]$, and*
3. *a decoder that assigns an estimate $\hat{m} \in [1 : 2^{nR}]$ or an error message e to each received sequence y^n.*

The performance of a given code is measured by the probability that the estimate of the message is different from the actual message sent. The average probability of error for a $(2^{nR}, n)$ code is defined as

$$P_e^{(n)} := \mathsf{P}\{\hat{M} \neq M\} = \sum_{m=1}^{|\mathcal{M}|} \mathsf{P}\{M = m\}\, \mathsf{P}\{\hat{M} \neq m | M = m\}.$$

We assume that the message is uniformly distributed over the message set, i.e., $M \sim \text{Unif}[1 : 2^{nR}]$. A rate R is said to be achievable if there exists a sequence of $(2^{nR}, n)$ codes such that $P_e^{(n)} \to 0$ as $n \to \infty$. The capacity C is the supremum over all achievable rates.

For a DMC without feedback the channel capacity is given by *Shannon's channel coding theorem* [2]:

$$C_{\text{No-FB}} = \max_{p(x)} I(X; Y).$$

Shannon [3] also showed that feedback does not increase the capacity of a DMC.

Theorem 2.2.1. *[2, 3] The capacity of the discrete memoryless channel $(\mathcal{X}, p(y|x), \mathcal{Y})$ with feedback is*

$$C = \max_{p(x)} I(X; Y),$$

which is the same as the capacity without feedback.

Although feedback does not increase the capacity for P2P channels, it can improve the capacity for multi-user networks as we see in subsequent chapters.

2.2.1 Gaussian Channel

Consider the discrete-time additive white Gaussian noise (AWGN) channel (or Gaussian channel in short) model with feedback in Figure 2.2.
At transmission time $i \in [1 : n]$, the channel output $Y_i \in \mathbb{R}$ corresponding to the

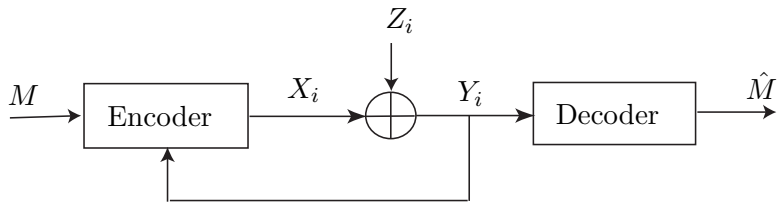


Figure 2.2: The Gaussian channel with feedback

input $X_i \in \mathbb{R}$ is

$$Y_i = X_i + Z_i, \tag{2.1}$$

where $\{Z_i\}$ is a discrete-time zero-mean white Gaussian noise process with unit average power, i.e., $Z_i \sim \mathrm{N}(0,1)$, and independent of the message M. We assume an average transmission power constraint

$$\sum_{i=1}^{n} x_i^2(m, Y^{i-1}) \leq nP \text{ for every } m \in [1 : 2^{nR}].$$

Note that the Gaussian channel has continuous, instead of finite, alphabets. Nonetheless, the achievable rate and capacity under power constraint P can be defined in a similar manner as for the DMC with an additional constraint on the input. Theorem 2.2.1 can then be generalized as follows.

Theorem 2.2.2. *[2, 3] The capacity of the Gaussian channel with feedback under average power constraint P is the same as the capacity without feedback given by*

$$C = \max_{F(x):\mathsf{E}(X^2)\leq P} I(X;Y) = \mathrm{C}(P),$$

where $\mathrm{C}(x) := (1/2)\log(1+x)$ *for* $x \geq 0$.

Remark. We assumed, without loss of generality, that noise has unit power since (2.1) under power constraint P is equivalent to a Gaussian channel with a general noise power σ^2 but under power constraint $P\sigma^2$. Hence, power P in the normalized Gaussian channel (2.1) represents the signal-to-noise ratio (SNR).

2.3 Estimation and Control

2.3.1 Estimation Error Exponent

Consider the feedback communication problem in Figure 2.1, where the sender has a continuous message point (random variable) $\Theta \in \mathbb{R}$, instead of a discrete message, and wishes to communicate it with minimum distortion by n transmissions over a DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ with feedback.

Definition 2.3.1. *An n-code for the DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ consists of*

1. *a continuous message set $(0,1) \subset \mathbb{R}$,*
2. *an encoder which assigns a symbol $x_i(\theta, y^{i-1}) \in \mathcal{X}$ to every message $\theta \in (0,1)$ and past received output sequence $y^{i-1} \in \mathcal{Y}^{i-1}$ for $i \in [1:n]$, and*
3. *a decoder that assigns an estimate $\hat{\theta}(y^n) \in (0,1)$ to each received sequence y^n.*

We assume that the message point is uniformly distributed over the unit interval $\Theta \sim \mathrm{Unif}(0,1)$. The performance of a given code is measured by the mean squared error (MSE) of the message estimate. The average MSE of an n-code is defined as

$$D^{(n)} = \mathsf{E}(\Theta - \hat{\Theta}(Y^n))^2 = \mathsf{E}_\Theta\, \mathsf{E}((\Theta - \hat{\Theta}(Y^n))^2 | \Theta).$$

Note that the estimation problem described above is different from the lossy source coding problem [4] where an identically and independently distributed (i.i.d) random process is to be estimated with minimum *average distortion*. Here, we have only *one* random variable Θ, however, we are allowed to have multiple transmissions over a DMC with feedback to *refine* the estimate of the random variable Θ at the receiver.

An MSE exponent E is said to be achievable if there exists a sequence of n-codes such that

$$E = \lim_{n\to\infty} -\frac{1}{2n} \log D^{(n)}.$$

The definitions of achievable rate and MSE exponent are closely related.

Lemma 2.3.1. *[5] If the MSE exponent E is achievable over a DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$, then any rate $R < E$ is achievable over the same channel. Conversely, if a rate R is achievable with probability of error satisfying $\lim_{n\to\infty} \frac{1}{n} \log P_e^{(n)} \leq -2R$, then the MSE exponent $E = R$ is achievable.*

Proof. For completeness, we provide the proof in Section 2.4.1.

Remark. Lemma 2.3.1 can be readily generalized to Gaussian channels considering the power constraint.

This lemma establishes the connection between the achievable MSE exponent for the estimation problem and the achievable rate for the communication problem described in Section 2.2. Recall that the achievable rate R is defined based on a sequence of *discrete* message sets $[1 : 2^{nR}]$, whereas the achievable MSE exponent E is defined based on a *continuous* message set $(0, 1)$ which does not depend on the block length n. According to Lemma 2.3.1, showing that an MSE exponent E is achievable is sufficient to show that any rate $R < E$ is achievable. We will return to this connection in Chapter 4.

2.3.2 Schalkwijk–Kailath Code

In this section we describe a simple capacity achieving code for the Gaussian channel with feedback known as the Schalkwijk–Kailath (SK) code [6, 7]. The idea behind the SK code is that the transmitter first sends a message at a rate higher than channel capacity, and then iteratively refines the receiver's knowledge about the message. We provide the analysis for the SK code based on the MSE exponent introduced in the previous section. A similar analysis framework will be used for generalizations of the SK code to feedback communication over the Gaussian MAC and BC in Chapter 3 and Chapter 4, respectively.

Let $\Theta \sim \text{Unif}(0, 1)$. At time 1, the encoder transmits

$$X_1 = \gamma \cdot \Theta$$

where constant $\gamma = P/\mathsf{E}(\Theta^2)$ is chosen such that $\mathsf{E}(X_1^2) = P$. For $i \geq 2$, the encoder refines the knowledge of the receiver according to the following linear

recursion:

$$\begin{aligned} X_{i+1} &= a \cdot (X_i - \hat{X}_i(Y_i)) \\ \hat{X}_i(Y_i) &= b \cdot Y_i \end{aligned} \tag{2.2}$$

where $a = \sqrt{1+P}$, $b = P/(1+P)$. It can be verified that $\mathsf{E}(X_i^2) = P$ for all $i \geq 2$ and

$$\hat{X}_i(Y_i) = \frac{P}{1+P} Y_i$$

is the minimum mean squared error (MMSE) linear estimate of X_i given Y_i.

From the recursion (2.2) we have

$$\begin{aligned} X_{i+1} &= a^i \Big(X_1 - b \sum_{j=1}^{i} a^{-j+1} \cdot Y_j \Big) \\ &= \gamma \cdot a^i \cdot (\Theta - \hat{\Theta}_i) \end{aligned}$$

where $\hat{\Theta}_i = b/\gamma \cdot \sum_{j=1}^{i} a^{-j+1} \cdot Y_j$. At time n, if the decoder chooses $\hat{\Theta}_n$ as the estimate of Θ, then the MSE is given by

$$D^{(n)} = \mathsf{E}(\Theta - \hat{\Theta}_n)^2 = \tilde{\gamma} \cdot a^{-2n} = \tilde{\gamma} \cdot 2^{-2n \log a}$$

where $\tilde{\gamma} = P/\gamma = \mathsf{E}(\Theta^2)$. Hence, the MSE exponent

$$E = \log a = \frac{1}{2} \log(1+P)$$

is achievable and by Lemma 2.3.1 any rate $R < C = 1/2 \log(1+P)$ is achievable.

2.3.3 Control over the Gaussian Channel

We juxtapose the feedback communication problem over a Gaussian channel with the control problem depicted in Figure 2.3, where the control signal is received over the same Gaussian channel. Let the state $\mathbf{S}_i$ belong to $\mathscr{S}_i \subset \mathbb{R}^d$ for some $d \geq 1$

and evolve as

$$\mathbf{S}_i = g_i(\mathbf{S}_{i-1}, Y_{i-1}), \quad i = 1, \ldots, n, \tag{2.3}$$

with initial state $S_0 \in \mathbb{R}$ and $Y_0 = 0$. We refer to the mappings $\{g_i\}_{i=1}^n$ as the *system*. The controller, which observes the current state $\mathbf{S}_i$, chooses an action (symbol) $X_i \in \mathbb{R}$,

$$X_i = \pi_i(\mathbf{S}_i), \quad i = 1, \ldots, n. \tag{2.4}$$

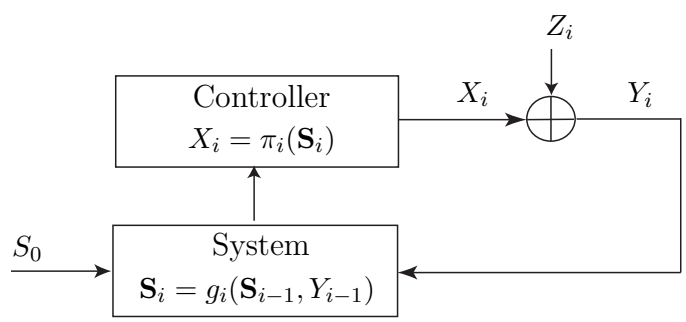


Figure 2.3: Control over the Gaussian channel

We refer to the mappings $\{\pi_i\}_{i=1}^n$ as the *control* (sequence). The communication problem in Figure 2.2 can be related to the control problem in Figure 2.3 as follows.

Let the initial state $S_0 = M$ be the same as the message $M \in [1 : 2^{nR}]$ for the communication problem in Figure 2.2, and the system $\{g_i\}_{i=1}^n$ be such that the state $\mathbf{S}_i$ at time i is the collection of the initial state $S_0 = M$ and the past observations Y^{i-1}, that is,

$$\mathbf{S}_i = (S_0, Y^{i-1}), \quad i = 1, \ldots, n. \tag{2.5}$$

Also, let the control $\{\pi_i\}_{i=1}^n$ be chosen according to the encoder in the communication problem such that

$$\pi_i(\mathbf{S}_i) = X_i(M, Y^{i-1}), \quad i = 1, \ldots, n.$$

Then, the joint distribution of (S_0, X^n, Y^n, Z^n) in the control problem is same as

that of (M, X^n, Y^n, Z^n) in the communication problem. Note that the decoder in the communication problem does not affect this distribution and simply maps the channel output sequence to the message estimate at the end of the communication. Therefore, for a given decoder, the combination of the system $\{g_i\}_{i=1}^n$ and the control $\{\pi_i\}_{i=1}^n$ determines an encoder for the feedback communication.

The system in (2.5) is the most general system which can represent all the encoders for the communication problem. However, if the system $\{g_i\}_{i=1}^n$ is more restricted such that the state $\mathbf{S}_i$ is a filtered version of (S_0, Y^{i-1}), then the set of controllers for that system represents only a subclass of encoders where the transmitted symbol X_i depends on (M, Y^{i-1}) only through $\mathbf{S}_i$ (see (2.4)). We will return to this connection in Chapter 4, where we present and analyze linear codes for feedback communications based on linear system/control.

Below, we show a subclass of encoders for which the state $\mathbf{S}_i$ does not include all the past output Y^{i-1} as in (2.5), yet it contains all the optimal encoders. Let $F_{M|Y^{i-1}}(\cdot|Y^{i-1}) \in \mathbb{R}^{|\mathcal{M}|-1}$ be the conditional distribution of the message $M \in [1 : 2^{nR}]$ given the previous channel outputs Y^{i-1}.

Lemma 2.3.2. *[5] The subclass of encoders which is determined by the system with state of the form*

$$\mathbf{S}_i = (M, F_{M|Y^{i-1}}(\cdot|Y^{i-1}))$$

contains an optimal encoder which minimizes the MSE $D^{(n)}$.

Proof. For completeness, we provide the proof in Section 2.4.2.

2.4 Proof of the Lemmas

2.4.1 Proof of Lemma 2.3.1

We show that a rate $R < E$ is achievable if there exists a sequence of n-codes for $\Theta \in (0, 1)$ such that

$$E = \lim_{n\to\infty} -\frac{1}{2n} \log(D^{(n)}). \tag{2.6}$$

First, consider

$$p_n := \mathsf{P}\left\{|\Theta - \hat{\Theta}| > \frac{1}{2}\cdot 2^{-nR}\right\} \leq 4\cdot 2^{2nR}\cdot D^{(n)} \tag{2.7}$$

$$\leq 4\cdot 2^{2nR}\cdot 2^{-2n(E-\epsilon_n)} \tag{2.8}$$

$$= 4\cdot 2^{-2n(E-R-\epsilon_n)} \tag{2.9}$$

where $\epsilon_n \to 0$ as $n \to \infty$. The inequalities (2.7) and (2.8) follow from the Chebyshev inequality and (2.6), respectively. Since $R < E$, from (2.9) we have

$$p_n \to 0 \text{ as } n \to 0. \tag{2.10}$$

We construct a sequence of $(2^{nR}, n)$ codes based on the given n-code by mapping the discrete message set $\mathcal{M} = [1 : 2^{nR}]$ to a set of message points $\mathcal{M}' = \{\theta_{i,n} \in (0,1)\}_{i=1}^{2^{nR}}$ in the unit interval such that the distance between any two message points is greater than or equal to 2^{-nR}. To send $m \in \mathcal{M}$ we use the given n-code and the corresponding message point $\theta(m)$. The decoder chooses $\hat{m}(y^n)$ such that $\theta(\hat{m})$ is the closest message point to the estimate $\hat{\theta}(y^n)$. The average probability of error is bounded as follows:

$$P_e^{(n)} \leq \max_{\theta_{i,n}\in\mathcal{M}'} \mathsf{P}\{|\Theta - \hat{\Theta}| > \frac{1}{2}\cdot 2^{-nR}\big|\Theta = \theta_{i,n}\} \tag{2.11}$$

Next, by the similar argument as in [8, Lemma II.3] we show that condition (2.10) is sufficient to find a set of message points in the unit interval such that the distance between any two message points is greater than or equal to 2^{-nR} and

$$\lim_{n\to\infty}\max_{\theta\in\mathcal{M}'} \mathsf{P}\left\{|\theta - \hat{\theta}| > \frac{1}{2}\cdot 2^{-nR}\Big|\Theta = \theta\right\} = 0. \tag{2.12}$$

Hence, by (2.11) we have $P_e^{(n)} \to 0$ as $n \to \infty$ and we conclude that rate R is achievable.

To show that we can always find the described $\mathcal{M}'$, define the event

$$T_n = \left\{\theta \in (0,1) : \mathsf{P}\left\{|\Theta - \hat{\Theta}| > \frac{1}{2}\cdot 2^{-nR}\big|\Theta = \theta\right\} > \sqrt{p_n}\right\}$$

Then we have $p_n > \sqrt{p_n}\,\mathsf{P}(T_n)$ and hence

$$\mathsf{P}(T_n) < \sqrt{p_n}.$$

To choose $\mathcal{M}'$ such that $\mathcal{M}' \cap T_n = \emptyset$ and also the distance between any two message points is greater than or equal to 2^{-nR}, it is sufficient that $|\mathcal{M}'|2^{-nR} \leq 1 - \sqrt{p_n}$ or considering (2.10),

$$|\mathcal{M}'| \leq (1 - \epsilon_n) \cdot 2^{nR}$$

where $\epsilon_n \to 0$ as $n \to \infty$. Moreover, by the definition of T_n and the fact that $\mathcal{M}' \cap T_n = \emptyset$ we have

$$\max_{\theta \in \mathcal{M}'} \mathsf{P}\left\{ |\theta - \hat{\theta}| > \frac{1}{2} \cdot 2^{-nR} \middle| \Theta = \theta \right\} \leq \sqrt{p_n} \tag{2.13}$$

and considering (2.10), the condition (2.12) holds. Therefore, we conclude that rate $R < E$ is achievable.

For the converse, let rate R be achievable by a given sequence of n-codes such that $\lim_{n\to\infty} \frac{1}{n} \log P_e^{(n)} \leq -2R$. For each n, we divide the unit interval $(0, 1)$ into 2^{nR} equal-size sub-intervals and map the continuous message point $\theta \in (0, 1)$ to the discrete message $m(\theta) \in \mathcal{M} = \{1 : 2^{nR}\}$ according to the sub-interval θ lies in. To communicate θ, we send the corresponding $m(\theta)$ using the given $(2^{nR}, n)$ code, and we pick the middle point of the interval corresponding to the decoded message $\hat{m}(y^n)$ as the estimate $\hat{\theta}(y^n) \in (0, 1)$ for θ. The MSE for Θ can be upper bounded by 2^{-2nR} if the corresponding discrete message is decoded correctly, and by 1 in case of an error. Hence,

$$D^{(n)} \leq P_e^{(n)} + (1 - P_e^{(n)})2^{-2nR} \tag{2.14}$$

From (2.14) and the assumption $\lim_{n\to\infty} \frac{1}{n} \log P_e^{(n)} \leq -2R$, we have

$$\lim_{n\to\infty} -\frac{1}{2n} \log D^{(n)} = R$$

and hence the MSE exponent $E = R$ is achievable.

2.4.2 Proof of Lemma 2.3.2

Note that without loss of generality we can decompose the encoding mappings $(M, Y^{i-1}) \to X_i$ into two steps as follows. First, based on the past output Y^{i-1}, the encoder picks a function

$$\tilde{f}_i : \mathcal{M} \to X. \tag{2.15}$$

Then it transmits

$$X_i = \tilde{f}_i(M).$$

With this decomposition, one can view the feedback communication as a control problem where the system has the state M, which does not vary over time, and the control action at time i is the function $\tilde{f}_i$, which is chosen based on partial observations Y^{i-1} of the state M. Note that the function $\tilde{f}_i$ depends only on the past outputs Y^{i-1} and not on the message M. The controller can be then defined by the set of mappings

$$\tilde{\pi}_i : \mathcal{Y}^{i-1} \to \{\tilde{f}\}$$

where $\{\tilde{f}\}$ is the set of all functions given in (2.15). Based on standard results in stochastic control [9, Chapter 6], there is no loss of optimality if the mapping $\tilde{\pi}_i$ is chosen only according to the conditional distribution $F_{M|Y^{i-1}}(\cdot|Y^{i-1})$. Therefore, to find $X_i = \tilde{f}_i(M)$ it is sufficient to have the message M and its posterior distribution $F_{M|Y^{i-1}}(\cdot|Y^{i-1})$ which determines the function $\tilde{f}_i(\cdot)$.

Chapter 2, in part, includes the material in [5]. The dissertation author was the primary investigator and author of this paper.

Chapter 3

Gaussian Multiple Access Channel with Feedback

It is known that feedback improves throughput over the multiple access channel by enabling the distributed senders to establish cooperation and coherently align their signals to achieve higher combined power. However, the capacity region of the k-sender additive white Gaussian noise (or Gaussian in short) multiple access channel with feedback is not known in general, despite significant contributions by Cover, Leung, Ozarow, Thomas, Pombra, Ordentlich, Kramer, and Gastpar. This chapter studies the class of *generalized linear feedback codes* that includes (nonlinear) nonfeedback codes at one extreme and the linear feedback codes by Schalkwijk and Kailath, Ozarow, and Kramer at the other extreme. The *linear sum capacity*, the maximum sum rate achieved by generalized linear feedback codes, under symmetric block power constraints P for all the senders is characterized as $C_{\mathsf{L}}(k, P) = 1/2 \log(1 + kP\phi)$. Here, $1 \leq \phi(k, P) \leq k$ captures the improvement due to feedback and for fixed k is increasing in P, that is, more power allows more cooperation.

3.1 Introduction

The sum capacity of the additive white Gaussian noise multiple access channel (AWGN-MAC) with feedback depicted in Figure 3.1 is not known in general. For $k = 2$ senders, Ozarow [10] established the capacity region which—unlike for the point-to-point channel—turns out to be strictly larger than the one without feedback. The capacity achieving code proposed by Ozarow is an extension of the Schalkwijk and Kailath code [6, 7] for point-to-point AWGN channels described in Section 2.3.2.

For $k \geq 3$, the capacity region is not known in general. On one hand, Thomas [11] proved that feedback can at most double the sum capacity, and later Ordentlich [12] showed that the same bound holds for the entire capacity region even when the noise sequence is not white (cf. Pombra and Cover [13]). On the other hand, Kramer [14] extended Ozarow's linear code to $k \geq 3$ users. Kramer's linear code achieves the sum capacity under the symmetric block power constraints P for all the senders, provided that the power P exceeds a certain threshold (3.56) that depends on the number of senders.

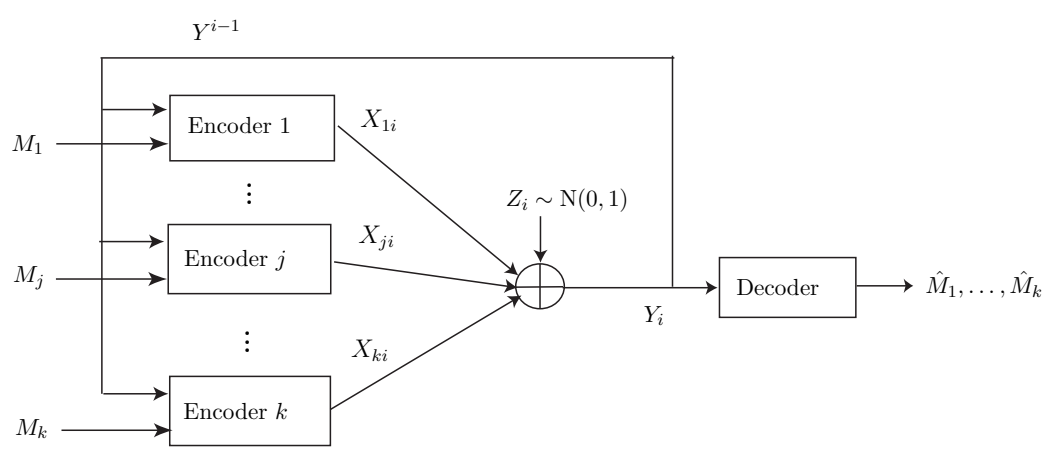


Figure 3.1: The k-sender Gaussian multiple access channel

In this chapter, we focus on the class of *generalized linear feedback codes* (or *linear codes* in short), whereby the feedback signals are incorporated linearly into the transmitted signals (see Definition 3.2.1 in Section 3.2 for the precise

definition). This class of generalized linear feedback codes includes the linear feedback codes by Schalkwijk and Kailath [6], Ozarow [10], and Kramer [14] as well as arbitrary (nonlinear) nonfeedback codes.

We characterize the linear sum capacity $C_{\mathsf{L}}(k, P)$, which is the maximum sum rate achieved by generalized linear feedback codes under symmetric block power constraints P. The main contribution is the proof of the converse. We first prove an upper bound on $C_{\mathsf{L}}(k, P)$, which is a multi-letter optimization problem over Gaussian distributions (cf. Cover and Pombra [15]). Next, we derive an equivalent optimization problem over the set of positive semidefinite (covariance) matrices by considering a dependence balance condition, introduced by Hekstra and Willems [16] and extended by Kramer and Gastpar [17]. Lastly, we carefully analyze this nonconvex optimization problem via Lagrange dual formulation [18].

The linear sum capacity $C_{\mathsf{L}}(k, P)$ can be achieved by Kramer's linear code. Hence, this rather simple code, which iteratively refines receiver's knowledge about the messages, is sum rate optimal among the class of generalized linear feedback codes. For completeness, we provide a representation of Kramer's linear code and analyze it via properties of discrete algebraic Riccati recursions (cf. Wu et al. [19]). This analysis differs from the original approaches by Ozarow [10] and Kramer [14].

The complete characterization of $C(k, P)$, the maximum sum rate among all feedback codes, still remains open. We conjecture that $C(k, P) = C_{\mathsf{L}}(k, P)$ based on the observation that linear codes are *greedy optimal* for a multi-letter optimization problem which upper bounds $C(k, P)$. We establish this fact in Section 3.5 by introducing and analyzing the properties of *conditional maximal correlation*, which is an extension of the Hirschfeld–Gebelein–Renyi maximal correlation [20] to the case where an additional common random variable is shared.

The rest of the chapter is organized as follows. In Section 3.2 we formally define the Gaussian multiple access channel and present our main result. Section 3.3 provides the proof of the converse and Section 5.2.1 gives an alternative proof of achievability via Kramer's linear code. Finally, Section 3.5 provides a discussion on the aforementioned conjecture.

3.2 Problem Setup and the Main Result

Consider the communication problem over an additive white Gaussian noise multiple access channel (AWGN-MAC) with feedback depicted in Figure 3.1. Each sender $j \in \{1, \ldots, k\}$ wishes to transmit a message $M_j \in \mathcal{M}_j$ reliably to the common receiver. At each time $i = 1, \ldots, n$, the output of the channel is

$$Y_i = \sum_{j=1}^{k} X_{ji} + Z_i$$

where $\{Z_i\}$ is a discrete-time zero-mean white Gaussian noise process with unit average power, i.e., $\mathsf{E}(Z_i^2) = 1$, and independent of $M_1, \ldots, M_k$. We assume that the output symbols are causally fed back to each sender and the transmitted symbol X_{ji} from sender j at time i can depend on both the previous channel output sequence $Y^{i-1} := \{Y_1, Y_2, \ldots, Y_{i-1}\}$ and the message M_j.

We define a $(2^{nR_1}, \ldots, 2^{nR_k}, n)$ code with power constraints $P_1, \ldots, P_k$ as

1. k message sets $\mathcal{M}_j := \{1, \ldots, 2^{nR_j}\}$, $j = 1, \ldots, k$,

2. a set of k encoders, where encoder j at each time i maps the pair (m_j, Y^{i-1}) to a symbol X_{ji} such that the sequence $X_{j1}, \ldots X_{jn}$ satisfies the *block power constraint*

$$\sum_{i=1}^{n} \mathsf{E}(X_{ji}^2(m_j, Y^{i-1})) \leq nP_j, \quad m_j \in \mathcal{M}_j,$$

   and

3. a decoder map which assigns message estimates $\hat{m}_j \in \mathcal{M}_j$, $j \in \{1, \ldots, k\}$, to each received sequence y^n.

We assume throughout that $M(\mathcal{S}) := (M_1, \ldots, M_k)$ is a random vector uniformly distributed over $\mathcal{M}_1 \times \cdots \times \mathcal{M}_k$. The probability of error is defined as

$$P_e^{(n)} := \mathsf{P}\{\hat{M}(\mathcal{S}) \neq M(\mathcal{S})\}.$$

A rate-tuple $(R_1, \ldots, R_k)$ is called achievable if there exists a sequence of $(2^{nR_1}, \ldots, 2^{nR_k}, n)$ codes such that $P_e^{(n)} \to 0$ as $n \to \infty$. The capacity region $\mathscr{C}$ is defined as the closure of the set of achievable rate-tuples and the sum capacity C is defined as

$$C := \max \left\{ \sum_{j=1}^{k} R_j : \ (R_1, \ldots, R_k) \in \mathscr{C} \right\}.$$

We refer to $R = \sum_{j=1}^{k} R_j$ as the sum rate of a given code.

Definition 3.2.1. *A $(2^{nR_1}, \ldots, 2^{nR_k}, n)$ code is called a* generalized linear feedback code *if the encoding maps can be decomposed as follows.*

1. *Nonfeedback (nonlinear) mappings: The message M_j is mapped to a vector $\mathbf{\Theta}_j \in \mathbb{R}^d$ for some d, which we refer to as the message point.*

2. *Linear feedback mappings: At each time i, the pair $(\mathbf{\Theta}_j, Y^{i-1})$ is mapped to a symbol X_{ji} such that $X_{ji} = \mathsf{L}_{ji}(\mathbf{\Theta}_j, Y^{i-1})$ is linear in $(\mathbf{\Theta}_j, Y^{i-1})$.*

As mentioned earlier, any nonfeedback code is a generalized linear feedback code by picking $d = n$ and $\mathbf{\Theta}_j \in \mathbb{R}^n$ to be the codeword of the j-th user. On the other hand, by picking $d = 1$ we can get the linear codes by Schalkwijk and Kailath [6] and Ozarow [10]. For Kramer's linear code [14], the message points are 2-dimensional and we need $d = 2$. Note that this subclass of linear codes, for which d is independent of n, does not include the nonfeedback codes (cf. [21]).

The linear capacity region $\mathscr{C}_{\mathsf{L}}$ is defined as the closure of the set of rate-tuples achievable by linear codes and the linear sum capacity C_{L} is defined as

$$C_{\mathsf{L}} := \max \left\{ \sum_{j=1}^{k} R_j : \ (R_1, \ldots, R_k) \in \mathscr{C}_{\mathsf{L}} \right\}.$$

The following theorem characterizes $C_{\mathsf{L}}(k, P)$, the linear sum capacity under symmetric block power constraints P for all the k senders.

Theorem 3.2.1. *For the AWGN-MAC with symmetric block power constraints*

$P_j = P$, we have

$$C_{\mathsf{L}}(k, P) = \frac{1}{2}\log(1 + kP\phi(k, P)) \tag{3.1}$$

where $\phi(k, P) \in \mathbb{R}$ is the unique solution in the interval $[1, k]$ to

$$(1 + kP\phi)^{k-1} = (1 + P\phi(k - \phi))^k . \tag{3.2}$$

Proof. The proof of the converse is provided in Section 3.3. It is known [14] that Kramer's linear code achieves the sum rate (3.1). For completeness, a simple analysis for Kramer's code is presented in Section 5.2.1.

Note that $\phi(k, P) \in [1, k]$ captures the ultimate amount of cooperation which can be established among the senders, such that $\phi = 1$ corresponds to no cooperation and $\phi = k$ corresponds to full cooperation. For a fixed k, $\phi(k, P)$ is increasing (more power allows more cooperation) and concave in P as depicted in Figure 3.2.

Corollary 3.2.2. *Consider the case of low signal-to-noise ratio (SNR). From (3.2) we can see that as $P \to 0$, $\phi(k, P) \to 1$ irrespective of the number of senders k, and thus*

$$C_{\mathsf{L}}(k, P) - \frac{1}{2}\log(1 + kP) \to 0$$

which means that the linear sum capacity approaches the sum capacity without feedback. Hence, in the low SNR regime almost no cooperation is possible.

Corollary 3.2.3. *Consider the case of high SNR. Again from (3.2) we can see that as $P \to \infty$, $\phi(k, P) \to k$ and*

$$C_{\mathsf{L}}(k, P) - \frac{1}{2}\log(1 + k^2P) \to 0.$$

Thus, the linear sum capacity approaches the sum capacity with full cooperation where all the transmitted signals are coherently aligned with combined SNR equal to k^2P.

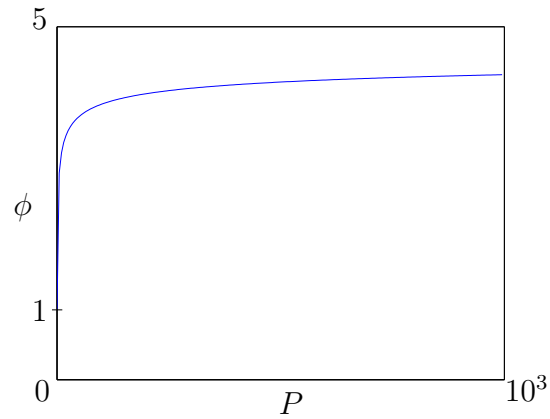


Figure 3.2: Plot of $\phi(k, P)$ for $k = 5$

3.3 Proof of the Converse

In this section we show that under the symmetric block power constraints P for all senders, the linear sum capacity $C_{\mathsf{L}}(k, P)$ is upper bounded as

$$C_{\mathsf{L}}(k, P) \leq \frac{1}{2} \log(1 + kP\phi(k, P)) \tag{3.3}$$

where $\phi(k, P) \in \mathbb{R}$ is the unique solution in the interval $[1, k]$ to

$$(1 + kP\phi)^{k-1} = (1 + P\phi(k - \phi))^k .$$

The proof can be summarized in four steps. First, we derive an upper bound on the linear sum capacity based on Fano's inequality, and we prove that in the resulting multi-letter optimization problem we can limit ourselves to Gaussian distributions (see Lemma 3.3.1). Second, we use a dependence balance condition [16, 17] and the Gaussianity of the involved random variables to derive an equivalent optimization problem (see (3.11)) over positive semidefinite matrices. This optimization problem is nonconvex due to the introduced dependence balance condition. Third, we upper bound the solution to this optimization problem using the Lagrange dual formulation and the symmetry of the involved functions. The so obtained upper bound depends on the choice of the Lagrange multipliers, and for each choice it is again a nonconvex optimization problem but involving only two

optimization variables (see Lemma 3.3.4). Finally, using a few technical tricks and strong duality, we show that there exists a set of Lagrange multipliers for which this upper becomes equal to the right hand side of (3.3) (see Lemma 3.3.5).

Details are as follows.

Step 1: We provide an upper bound on the linear sum capacity based on Fano's inequality. Then we use linearity of the code and a conditional version of the maximum entropy theorem [11, Lemma 1] to show that it is sufficient to consider only Gaussian distributions.

Lemma 3.3.1. *The linear sum capacity $C_{\mathsf{L}}(k, P)$, under symmetric block power constraints P for all k senders, is bounded as*

$$C_{\mathsf{L}}(k, P) \leq \lim_{n\to\infty} C_n(P)$$

where

$$C_n(P) := \max \frac{1}{n} \sum_{i=1}^{n} I(X_{1i}, \ldots, X_{ki}; Y_i | Y^{i-1}). \tag{3.4}$$

Here the maximization is over all inputs X_{ji} of the form

$$\begin{aligned} X_{ji} &= \mathsf{L}_{ji}(\mathbf{V}_j, Y^{i-1}),\ i = 1, \ldots, n \\ \sum_{i=1}^{n} \mathsf{E}(X_{ji}^2) &\leq nP,\ j = 1, \ldots, k \end{aligned} \tag{3.5}$$

where each $\mathbf{V}_j \in \mathbb{R}^n \sim \mathrm{N}(0, K_{\mathbf{V}_j})$ is Gaussian and independent of Z^n and $\{\mathbf{V}_{j'} : j' \neq j\}$.

Remark. Although the functions that will be defined in the rest of the chapter depend on the number of senders k, for simplicity of the notation, we avoid including k explicitly, e.g., $C_n(P)$.

Proof. For any achievable rate-tuple $(R_1, \ldots, R_k)$, the sum rate R can be upper

bounded as follows.

$$
\begin{aligned}
nR = n\sum_{k=1}^{k} R_j &= H(M(\mathcal{S})) \\
&\leq I(M(\mathcal{S}); Y^n) + n\epsilon_n \qquad (3.6)\\
&\leq I(\Theta(\mathcal{S}); Y^n) + n\epsilon_n \qquad (3.7)\\
&\leq \sum_{i=1}^{n} I(X_i(\mathcal{S}); Y_i|Y^{i-1}) + n\epsilon_n \qquad (3.8)
\end{aligned}
$$

where $\{\epsilon_n\}$ denotes a sequence such that $\epsilon_n \to 0$ as $n \to \infty$. Inequality (3.6) follows from Fano's inequality [22],

$$H(M(\mathcal{S})|Y^n) \leq 1 + nP_e^{(n)} \sum_{k=1}^{k} R_j =: n\epsilon_n,$$

and the fact that $P_e^{(n)} \to 0$ as $n \to \infty$. Inequalities (3.7) and (3.8) follow from the data processing inequality and the memoryless property of the channel.

From (3.8), we upper bound the linear sum capacity as

$$C_{\mathsf{L}}(k, P) \leq \lim_{n\to\infty} \max \frac{1}{n} \sum_{i=1}^{n} I(X_i(\mathcal{S}); Y_i|Y^{i-1}) \qquad (3.9)$$

where the maximization is over all linear codes which satisfy the the symmetric power constraints P, i.e.,

$$
\begin{aligned}
&X_{ji} = \mathsf{L}_{ji}(\mathbf{\Theta}_j, Y^{i-1}),\ i = 1, \ldots, n \\
&\sum_{i=1}^{n} \mathsf{E}(X_{ji}^2) \leq nP,\ j = 1, \ldots, k.
\end{aligned}
$$

We next prove that message points $\mathbf{\Theta}_1, \ldots, \mathbf{\Theta}_k$ can be replaced by Gaussian random variables $\mathbf{V}_1, \ldots, \mathbf{V}_k$ with the same covariance matrix. Given a linear code with message points $\mathbf{\Theta}(\mathcal{S})$, let

$$\mathbf{V}(\mathcal{S}) \sim \mathrm{N}(0, K_{\mathbf{\Theta}(\mathcal{S})}).$$

We use $\mathbf{V}(\mathcal{S})$ with the same linear functions as in the given code to generate

$$\tilde{X}_{ji} = \mathsf{L}_{ji}(\mathbf{V}_j, \tilde{Y}^{i-1})$$

where $\tilde{Y}_i$ is the output of the AWGN-MAC corresponding to $\tilde{X}_i(\mathcal{S})$. It is not hard to see that

$$(\tilde{X}_i(\mathcal{S}), \tilde{Y}^i) \sim \mathrm{N}(0, K_{X_i(\mathcal{S}),Y^i}).$$

Therefore, by the conditional maximum entropy theorem [11, Lemma 1] we have

$$I(X_i(\mathcal{S}); Y_i|Y^{i-1}) \leq I(\tilde{X}_i(\mathcal{S}); \tilde{Y}_i|\tilde{Y}^{i-1}). \tag{3.10}$$

Combining (3.9) and (3.10) completes the proof. □

Step 2: We show that the optimization problem defining $C_n(P)$ in (3.4) is equivalent to the following optimization problem

$$\begin{aligned} \text{maximize} \quad & \tfrac{1}{n}\textstyle\sum_{i=1}^n f_1(K_i) \\ \text{subject to} \quad & K_i \succeq 0, \quad i = 1, \ldots, n \\ & \textstyle\sum_{i=1}^n (K_i)_{jj} \leq nP, \quad j = 1, \ldots, k \\ & \textstyle\sum_{i=1}^n f_1(K_i) - f_2(K_i) \leq 0 \end{aligned} \tag{3.11}$$

where

$$f_1(K_i) := \frac{1}{2} \log \Big(1 + \sum_{j,j'} (K_i)_{jj'}\Big) \tag{3.12}$$

and

$$f_2(K_i) := \frac{1}{2(k-1)} \sum_{j=1}^{k} \log \Bigg[1 + \sum_{j',j''} (K_i)_{j'j''} - \frac{\Big(\sum_{j'} (K_i)_{jj'}\Big)^2}{(K_i)_{jj}}\Bigg]. \tag{3.13}$$

Before proving the equivalence we state two useful lemmas.

Lemma 3.3.2. *The functions $f_1(K)$ and $f_2(K)$ in (3.12) and (3.13) are concave in K.*

Proof. See Section 3.6.1.

From [16, 17] we know the following dependence balance condition.

Lemma 3.3.3 ([17], Theorem 1)**.** *Let X_{ji} for $i = 1, \ldots, n$, and $j = 1, \ldots, k$, be defined by the (causal) functional relationship in (3.5). Then,*

$$\sum_{i=1}^{n} I(X_i(\mathcal{S}); Y_i | Y^{i-1}) \leq \frac{1}{k-1} \sum_{i=1}^{n} \sum_{j=1}^{k} I(X_i(\mathcal{S} \backslash \{j\}); Y_i | Y^{i-1}, X_{ji}). \tag{3.14}$$

Proof. For completeness, we provide the proof in Section 3.6.2.

Remark. The proof of Lemma 3.3.3 relies only on the independence of $\mathbf{V}_j \in \mathbb{R}^n$ from Z^n and $\{\mathbf{V}_{j'} : j' \neq j\}$. Thus, Lemma 3.3.3 remains valid also in the more general case where the inputs $X_{ji} = f_{ji}(\mathbf{V}_j, Y^{i-1})$ are obtained using arbitrary functions $\{f_{ji}\}$ and non-Gaussian $\mathbf{V}(\mathcal{S})$.

We now prove the equivalence of the optimization problems (3.4) and (3.11). Since random vectors $\{\mathbf{V}_j\}$ in (3.5) are jointly Gaussian and the functions $\{\mathsf{L}_{ji}\}$ are linear, the random variables $(X^n(\mathcal{S}), Y^n)$ generated according to (3.5) are also jointly Gaussian and we can replace the mutual information terms in condition (3.14) with functions of the covariance matrices. Specifically, let $\mathbf{X}_i = (X_{1i}, \ldots, X_{ki})^T \sim \mathrm{N}(0, K_i)$ where

$$K_i := K_{\mathbf{X}_i} \succeq 0. \tag{3.15}$$

Then

$$I(X_{1i}, \ldots, X_{ki}; Y_i | Y^{i-1}) = f_1(K_i)$$
$$\frac{1}{k-1} \sum_{j=1}^{k} I(X_i(\mathcal{S} \backslash \{j\}); Y_i | Y^{i-1}, X_{ji}) = f_2(K_i).$$

Hence, the condition (3.14) reduces to

$$\sum_{i=1}^{n} f_1(K_i) - f_2(K_i) \leq 0. \tag{3.16}$$

Recall that the condition (3.16) follows from the functional relationship (3.5). Hence, adding the condition (3.16) to the optimization problem (3.4), as an additional constraint, does not decrease the maximum. Finally, note that given the functional relationship in (3.5), the objective function and the power constraints can also be represented only in terms of the covariance matrices $\{K_i\}_{i=1}^n$. Therefore, the functional relationship translates to the constraints that $K_i \succeq 0$ be positive semidefinite for all i, and the equivalence between the optimization problems (3.4) and (3.11) follows.

Notice that even though both functions $f_1(K)$ and $f_2(K)$ are concave (see Lemma 3.3.2), their difference $f_1(K) - f_2(K)$ is neither concave nor convex. Hence, the optimization problem (3.11) is nonconvex [18] due to the constraint (3.16).

Step 3: Using Lagrange multipliers $\lambda, \gamma \geq 0$, we provide a general upper bound $U(\lambda, \gamma)$ for the solution of the optimization problem given in (3.11). We further simplify this upper bound exploiting symmetry.

For the optimization problem (3.11), consider the Lagrange dual function [18]

$$L(\lambda, \gamma) = \max_{K_i \succeq 0} \frac{1}{n} \sum_{i=1}^{n} \Bigg[f_1(K_i) + \gamma(f_2(K_i) - f_1(K_i)) + \lambda \Big(\sum_{j=1}^{k} P - (K_i)_{jj} \Big) \Bigg] \tag{3.17}$$

with equal Lagrange multipliers $\lambda_j = \lambda \geq 0,\ j \in \{1, \ldots, k\}$ for the power constraints $\frac{1}{n}\sum_{i=1}^{n} P - (K_i)_{jj} \geq 0, \quad j \in \{1, \ldots, k\}$, and the Lagrange multiplier $\gamma \geq 0$ for the constraint $\frac{1}{n}\sum_{i=1}^{n} f_2(K_i) - f_1(K_i) \geq 0$.

It is easy to see that for any Lagrange multipliers $\lambda, \gamma > 0$, the solution to the optimization problem (3.11) is upper bounded by the Lagrange dual function $L(\lambda, \gamma)$, see [18]. Moreover, the right hand side of (3.17) is an average of some function of K_i, and can further be upper bounded by the maximum

$$U(\lambda, \gamma) := \max_{K \succeq 0} (1-\gamma) f_1(K) + \gamma f_2(K) + \lambda \sum_{j=1}^{k} (P - K_{jj}). \tag{3.18}$$

Thus, for any $\lambda, \gamma > 0$, the term $U(\lambda, \gamma)$ upper bounds the solution of the optimization problem (3.11).

Next, we simplify the upper bound $U(\lambda, \gamma)$ exploiting the properties of the functions $f_1(K)$ and $f_2(K)$.

Lemma 3.3.4. *Let $\lambda, \gamma \geq 0$. Then, the upper bound $U(\lambda, \gamma)$ can be simplified as follows.*

$$U(\lambda, \gamma) = \max_{x \geq 0} \max_{0 \leq \phi \leq k} g(\gamma, x, \phi) + \lambda k (P - x). \tag{3.19}$$

where

$$g(\gamma, x, \phi) := (1-\gamma) C_1(x, \phi) + \gamma C_2(x, \phi). \tag{3.20}$$

and

$$\begin{aligned} C_1(x, \phi) &:= \frac{1}{2} \log(1 + kx\phi) \\ C_2(x, \phi) &:= \frac{k}{2(k-1)} \log(1 + (k-\phi)x\phi). \end{aligned} \tag{3.21}$$

Proof. First, we show that there exists a matrix K of the following form

$$K = x \cdot \begin{pmatrix} 1 & \rho & \rho & \dots & \rho \\ \rho & 1 & \rho & \dots & \rho \\ \rho & \rho & 1 & \dots & \rho \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \rho & \rho & \rho & \dots & 1 \end{pmatrix} \tag{3.22}$$

which achieves the maximum in (3.18). Towards this end, we shall consider a covariance matrix K' (not necessarily of the from in (3.22)) that achieves the maximum in (3.18), and construct a matrix $\bar{K}$ as in (3.22) with objective function at least as large as the original matrix K':

$$\begin{aligned} &(1-\gamma) f_1(\bar{K}) + \gamma f_2(\bar{K}) + \lambda \sum_{j=1}^{k} (P - \bar{K}_{jj}) \\ &\geq (1-\gamma) f_1(K') + \gamma f_2(K') + \lambda \sum_{j=1}^{k} (P - K'_{jj}). \end{aligned} \tag{3.23}$$

Fix a covariance matrix K' that achieves the maximum in (3.18) and let $\bar{K}$ be the arithmetic average over all $k!$ matrices that can be obtained from the original matrix K' through simultaneous permutation of its rows and columns. That means:

$$\bar{K} := \frac{1}{k!} \sum_{\ell=1}^{k!} \pi_\ell(K'),$$

where $\pi_1, \dots, \pi_{k!}$ denote all $k!$ possible permutations on the set of indices $\{1, \dots, k\}$ and where $\pi(K')$ denotes the matrix that is obtained by permuting the rows and the columns of K' according to the permutation π.

It is easily seen that the so obtained matrix $\bar{K}$ has the desired form (3.22) and it remains to prove the inequality (3.23). To this end, we first notice that since the function $f_1(K)$ depends on the matrix K only via the sum of its entries:

$$f_1(\bar{K}) = f_1(K'), \tag{3.24}$$

and similarly,

$$\lambda \sum_{j=1}^{k} K'_{jj} = \lambda \sum_{j=1}^{k} \bar{K}_{jj}. \tag{3.25}$$

Also, by symmetry it follows that for each permutation π_ℓ, for $\ell = 1, \ldots, k!$:

$$f_2(\pi_\ell(K')) = f_2(K'). \tag{3.26}$$

Therefore, by concavity of $f_2(K)$ in K (see Lemma 3.3.2) and Jensen's inequality we can conclude that

$$f_2(\bar{K}) \geq f_2(K'). \tag{3.27}$$

Combining (3.24), (3.25), and (3.27) yields the desired inequality (3.23).

Thus, we continue our analysis with matrices of the form in (3.22) and by defining

$$\phi = 1 + (k-1)\rho$$

we have

$$\begin{aligned} f_1(K) &= C_1(x, \phi) \\ f_2(K) &= C_2(x, \phi). \end{aligned} \tag{3.28}$$

Since K is positive semidefinite, $x \geq 0$ and $-1/(k-1) \leq \rho \leq 1$, where the lower bound on ρ comes from the fact that $\sum_{i,j=1}^{k} K_{ij}$ is nonnegative for $K \succeq 0$. Hence, $0 \leq \phi \leq k$ and (3.18) reduces to (3.19). □

The form of K in (3.22) was also considered in [11, 14]. However, in those cases the objective function was concave. In our case if $\gamma > 1$ the objective function is not necessarily concave and proving this claim needs further treatment based on the symmetry of the functions (see (3.24)–(3.26)).

Step 4: We complete the proof of the converse by showing that there exists Lagrange multipliers (λ^*, γ^*) such that $U(\lambda^*, \gamma^*)$ becomes equal to (3.3).

Lemma 3.3.5. *There exists $\lambda^*, \gamma^* \geq 0$ such that*

$$\begin{aligned} U(\lambda^*, \gamma^*) &= C_1(P, \phi(k, P)) \\ &= \frac{1}{2}\log(1 + kP\phi(k, P)) \end{aligned}$$

where $\phi(k, P) \in \mathbb{R}$ is the unique solution in the interval $[1, k]$ to

$$(1 + kP\phi)^{k-1} = (1 + P\phi(k - \phi))^k .$$

Proof. Consider the optimization problem over (x, ϕ) which defines $U(\lambda, \gamma)$ in (3.19). Note that $g(\gamma, x, \phi)$ given by (3.20) is neither concave or convex in (x, ϕ) for $\gamma > 1$. Let

$$U(\gamma) := U(\lambda^*(\gamma), \gamma) = \min_{\lambda \geq 0} U(\lambda, \gamma). \tag{3.29}$$

where $\lambda^*(\gamma)$ is the minimizer corresponding to γ. We use the following lemma to find $U(\gamma)$.

Lemma 3.3.6. *The function $g(\gamma, x, \phi)$ is concave in ϕ for fixed $x, \gamma \geq 0$.*

Proof. See Section 3.6.3.

By concavity of $g(\gamma, x, \phi)$ in ϕ for fixed γ and x, the inner maximum in (3.19) happens at $0 < \phi^*(\gamma, x) < k$ such that

$$\begin{aligned} & \frac{\partial g(\gamma, x, \phi)}{\partial \phi} = 0 \\ \Leftrightarrow \quad & \frac{(1-\gamma)(k-1)}{1 + \ kx\phi^*} = \frac{\gamma(2\phi^* - k)}{1 + x\phi^*(k - \phi^*)} \end{aligned} \tag{3.30}$$

or at the boundaries $\phi^*(\gamma, x) \in \{0, k\}$. Therefore,

$$\begin{aligned} U(\gamma) &= \min_{\lambda \geq 0} \max_{x \geq 0} \max_{0 \leq \phi \leq k} g(\gamma, x, \phi) + \lambda k(P - x) \\ &= \min_{\lambda \geq 0} \max_{x \geq 0} g(\gamma, x, \phi^*(\gamma, x)) + \lambda k(P - x). \end{aligned} \tag{3.31}$$

for any $\gamma \geq 0$. To evaluate the last expression we use the following lemma.

Lemma 3.3.7. *Let $\gamma, x \geq 0$ and $\phi^*(\gamma, x) > 0$ be the positive solution to (3.30). Then, $g(\gamma, x, \phi^*(\gamma, x))$ is increasing and concave in x.*

Proof. See Section 3.6.4.

Remark. As pointed out earlier, for $\gamma > 1$, $g(\gamma, x, \phi)$ is not concave in both x, ϕ in general. However, this lemma shows that $g(\gamma, x, \phi^*(\gamma, x))$ is concave in x for all $\gamma \geq 0$ and this is sufficient for the rest of the proof.

By concavity of $g(\gamma, x, \phi^*(\gamma, x))$ and Slater's condition [18] we have strong duality as follows.

$$\begin{aligned}
&\min_{\lambda \geq 0} \max_{x} g(\gamma, x, \phi^*(\gamma, x)) + \lambda k(P - x) \\
&\quad = \max_{x \leq P} g(\gamma, x, \phi^*(\gamma, x)) \\
&\quad = g(\gamma, P, \phi^*(\gamma, P)) \qquad (3.32)
\end{aligned}$$

where the last equality follows from the fact that $g(\gamma, x, \phi^*(\gamma, x))$ is increasing in x (see Lemma 3.3.7). Combining (3.31) and (3.32) we have

$$U(\gamma) = g(\gamma, P, \phi^*(\gamma, P)). \qquad (3.33)$$

Lastly, we find $\gamma^* \geq 0$ such that $U(\gamma^*) = C_1(P, \phi(k, P))$.

Lemma 3.3.8. *For a fixed $x \geq 0$, the equation $C_2(x, \phi) - C_1(x, \phi) = 0$ has a unique solution $1 \leq \phi(k, x) \leq k$. Moreover,*

$$1 + \frac{(2\phi(k, x) - k)(1 + kx\phi(k, x))}{(k - 1)(1 + x\phi(k, x)(k - \phi(k, x)))} > 0. \qquad (3.34)$$

Proof. See Section 3.6.5.

Let $\phi(k, P) \in [1, k]$ be the unique solution to $C_1(P, \phi) = C_2(P, \phi)$, which is equivalent to the equation (3.2). Given k and P, we pick $\gamma^*(P, \phi(k, P))$ such that it satisfies (3.30) for $x = P$ and $\phi^* = \phi(k, P)$. It is easy to check that $\gamma^* := \gamma^*(P, \phi(k, P)) > 0$ is greater than zero by plugging $x = P$ in (3.34). Since

we picked γ^* such that γ^*, P and $\phi(k, P)$ satisfy (3.30) we conclude that $\phi^*(\gamma^*, P)$, the positive solution of (3.30), is equal to $\phi(k, P)$. Plugging $\gamma^* > 0$ and $\phi^*(\gamma^*, P)$ into (3.33) we have

$$\begin{aligned}
&U(\gamma^*) \\
&\quad = g(\gamma^*, P, \phi^*(\gamma^*, P)) \\
&\quad = (1-\gamma^*)C_1(P, \phi^*(\gamma^*, P)) + \gamma^* C_2(P, \phi^*(\gamma^*, P)) \\
&\quad = (1-\gamma^*)C_1(P, \phi(k, P)) + \gamma^* C_2(P, \phi(k, P)) && (3.35) \\
&\quad = C_1(P, \phi(k, P)) && (3.36)
\end{aligned}$$

where (3.35) and (3.36) follow from $\phi^*(\gamma^*, P) = \phi(k, P)$ and $C_1(P, \phi) = C_2(P, \phi)$, respectively. Hence, by picking $\lambda^* = \lambda^*(\gamma^*)$ (see (3.29)), we have $U(\lambda^*, \gamma^*) = C_1(P, \phi(k, P))$. □

Combining the previous four steps we have $C_{\mathsf{L}}(k, P) \leq C_1(P, \phi(k, P))$, and the proof of the converse is complete.

3.4 Achievability

In this section we present an equivalent representation for the Kramer linear code [14] and analyze it based on the properties of discrete algebraic Riccati equations (DARE).

3.4.1 Code Representation

Recall that a linear code has a nonfeedback mapping

$$\mathcal{M}_j \to \Theta_j \in \mathbb{R}^k, \quad j = 1, \ldots, k.$$

We pick $k = 2$ such that $\Theta_j \in \mathbb{C} = \mathbb{R}^2$. With slight abuse of notation we represent $\Theta_j \in \mathbb{C}$ as a scalar and reserve the vector notation for $\mathbf{\Theta} := (\Theta_1, \ldots, \Theta_k)^T$. We also assume that the transmitted signals $X_{ji} \in \mathbb{C}$ are complex (each sent over two

transmissions). We present the following linear code.

Message sets: Let $M_j = (M_{j1}, M_{j2})$ be a two dimensional message, where

$$(M_{j1}, M_{j2}) \sim \text{Unif}\left(\{1, \ldots, 2^{nR_j}\} \times \{1, \ldots, 2^{nR_j}\}\right).$$

Nonfeedback mapping: Divide the square with corners at $(\pm 1 \pm i)$ on the complex plane ($i^2 = -1$) into 2^{2nR_j} equal sub-squares and map $m_j = (m_{j1}, m_{j2})$ to the center of the corresponding sub-square. The distance between neighboring points is

$$\Delta = 2 \cdot 2^{-nR_j} \tag{3.37}$$

in each direction.

Linear feedback mapping: Let the transmissions by all the senders at time i be denoted by the vector $\mathbf{X}_i := (X_{1i}, X_{2i}, \ldots, X_{ki})^T$. Then, the linear feedback mapping is

$$\begin{aligned} \mathbf{X}_0 &= \mathbf{\Theta}, \\ \mathbf{X}_i &= A \cdot (\mathbf{X}_{i-1} - \hat{\mathbf{X}}_{i-1}(Y_{i-1})), \qquad i > 1 \end{aligned} \tag{3.38}$$

where

$$A = \begin{pmatrix} \beta_1\omega_1 & 0 & 0 & \ldots & 0 \\ 0 & \beta_2\omega_2 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \beta_k\omega_k \end{pmatrix}, \tag{3.39}$$

in which $\omega_1, \ldots, \omega_k$ are distinct points on the unit circle and $\beta_1, \ldots, \beta_k > 1$ are real coefficients, and

$$\hat{\mathbf{X}}_{i-1}(Y_{i-1}) = \frac{\mathsf{E}(\mathbf{X}_{i-1}Y'_{i-1})}{\mathsf{E}(|Y_{i-1}|^2)} \cdot Y_{i-1}$$

is the linear minimum mean square error (MMSE) estimate of $\mathbf{X}_{i-1}$ given Y_{i-1}. Note that the linear feedback mapping (3.38) is stationary and recursive.

Decoding: At time n, the decoder forms an estimate

$$\hat{\mathbf{\Theta}}_n = \sum_{i=0}^{n-1} A^{-i}\hat{\mathbf{X}}_i \tag{3.40}$$

and decodes Θ_j to the nearest point of $\hat{\mathbf{\Theta}}(j)$.

Theorem 3.4.1. *Under the symmetric block power constraints $P_j = P$, the linear code described above achieves any sum rate $R < C_{\mathsf{L}}(k, P)$.*

Proof. Proof follows from Lemma 3.4.3 and Lemma 3.4.4 in Section 3.4.2. □

3.4.2 Analysis

First, using control theoretic tools [23], we analyze the behavior of the sequence of covariance matrices

$$K_n := K_{\mathbf{X}_n}$$

where $\mathbf{X}_n$ is the transmitted vector at time n.

Lemma 3.4.2. *For the sequence K_n we have*

$$K_n \to \bar{K} \succ 0 \quad \text{as } n \to \infty \tag{3.41}$$

where $\bar{K}$ is the unique positive-definite solution to the following discrete algebraic Riccati equation (DARE)

$$K = AKA' - (AKB)(1 + B'KB)^{-1}(AKB)'. \tag{3.42}$$

Proof. From (3.38) we have

$$K_{i+1} = AK_{(\mathbf{X}_i - \hat{\mathbf{X}}_i)}A' \tag{3.43}$$

where

$$K_{(\mathbf{X}_i-\hat{\mathbf{X}}_i)} = K_{\mathbf{X}_i} - K_{\mathbf{X}_iY_i}K_{Y_i}^{-1}K'_{\mathbf{X}_iY_i} \tag{3.44}$$

is the error covariance matrix for the linear MMSE estimate of $\mathbf{X}_i$ given Y_i. Since $Y_i = B^T\mathbf{X}_i + Z_i$, where

$$B^T = [11\ldots1]_{(1\times k)} \tag{3.45}$$

we have

$$K_{(\mathbf{X}_i-\hat{\mathbf{X}}_i)} = K_i - (K_iB)(1+B'K_iB)^{-1}(K_iB)'. \tag{3.46}$$

Combining (3.43) and (3.46) we have the following Riccati recursion [24] for K_i:

$$K_{i+1} = AK_iA' - (AK_iB)(1+B'K_iB)^{-1}(AK_iB)'. \tag{3.47}$$

Since A has no unit-circle eigenvalue and the pair (A, B) is detectable [23], that is, there exists a matrix $C \in \mathbb{R}^{1\times k}$ such that all the eigenvalues of $A - BC$ lie inside the unit circle[1], we can use Lemma II.4 in [25] to show that (3.41) holds. □

Probability of error: The following lemma provides a sufficient condition such that $P_e^{(n)} \to 0$ as $n \to \infty$.

Lemma 3.4.3. *If $R_j < \log(\beta_j), j = 1, \ldots, k$, then $P_e^{(n)} \to 0$ as $n \to \infty$.*

Proof. Let the difference vector be

$$\mathbf{D}_n = \mathbf{\Theta} - \hat{\mathbf{\Theta}}_n.$$

[1]For a diagonal matrix $A = \mathrm{diag}([\lambda_1 \ldots \lambda_k])$ and a column vector $B = [b_1 \ldots b_k]'$, the pair (A,B) is detectable if and only if all the unstable eigenvalues λ_i, i.e. the ones on or outside the unit-circle, are distinct and the corresponding b_i are nonzero.

Considering (3.37), the probability of error can be bounded as

$$
\begin{aligned}
P_e^{(n)} &\leq \mathsf{P}\left(\bigcup_j \left\{|\mathbf{D}_n(j)| > 2^{-nR_j}\right\}\right) \\
&\leq \sum_{j=1}^{k} \mathsf{P}\left(\left\{|\mathbf{D}_n(j)| > 2^{-nR_j}\right\}\right) \qquad (3.48) \\
&\leq \sum_{j=1}^{k} 2^{2nR_j}\, \mathsf{E}(|\mathbf{D}_n(j)|^2), \qquad (3.49)
\end{aligned}
$$

where (3.48) and (3.49) follow from the union bound and the Chebyshev inequality, respectively.

To find $\mathsf{E}(|\mathbf{D}_n(j)|^2)$, note that from the encoding rule (3.38) we have

$$\mathbf{X}_n = A^n \mathbf{\Theta} - \sum_{i=0}^{n-1} A^{n-i} \hat{\mathbf{X}}_i.$$

Comparing this form of $\mathbf{X}_n$ with the decoding estimate rule (3.40), we can rewrite $\mathbf{D}_n$ as follows,

$$\mathbf{D}_n = A^{-n} \mathbf{X}_n.$$

Hence, $K_{\mathbf{D}_n} = A^{-n} K_n (A')^{-n}$ and the diagonal elements of $K_{\mathbf{D}_n}$ are

$$\mathsf{E}(|\mathbf{D}_n(j)|^2) = \beta_j^{-2n} (K_n)_{jj}.$$

Plugging $\mathsf{E}(|\mathbf{D}_n(j)|^2)$ into (3.49) we get

$$P_e^{(n)} \leq \sum_{j=1}^{k} (K_n)_{jj} \cdot 2^{2n(R_j - \log(\beta_j))}. \qquad (3.50)$$

From Lemma 3.4.2 we know that $\limsup_{n\to\infty} (K_n)_{jj} < \infty$. Therefore, it follows from (3.50) that $P_e \to 0$ as $n \to \infty$ if $R_j < \log(\beta_j)$ for $j = 1, \ldots, k$. $\square$

Asymptotic power allocation: For the linear code described above, the asymptotic power of user j is

$$\begin{aligned}\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\mathsf{E}(X_{ji}^2) &= \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}(K_i)_{jj}\\ &= \bar{K}_{jj}\end{aligned}$$

where $\bar{K}$ is the unique solution to (3.42) and the last equality follows from the Cesàro mean theorem and Lemma 3.4.2.

Thus, a rate-tuple $(R_1, \ldots, R_k)$ is achievable with the code described above if for some $(\beta_1, \ldots, \beta_k)$ satisfying

$$\log(\beta_j) > R_j$$

we can find a set of $(\omega_1, \ldots, \omega_k)$ such that the corresponding asymptotic power allocation $(\bar{K}_{11}, \ldots, \bar{K}_{kk})$ strictly satisfies the power constraints, i.e.,

$$\bar{K}_{jj} < P_j \quad j = 1, \ldots, k.$$

The strict condition above makes sure that the power constraint is satisfied for sufficiently large n.

The following lemma shows that for every sum rate $R < C_{\mathsf{L}}(k, P)$, there exists a choice of the coefficients $\{\beta_j\}$ and $\{\omega_j\}$ such that $\sum_{j=1}^{k}\log(\beta_j) > R$ and the corresponding asymptotic matrix $\bar{K}$ strictly satisfies the symmetric power constraints, i.e., $\bar{K}_{jj} < P$. Thus, the lemma establishes the achievability of the sum capacity $C_{\mathsf{L}}(k, P)$ and concludes our analysis.

Lemma 3.4.4. *Given a sum rate $R < C_{\mathsf{L}}(k, P)$, let A be of the form* (3.39) *with coefficients*

$$\beta_j = \beta, \quad j = 1, \ldots, k,$$

for some choice of $\beta > 1$ satisfying

$$R < k\log(\beta) < C_{\mathsf{L}}(k, P), \tag{3.51}$$

and with coefficients

$$\omega_j = e^{2\pi i \frac{(j-1)}{k}}, \quad j = 1, \ldots, k.$$

Then, the unique positive definite solution $\bar{K} \succ 0$ *of the discrete algebraic Riccati equation* (3.42) *satisfies*

$$\bar{K}_{jj} < P.$$

Before presenting the proof, we show that for this symmetric choice of A, the matrix $\bar{K}$ is completely characterized by β as follows.

Lemma 3.4.5. *Let* A *and* B *be of the form (3.39) and (3.45) with* $\beta_j = \beta$ *and* $\omega_j = e^{2\pi i \frac{(j-1)}{k}}$. *Then the unique positive-definite solution* $\bar{K} \succ 0$ *of the following discrete algebraic Riccati equation*

$$K = AKA' - AKB(1 + B'KB)^{-1}(AKB)',$$

is circulant with real eigenvalues satisfying

$$\lambda_i = \frac{1}{\beta^2}\lambda_{i-1},$$

for $i = 2, \ldots, k$. *The largest eigenvalue* λ_1 *satisfies*

$$1 + k\lambda_1 = \beta^{2k} \tag{3.52}$$

$$\Big(1 + \lambda_1\big(k - \frac{\lambda_1}{\bar{K}_{jj}}\big)\Big) = \beta^{2(k-1)}. \tag{3.53}$$

Proof. See Section 3.6.6.

We use this lemma to prove Lemma 3.4.4.

Proof of Lemma 3.4.4: From (3.52) we have

$$\frac{1}{2}\log(1 + k\lambda_1) = k\log(\beta).$$

and thus by (3.51)

$$\frac{1}{2}\log(1 + k\lambda_1) < C_{\mathsf{L}}(k, P) = \frac{1}{2}\log\left(1 + kP\phi(k, P)\right).$$

We can hence conclude that

$$\lambda_1 < P\phi(k, P). \tag{3.54}$$

On the other hand, from (3.52) and (3.53) we have

$$\Big(1 + k\lambda_1\Big)^{k-1} = \left(1 + \lambda_1\Big(k - \frac{\lambda_1}{\bar{K}_{jj}}\Big)\right)^k,$$

and hence by the definition of the function $\phi(k, \cdot)$ in Theorem 3.2.1,

$$\lambda_1 = \bar{K}_{jj}\phi(k, \bar{K}_{jj}). \tag{3.55}$$

Combining (3.54) and (3.55) we get

$$\bar{K}_{jj}\phi(k, \bar{K}_{jj}) < P\phi(k, P)$$

and the monotonicity of $\phi(k, \cdot)$ completes the proof.

3.5 Discussion

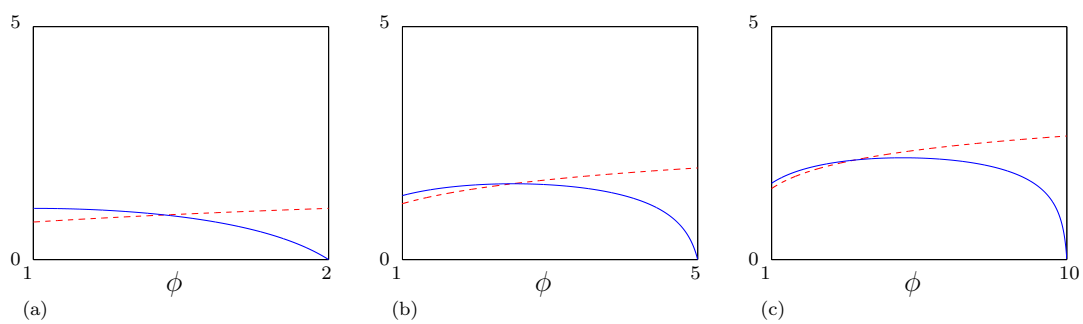


Figure 3.3: $C_1(P, \phi)$ (dashed) and $C_2(P, \phi)$ for $P = 2$ and (a) $k = 2$ (b) $k = 5$ (c) $k = 10$

It is still unknown whether the linear sum capacity $C_{\mathsf{L}}(k, P)$ is in general equal to the sum capacity $C(k, P)$ under symmetric power constraints P for all

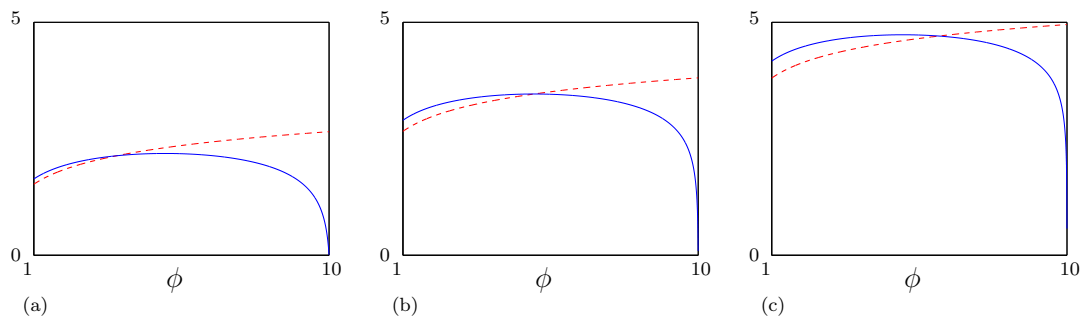


Figure 3.4: $C_1(P,\phi)$ (dashed) and $C_2(P,\phi)$ for $k = 10$ and (a) $P = 2$ (b) $P = 20$ (c) $P = 200$

k senders. However, we know [14] that they coincide if the power P exceeds the threshold $P_c(k) \geq 0$, which is the unique solution to

$$(1 + k^2 P/2)^{k-1} = (1 + k^2 P/4)^k. \tag{3.56}$$

We show that the condition (3.56) corresponds to the case where the the linear sum capacity $C_{\mathsf{L}}(k,P)$ coincides with the following cutset upper bound [11] on the sum capacity,

$$C(k,P) \leq \max_{\phi} \min \Big\{ C_1(P,\phi), C_2(P,\phi) \Big\}. \tag{3.57}$$

Here, the functions $C_1(P,\phi), C_2(P,\phi)$ are same as in (3.21).

Towards this end, note that $\phi(k,P)$ defined in Theorem 3.2.1, is the unique solution to $C_1(P,\phi) = C_2(P,\phi)$ for fixed k and P, and the linear sum capacity is

$$C_{\mathsf{L}}(k,P) = C_1(P,\phi(k,P)) = C_2(P,\phi(k,P)).$$

Since the functions $C_1(P,\phi)$ and $C_2(P,\phi)$ are concave in ϕ (see Section 3.6.1) and $C_1(P,\phi)$ is increasing in ϕ, the intersection point of the two functions and the max-min in (3.57) coincides if and only if $C_2(P,\phi)$ is nonincreasing at $\phi(k,P)$ (see

Fig. 3.3 (a,b) and Fig. 3.4 (b,c)), that is,

$$\frac{\partial C_2(P,\phi)}{\partial \phi}\Big|_{\phi(k,P)} \leq 0. \tag{3.58}$$

Considering (3.21), the condition (3.58) is equivalent to

$$\phi(k,P) \geq k/2$$

and plugging $\phi(k,P) = k/2$ into (3.2) gives (3.56).

For $P < P_c$, we conjecture that we still have $C(k,P) = C_{\mathsf{L}}(k,P)$ based on the properties of Hirschfeld–Gebelein–Rényi maximal correlation [20]. In the following we provide some insights.

Let $\rho^*(\Theta_1,\Theta_2)$ denote the maximal correlation between two random variables Θ_1 and Θ_2 as defined in [20]:

$$\rho^*(\Theta_1,\Theta_2) = \sup_{g_1,g_2} \mathsf{E}\left(g_1(\Theta_1)g_2(\Theta_2)\right) \tag{3.59}$$

where the supremum is over all functions g_1, g_2 such that

$$\mathsf{E}(g_1) = \mathsf{E}(g_2) = 0 \quad \text{and} \quad \mathsf{E}(g_1^2) = \mathsf{E}(g_2^2) = 1.$$

We extend this notion of maximal correlation to *conditional maximal correlation* as follows. Let the random variables Θ_1, Θ_2, Y be given. The conditional maximal correlation between Θ_1 and Θ_2 given a common random variable Y is defined as

$$\rho^*(\Theta_1,\Theta_2|Y) = \sup_{g_1,g_2} \mathsf{E}\left(g_1(\Theta_1,Y)g_2(\Theta_2,Y)\right) \tag{3.60}$$

where the supremum is over all functions g_1, g_2 such that

$$\mathsf{E}(g_1|Y) = \mathsf{E}(g_2|Y) = 0 \quad \text{and} \quad \mathsf{E}(g_1^2) = \mathsf{E}(g_2^2) = 1.$$

The assumption $\mathsf{E}(g_1|Y) = \mathsf{E}(g_2|Y) = 0$ is crucial; otherwise, g_1 and g_2 can be picked as Y and $\rho^*(\Theta_1,\Theta_2|Y) = 1$ trivially. For conditional maximal correlation

we have the following lemma.

Lemma 3.5.1. *If* (Θ_1, Θ_2, Y) *are jointly Gaussian, then*

$$\rho^*(\Theta_1, \Theta_2|Y) = \rho(\Theta_1, \Theta_2|Y)$$

and linear functions $g_1^{\mathsf{L}}, g_2^{\mathsf{L}}$ *of the form*

$$\begin{aligned} g_1^{\mathsf{L}}(\Theta_1, Y) &= \frac{\Theta_1 - \mathsf{E}(\Theta_1|Y)}{\sqrt{\mathsf{E}\left((\Theta_1 - \mathsf{E}(\Theta_1|Y))^2\right)}} \\ g_2^{\mathsf{L}}(\Theta_2, Y) &= \frac{\Theta_2 - \mathsf{E}(\Theta_2|Y)}{\sqrt{\mathsf{E}\left((\Theta_2 - \mathsf{E}(\Theta_2|Y))^2\right)}} \end{aligned} \tag{3.61}$$

attain the supremum in $\rho^*(\Theta_1, \Theta_2|Y)$.

Proof. See Section 3.6.7.

Based on the conditional maximal correlation, we now present an upper bound on the (general) sum capacity. For simplicity, we focus on $k = 2$ and equal per-symbol power constraints $\mathsf{E}(X_{ji}^2) \leq P$, for $j = 1, 2$. Also, without loss of generality, we assume that the message $M_j \in \{1, \ldots, 2^{nR}\}$ is mapped to a message point $\Theta_j \in \mathbb{R}$ and X_{ji} is a function of (Θ_j, Y^{i-1}). Note that by picking the identity mapping we have $\Theta_j = M_j$.

Lemma 3.5.2. *A sum rate* R*, achievable by a code with block length* n *and per-symbol power constraints* $\mathsf{E}(X_{ji}^2) \leq P$*, is upper bounded as*

$$R \leq \frac{1}{n} \sum_{i=1}^{n} I(X_{1i}, X_{2i}; Y_i|Y^{i-1}) + \epsilon_n \tag{3.62}$$

$$\leq \frac{1}{2n} \sum_{i=1}^{n} \log\left(1 + 2P\left(1 + \rho^*\left(\Theta_{1i}, \Theta_{2i}\middle|Y^{i-1}\right)\right)\right) + \epsilon_n \tag{3.63}$$

where $\epsilon_n \to 0$ *as* $n \to \infty$.

Proof. See Section 3.6.8.

Consider the multi-letter maximization problem where the objective function is the right hand side of (3.62). For the special class of Gaussian message

points $(\Theta_1, \Theta_2) \sim \mathrm{N}(0, K_{\Theta_1,\Theta_2})$, we show that linear functions are greedy optimal for this maximization problem.

First note that the first term $I(X_{11}, X_{21}; Y_1)$ is maximized by linear functions, because (Θ_1, Θ_2) are Gaussian. Now, suppose that we have used linear functions up to time $i-1$ and therefore $(\Theta_1, \Theta_2, Y^{i-1})$ are Gaussian. Then, by Lemma 3.5.1 we know that $\rho^*(\Theta_1, \Theta_2|Y^{i-1}) = \rho(\Theta_1, \Theta_2|Y^{i-1})$ and $X_{ji} = \mathsf{L}_{ji}(\Theta_j, Y^{i-1})$, where L_{ji} is of the form (3.61), achieves the conditional maximal correlation. Hence, the i-th term $I(X_{1i}, X_{2i}; Y_i|Y^{i-1})$ which is upper bounded by (see Section 3.6.8)

$$\frac{1}{2}\log\Big(1 + 2P\Big(1 + \rho^*\big(\Theta_{1i}, \Theta_{2i}\big|Y^{i-1}\big)\Big)\Big)$$

is maximized by linear functions of the form (3.61). A similar argument holds for any number of senders k, where we have the the following upper bound,

$$\begin{aligned} R &\leq \frac{1}{n}\sum_{i=1}^{n} I(X(\mathcal{S}); Y_i|Y^{i-1}) \\ &\leq \frac{1}{2n}\sum_{i=1}^{n}\log\Big(1 + kP + P\sum_{j\neq k}\rho^*\big(\Theta_{ji}, \Theta_{ki}\big|Y^{i-1}\big)\Big). \end{aligned}$$

Therefore, in establishing the sum rate optimality of linear codes, the missing step is as follows. We need to show that without loss of optimality we can consider only Gaussian message points and that linear functions are not only greedy optimal but also globally optimal for maximizing the right hand side of (3.62). Note that using functions which might hurt the current mutual information term $I(X_i(\mathcal{S}); Y_i|Y^{i-1})$ at time i, can be potentially advantageous for the future terms $I(X_{i'}(\mathcal{S}); Y_{i'}|Y^{i'-1}), i' > i$. Hence, this last step requires an analysis which captures the effect of the functions used at each time i, on the joint distribution of all the random variables $(\Theta(\mathcal{S}), X^n(\mathcal{S}), Y^n)$ in the entire block.

3.6 Proof of the Lemmas

3.6.1 Proof of Lemma 3.3.2

Using similar argument as in Bergstrøm's theorem [22, Theorem, 17.10.1], we show both $f_1(K)$ and $f_2(K)$ are concave in K, where

$$f_1(K) = \frac{1}{2}\log\left(1 + \sum_{j,j'} K_{jj'}\right)$$

and

$$f_2(K) = \frac{1}{2(k-1)}\sum_{j=1}^{k}\log\left[1 + \sum_{j',j''} K_{j'j''} - \frac{\left(\sum_{j'} K_{jj'}\right)^2}{K_{jj}}\right].$$

Let $X(\mathcal{S}) = X^{(t)}(\mathcal{S})$, $\mathsf{P}(t=1) = \lambda = 1 - \mathsf{P}(t=2)$, $X^{(1)}(\mathcal{S}) \sim N(0, K_1), X^{(2)}(\mathcal{S}) \sim N(0, K_2)$ and $Y = Y^{(t)} = \sum_{j=1}^{k} X_j^{(t)} + Z$, where $Z \sim \mathrm{N}(0,1)$. Assume $Z, X^{(1)}, X^{(2)}$, and t are independent. Under these assumptions, the covariance matrix of $X(\mathcal{S})$ is given by $K = \lambda K_1 + (1-\lambda)K_2$ and

$$f_1(K) = \frac{1}{2}\log(\mathrm{Var}(Y)) \tag{3.64}$$

and

$$f_2(K) = \frac{1}{2(k-1)}\sum_{j=1}^{k}\log(\mathrm{Var}(Y|X_j)). \tag{3.65}$$

Note that since $X(\mathcal{S})$ and Y are jointly Gaussian $\mathrm{Var}(Y|X_j)$ is a constant independent of X_j. Consider

$$\begin{aligned}
&\frac{\lambda}{2}\log\mathrm{Var}(Y^{(1)}|X_j^{(1)}) + \frac{(1-\lambda)}{2}\log\mathrm{Var}(Y^{(2)}|X_j^{(2)}) \\
&\quad = \frac{\lambda}{2}\log\left(\frac{\left|K_{Y^{(1)},X_j^{(1)}}\right|}{\left|K_{X_j^{(1)}}\right|}\right) + \frac{(1-\lambda)}{2}\log\left(\frac{\left|K_{Y^{(2)},X_j^{(2)}}\right|}{\left|K_{X_j^{(2)}}\right|}\right) \\
&\quad = \lambda(h(Y^{(1)}|X_j^{(1)}) - h(Z)) + (1-\lambda)(h(Y^{(2)}|X_j^{(2)}) - h(Z))
\end{aligned} \tag{3.66}$$

$$
\begin{aligned}
&= h(Y^{(t)}|X_j^t, t) - h(Z) \\
&\leq h(Y|X_j) - h(Z) \\
&= \frac{1}{2}\log\frac{|K_{Y,X_j}|}{|K_{X_j}|} \\
&= \frac{1}{2}\log \mathrm{Var}(Y|X_j).
\end{aligned} \tag{3.67}
$$

where (3.66) and (3.67) come form the fact that $Y^{(t)}$ is jointly Gaussian with $X_j^{(t)}$. Thus $\mathrm{Var}(Y|X_j)$ is concave in K for all j. The same argument holds for $h(Y)$. Then, concavity of $f_1(K)$ and $f_2(K)$ in K follows.

3.6.2 Proof of Lemma 3.3.3

Let $X_{ji} = \mathsf{L}_{ji}(\mathbf{V}_j, Y^{i-1})$ for $i = 1, \ldots, n$ and $j = 1, \ldots, k$ such that $\mathbf{V}_j \in \mathbb{C}^n$ is independent of $\{\mathbf{V}_{j'} : j' \neq j\}$ and Z^n. We show that

$$
\begin{aligned}
\sum_{i=1}^{n} \Big(& I(X_i(\mathcal{S}); Y_i|Y^{i-1}) \\
& \leq \frac{1}{k-1}\sum_{i=1}^{n}\sum_{j=1}^{k} I(X_i(\mathcal{S}\backslash\{j\}); Y_i|Y^{i-1}, X_{ji})\Big).
\end{aligned} \tag{3.68}
$$

By independence of $\mathbf{V}_j$'s we have

$$
h(\mathbf{V}(\mathcal{S})) = \sum_{j=1}^{k} h(\mathbf{V}_j). \tag{3.69}
$$

Consider

$$
\begin{aligned}
0 &\leq I(\mathbf{V}(\mathcal{S}); Y^n) - \sum_{j=1}^{k} I(\mathbf{V}_j; Y^n) \qquad (3.70) \\
&= \sum_{i=1}^{n}\Big[I(\mathbf{V}(\mathcal{S}); Y_i|Y^{i-1}) - \sum_{j=1}^{k} I(\mathbf{V}_j; Y_i|Y^{i-1})\Big] \\
&= \sum_{i=1}^{n}\Big[I(\mathbf{V}(\mathcal{S}), X_i(\mathcal{S}); Y_i|Y^{i-1}) - \sum_{j=1}^{k} I(\mathbf{V}_j, X_{ji}; Y_i|Y^{i-1})\Big]
\end{aligned}
$$

$$\leq \sum_{i=1}^{n} \Big[I(X_i(\mathcal{S}); Y_i | Y^{i-1}) - \sum_{j=1}^{k} I(X_{ji}; Y_i | Y^{i-1}) \Big]. \tag{3.71}$$

where inequality (3.70) follows from (3.69) and the fact that conditioning reduces entropy. Inequality (3.71) follows from the facts that mutual information is positive and that the following Markov chain holds

$$\mathbf{V}(\mathcal{S}) \to (X_i(\mathcal{S}), Y^{i-1}) \to Y_i.$$

Adding $(k-1)\sum_{i=1}^{n} I(X_i(\mathcal{S}); Y_i | Y^{i-1})$ to both sides in (3.71) and rearranging terms we have

$$\sum_{i=1}^{n} \Big(I(X_i(\mathcal{S}); Y_i | Y^{i-1}) \\ \leq \frac{1}{k-1} \sum_{i=1}^{n} \sum_{j=1}^{k} I(X_i(\mathcal{S} \backslash \{j\}); Y_i | Y^{i-1}, X_{ji}) \Big).$$

3.6.3 Proof of Lemma 3.3.6

We show

$$g(\gamma, x, \phi) = (1-\gamma) C_1(x, \phi) + \gamma C_2(x, \phi).$$

where

$$C_1(x, \phi) = \frac{1}{2} \log(1 + kx\phi)$$
$$C_2(x, \phi) = \frac{k}{2(k-1)} \log(1 + (k-\phi)x\phi), \tag{3.72}$$

is concave in ϕ for fixed $x, \gamma \geq 0$.

Note that $C_1(x, \phi) = f_1(K)$ and $C_2(x, \phi) = f_2(K)$ for symmetric K given in (3.22) (see (3.21)). For general $K \succeq 0$ with fixed diagonal elements we prove that $(1-\gamma) f_1(K) + \gamma f_2(K)$ is concave in K for any $\gamma \geq 0$ and concavity of $g(\gamma, x, \phi)$ in ϕ for fixed x, γ immediately follows.

Let $X = X_1, \ldots, X_k \sim N(0, K)$ and $Y = \sum_{j=1}^{k} X_j + Z$, where $Z \sim \mathrm{N}(0, 1)$

is independent of $X_1, \ldots, X_k$. Then, we have

$$\begin{aligned}
&(1-\gamma)f_1(K) + \gamma f_2(K) \\
&\quad = (1-\gamma)h(Y) + \frac{\gamma}{k-1}\sum_{j=1}^{k} h(Y|X_j) \\
&\quad = (1-\gamma)h(Y) + \frac{\gamma}{k-1}\sum_{j=1}^{k} \Big(h(Y) + h(X_j|Y) - h(X_j)\Big) \\
&\quad = h(Y)\Big(1 + \frac{\gamma}{k-1}\Big) + \frac{\gamma}{k-1}\sum_{j=1}^{k} h(X_j|Y) - h(X_j).
\end{aligned}$$

By Lemma 3.3.2, we know that $h(Y)$ and $h(X_j|Y)$ are concave in K. If the diagonal of K are fixed then $h(X_j) = \frac{1}{2}\log(2\pi e K_{jj})$ is also fixed and as long as $\gamma \geq 0$, $(1-\gamma)f_1(K) + \gamma f_2(K)$ is concave in K.

3.6.4 Proof of Lemma 3.3.7

Let $\gamma, x \geq 0$ and $\phi^*(\gamma, x) > 0$ be the positive solution to

$$\frac{(1-\gamma)(k-1)}{1+\ kx\phi} = \frac{\gamma(2\phi - k)}{1 + x\phi(k-\phi)}. \tag{3.73}$$

and

$$g(\gamma, x, \phi) = (1-\gamma)C_1(x, \phi) + \gamma C_2(x, \phi).$$

We show $g(\gamma, x, \phi^*(\gamma, x))$ is increasing and concave in x. Let

$$g(x, \phi) := (1-\gamma)C_1(x, \phi) + \gamma C_2(x, \phi). \tag{3.74}$$

Note that $g(x, \phi)$ is same as $g(\gamma, x, \phi)$, but for simplicity we do not include γ explicitly. Similarly, let

$$\phi^*(x) := \phi^*(\gamma, x).$$

Equation (3.73) can be written as

$$a\phi^2 + b\phi + c = 0 \tag{3.75}$$

where

$$a = (k + \gamma - 1 + \gamma k)x$$
$$b = -k(k + \gamma - 1)x + 2\gamma$$
$$c = -(k + \gamma - 1).$$

Since $ac < 0$, there is a unique positive solution $\phi^*(x) > 0$, where

$$0 < \phi^*(x) = \frac{-b + \sqrt{b^2 - 4ac}}{2a}. \tag{3.76}$$

We wish to show that the first derivative of

$$f(x) := g(x, \phi^*(x)).$$

is positive and the second derivative is negative.

First derivative: As shown in (3.30), for $\phi^*(x)$ which satisfy (3.73) we have

$$\frac{\partial g(x,\phi)}{\partial \phi}\Big|_{x,\phi^*(x)} = 0.$$

Hence,

$$\begin{aligned}\frac{df(x)}{dx} &= \frac{\partial g(x,\phi)}{\partial x} + \frac{\partial g(x,\phi)}{\partial \phi}\frac{d\phi}{dx}\Big|_{x,\phi^*(x)} \\ &= \frac{\partial g(x,\phi)}{\partial x}\Big|_{x,\phi^*(x)}\end{aligned}$$

Plugging $C_1(x,\phi)$ and $C_2(x,\phi)$ from (3.72) in $g(x,\phi)$, we have

$$\begin{aligned}\frac{df(x)}{dx} &= (1-\gamma)\frac{k\phi}{1+kx\phi} + \gamma\frac{k\phi(k-\phi)}{(k-1)(1+x\phi(k-\phi))}\Big|_{x,\phi^*(x)} \\ &= \frac{k\phi}{1+kx\phi} \times \left(1 - \gamma + \gamma\frac{(k-\phi)(1+kx\phi)}{(k-1)(1+x\phi(k-\phi))}\right)\Bigg|_{x,\phi^*(x)} \\ &= \frac{k(\gamma-1)(\phi^*(x))^2}{(1+kx\phi^*(x))(k-2\phi^*(x))} \qquad (3.77) \\ &\geq 0 \qquad (3.78)\end{aligned}$$

where equality (3.77) follows from the fact that $\phi^*(x)$ satisfies (3.73), and inequality (3.78) follows from the fact that $(1-\gamma)$ and $(2\phi^*(x)-k)$ have the same sign (see (3.73)).

Second derivative: For $0 \le \gamma \le 1$, the concavity is immediate since

$$C_1(x,\phi) = f_1(K)$$
$$C_2(x,\phi) = f_2(K)$$

for symmetric K given in (3.22) (see (3.21)) and $f_1(K)$ and $f_2(K)$ are concave in K (see Appendix 3.6.1).

To prove the concavity of $f(x)$ for $\gamma > 1$, we show that

$$\frac{d^2 f(x)}{dx^2} < 0.$$

From (3.77) we have

$$\frac{df(x)}{dx} = k(\gamma-1)\tilde{f}(x),$$

where

$$\tilde{f}(x) := h(x,\phi^*(x))$$
$$h(x,\phi) := \frac{\phi^2}{(1+kx\phi)(k-2\phi)}.$$

Therefore it is enough to show that

$$\frac{d\tilde{f}(x)}{dx} < 0.$$

Consider

$$\begin{aligned}
\frac{d\tilde{f}(x)}{dx} &= \frac{\partial h(x,\phi)}{\partial x} + \frac{\partial h(x,\phi)}{\partial \phi}\frac{d\phi}{dx}\Big|_{x,\phi^*(x)} \\
&= \frac{-k\phi^3}{(1+kx\phi)^2(k-2\phi)} + \frac{\phi(k^2x\phi+2(k-\phi))}{(1+kx\phi)^2(k-2\phi)^2}\frac{d\phi}{dx}\Big|_{x,\phi^*(x)} \\
&= \phi \cdot \frac{\frac{d\phi}{dx}\Big(k^2x\phi+2(k-\phi)\Big) - k\phi^2(k-2\phi)}{(1+kx\phi)^2(k-2\phi)^2}\Big|_{x,\phi^*(x)}
\end{aligned}$$

Since $\phi > 0$ and the denominator is also positive we need to show

$$\frac{d\phi^*(x)}{dx} < \left.\frac{k\phi^2(k-2\phi)}{k^2x\phi + 2(k-\phi)}\right|_{x,\phi^*(x)} \tag{3.79}$$

For the rest of the proof, with abuse of notation, we alternatively use ϕ for $\phi^*(x)$, the positive solution of (3.75). Taking the derivative of (3.75) with respect to x we have

$$\begin{aligned}\frac{d\phi^*(x)}{dx} &= \frac{-\phi^2(a'\phi + b')}{2a\phi^2 + b\phi} \\ &= \frac{-\phi^2(a'\phi + b')}{a\phi^2 - c}.\end{aligned} \tag{3.80}$$

where

$$\begin{aligned}a' &= k + \gamma - 1 + \gamma k \\ b' &= -k(k + \gamma - 1).\end{aligned} \tag{3.81}$$

are derivatives of a, b with respect to x. Defining

$$\alpha := \frac{k + \gamma - 1}{k}$$

we have $a = k(\alpha+\gamma)x,\ b = -k^2\alpha x + 2\gamma,\ c = -\alpha k,\ a' = k(\alpha+\gamma),\ b' = -k^2\alpha$, and

$$\begin{aligned}\frac{d\phi^*(x)}{dx} &= \frac{-\phi^2(a'\phi + b')}{a\phi^2 - c}, \\ &= \frac{k\phi^2(k\alpha - (\alpha+\gamma)\phi)}{(\alpha+\gamma)kx\phi^2 + \alpha k} \\ &= \frac{k\phi^2(k - \beta\phi)}{\beta kx\phi^2 + k},\end{aligned} \tag{3.82}$$

where

$$\beta := 1 + \frac{\gamma}{\alpha}.$$

It is not hard to see that $\beta \in (2, k+1\big)$ for $\gamma > 1$. Considering (3.82), (3.79)

becomes equivalent to

$$\begin{aligned} & \frac{k-\beta\phi}{k-2\phi} < \frac{\beta k x\phi^2 + k}{k^2 x\phi + 2(k-\phi)} \\ \iff \quad & \frac{k-\beta\phi}{k-2\phi} < \frac{k-\beta\phi+\beta\phi(kx\phi+1)}{k-2\phi+k(kx\phi+1)} \\ \iff \quad & \frac{k-\beta\phi}{k-2\phi} < \frac{\beta\phi}{k}, \end{aligned} \tag{3.83}$$

where (3.83) follows from the fact that for $b, d > 0$,

$$\frac{a}{b} < \frac{c}{d} \quad \Leftrightarrow \quad \frac{a}{b} < \frac{a+c}{b+d}. \tag{3.84}$$

Considering (3.84) again with $c = d = 2\phi$ and noting that $\beta > 2$, we can see that to prove (3.83) it is sufficient to show

$$\begin{aligned} & \frac{k-(\beta-2)\phi}{k} \leq \frac{\beta\phi}{k} \\ \iff \quad & \frac{k+\gamma-1}{2\gamma} \leq \phi. \end{aligned} \tag{3.85}$$

To show the last condition, note that

$$\phi^*(0) = \frac{k+\gamma-1}{2\gamma}. \tag{3.86}$$

$$\left.\frac{d\phi^*}{dx}\right|_{x=0} > 0. \tag{3.87}$$

where (3.86) follows from (3.75). Condition (3.87) follows from (3.80) and the facts that $2a\phi^*(0) + b > 0$ by (3.76) and that for $\gamma > 1$, $a'\phi^*(0) + b' < 0$. Therefore, condition (3.85) holds and the proof is complete.

3.6.5 Proof of Lemma 3.3.8

We show that for a fixed $x \geq 0$, $C_2(x,\phi) - C_1(x,\phi) = 0$ has a unique solution $1 \leq \phi(k,x) \leq k$. Moreover,

$$1 + \frac{(2\phi(k,x)-k)(1+kx\phi(k,x))}{(k-1)(1+x\phi(k,x)(k-\phi(k,x)))} > 0. \tag{3.88}$$

Let $f(\phi) = C_2(x,\phi) - C_1(x,\phi)$. We prove there exists a unique solution by showing $f(1) \geq 0$, $f(k) < 0$, and $f'(\phi) < 0$ for $1 \leq \phi \leq k$. The fact that $f(k) < 0$ is immediate. Condition $f(1) \geq 0$ is equivalent to

$$\Big(1 + x(k-1)\Big)^k \geq \Big(1 + kx\Big)^{k-1}.$$

For the above condition to hold it is sufficient that

$$\binom{k}{i}(k-1)^i \geq \binom{k-1}{i}k^i, \tag{3.89}$$

which is true since $(1 - 1/k)^i \geq 1 - i/k$ for $k > 1$.

Finally, we need to show $f'(\phi) < 0$ which is equivalent to

$$\frac{k - 2\phi}{1 + x\phi(k-\phi)} - \frac{k-1}{1 + kx\phi} < 0. \tag{3.90}$$

Rearranging the terms we have

$$1 + kx\phi - (2\phi + x\phi^2 + kx\phi^2) < 0,$$

which holds for any $\phi \geq 1$. This completes the proof of the uniqueness. Moreover, the condition (3.88) follows from plugging $\phi(k,x)$ in (3.90).

3.6.6 Proof of Lemma 3.4.5

Let A be of the form (3.39) with $\beta_j = \beta$ and $\omega_j = e^{2\pi i \frac{(j-1)}{k}}$ and $B = \mathbf{1}_{k\times 1}$ same as (3.45). We show that the unique positive-definite solution $\bar{K} \succ 0$ of the following discrete algebraic Riccati equation

$$K = AKA' - AKB(1 + B'KB)^{-1}(AKB)',$$

is circulant with real eigenvalues satisfying

$$\lambda_i = \frac{1}{\beta^2}\lambda_{i-1},$$

for $i = 2, \ldots, k$ and the largest eigenvalue λ_1 satisfies

$$1 + k\lambda_1 = \beta^{2k}$$
$$\Big(1 + \lambda_1\big(k - \frac{\lambda_1}{\bar{K}_{jj}}\big)\Big) = \beta^{2(k-1)}.$$

We know that any circulant matrix can be written as $Q\Lambda Q'$, where Q is the k point DFT matrix with

$$Q_{j\ell} = \frac{1}{\sqrt{k}} e^{-2\pi i(j-1)(\ell-1)/k}, \tag{3.91}$$

and $\Lambda = \mathrm{diag}([\lambda_1, \ldots, \lambda_k])$ is the matrix with eigenvalues on its diagonal. We show that the circulant matrix $\bar{K} = Q\Lambda Q'$ with positive $\lambda_j > 0$, such that $\lambda_j = \lambda_{j-1}/\beta^2$ for $j \geq 2$, satisfies the Riccati equation (3.42). Plugging $Q\Lambda Q'$ into (3.42) and rearranging we get

$$\Lambda = (Q'AQ)\Lambda(Q'AQ)' - ((Q'AQ)\ \Lambda\ (Q'B))$$
$$(1 + B'Q\Lambda Q'B)^{-1}((Q'AQ)\ \Lambda\ (Q'B))'.$$

For this symmetric choice of A we have

$$Q'AQ = \beta \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & 0 \end{pmatrix}, Q'B = \begin{pmatrix} \sqrt{k} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Hence,

$$(Q'AQ)\Lambda(Q'AQ)' = \beta^2 \begin{pmatrix} \lambda_2 & 0 & \ldots & 0 \\ 0 & \lambda_3 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda_1 \end{pmatrix}$$

$$(Q'AQ)\Lambda(Q'B) = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ \beta\lambda_1\sqrt{k} \end{pmatrix}$$

and the Riccati equation turns into k diagonal equations. The first $k-1$ equations are

$$\lambda_j = \beta^2\lambda_{j+1}, \quad j = 1, \ldots, k-1 \tag{3.92}$$

and the k-th equation is

$$\lambda_k = \beta^2\lambda_1 - \frac{\beta^2\lambda_1^2 k}{1 + k\lambda_1}. \tag{3.93}$$

From (3.92) we see that λ_1 is the largest eigenvalue and $\lambda_k = \beta^{-2(k-1)}\lambda_1$. Combining this fact with (3.93) we get

$$(1 + k\lambda_1) = \beta^{2k}. \tag{3.94}$$

Hence, λ_1 is real and so are $\lambda_j, j = 2, \ldots, k$. Note that from the form of Q in (3.91), $\lambda_1 = \sigma_1$ where

$$\sigma_j := \sum_{\ell=1}^{k} \bar{K}_{j\ell}.$$

Moreover, since $\bar{K}$ is circulant $\sigma_j = \sigma_1$ for all j, and $(1 + B'\bar{K}B) = 1 + k\lambda_1$. Hence, the diagonal equations of the original (not the eigenvalue equations) Riccati equation (3.42) can be written as

$$\bar{K}_{jj} = \beta^2\bar{K}_{jj} - \beta^2\frac{\sigma_j^2}{(1 + B'\bar{K}B)}, \quad j = 1, \ldots, k \tag{3.95}$$

which are equivalent to

$$\beta^2 = \frac{1 + k\lambda_1}{1 + \lambda_1\left(k - \frac{\lambda_1}{\bar{K}_{jj}}\right)}, \quad j = 1, \ldots, k.$$

Finally, by (3.94) we have

$$\Big(1+\lambda_1\big(k-\frac{\lambda_1}{\bar{K}_{jj}}\big)\Big)=\beta^{2(k-1)}.$$

3.6.7 Proof of Lemma 3.5.1

We show that for jointly Gaussian (Θ_1,Θ_2,Y), we have

$$\rho^*(\Theta_1,\Theta_2|Y)=\rho(\Theta_1,\Theta_2|Y)$$

and linear functions $g_1^{\mathsf{L}},g_2^{\mathsf{L}}$ of the form

$$\begin{aligned} g_1^{\mathsf{L}}(\Theta_1,Y)&=\frac{\Theta_1-\mathsf{E}(\Theta_1|Y)}{\sqrt{\mathsf{E}\left((\Theta_1-\mathsf{E}(\Theta_1|Y))^2\right)}}\\ g_2^{\mathsf{L}}(\Theta_2,Y)&=\frac{\Theta_2-\mathsf{E}(\Theta_2|Y)}{\sqrt{\mathsf{E}\left((\Theta_2-\mathsf{E}(\Theta_2|Y))^2\right)}} \end{aligned} \tag{3.96}$$

attain the supremum in $\rho^*(\Theta_1,\Theta_2|Y)$.

Let (U,V) be two zero-mean jointly Gaussian random variables with correlation $\rho(U,V)$. It is well known [26] that

$$\rho^*(U,V)=\rho(U,V). \tag{3.97}$$

Hence, the maximal correlation $\rho^*(U,V)$ is attained by linear functions

$$g_1^{\mathsf{L}}(U)=\frac{U}{\sqrt{\mathsf{E}(U^2)}},\ g_2^{\mathsf{L}}(V)=\frac{V}{\sqrt{\mathsf{E}(V^2)}}.$$

Since (Θ_1,Θ_2,Y) is Gaussian we know that given $Y=y$, $(\Theta_1,\Theta_2)\big|_{Y=y}$ is Gaussian with some correlation

$$\rho(\Theta_1,\Theta_2\big|Y=y)=\rho \quad \text{for all } y \tag{3.98}$$

independent of y. From (3.97) and (3.98), we have

$$\rho^*(\Theta_1, \Theta_2 \big| Y = y) = \rho(\Theta_1, \Theta_2 | Y = y) = \rho \quad \text{for all } y \tag{3.99}$$

and therefore

$$\begin{aligned}
&\rho^*(\Theta_1, \Theta_2 | Y) \\
&\quad = \sup_{g_1, g_2} \mathsf{E}\left(g_1(\Theta_1, Y) g_2(\Theta_2, Y)\right) \\
&\quad = \sup_{g_1, g_2} \mathsf{E}_Y\left(\mathsf{E}\left(g_1(\Theta_1, Y = y) g_2(\Theta_2, Y = y)\right)\right) \\
&\quad \leq \mathsf{E}_Y\left(\sup_{g_1, g_2} \mathsf{E}\left(g_1(\Theta_1, Y = y) g_2(\Theta_2, Y = y)\right)\right) && (3.100) \\
&\quad = \mathsf{E}_Y\left(\rho^*(\Theta_1, \Theta_2 \big| Y = y)\right) \\
&\quad = \rho && (3.101)
\end{aligned}$$

where inequality (3.100) follows from Jensen's inequality and equality (3.101) follows from (3.99). It is easy to check that for linear functions $g_1^{\mathsf{L}}, g_2^{\mathsf{L}}$ of the form (3.96) we have

$$\mathsf{E}(g_1 | Y) = \mathsf{E}(g_2 | Y) = 0, \mathsf{E}(g_1^2) = \mathsf{E}(g_2^2) = 1 \tag{3.102}$$

and

$$\mathsf{E}\left(g_1(\Theta_1, Y) g_2(\Theta_2, Y)\right) = \rho. \tag{3.103}$$

From (3.101), (3.102) and (3.103) we conclude that linear functions of the form (3.96) achieves the supremum in $\rho^*(\Theta_1, \Theta_2 | Y)$.

3.6.8 Proof of Lemma 3.5.2

For a sum rate R achievable by a code with block length n and per-symbol power constraints $\mathsf{E}(X_{ji}^2) \leq P$ for $j = 1, 2$, we show

$$R \leq \frac{1}{2n} \sum_{i=1}^{n} \log \Big(1 + 2P\Big(1 + \rho^*\big(\Theta_{1i}, \Theta_{2i}\big|Y^{i-1}\big)\Big)\Big) + \epsilon_n \tag{3.104}$$

where $\epsilon_n \to 0$ as $n \to \infty$ and $\rho^*\big(\Theta_{1i}, \Theta_{2i}\big|Y^{i-1}\big)$ is the conditional maximal correlation between message points Θ_1 and Θ_2 given the previous channel outputs Y^{i-1}. By standard arguments based on Fano's inequality, we have

$$R \leq \frac{1}{n} \sum_{i=1}^{n} I(X_{1i}, X_{2i}; Y_i|Y^{i-1}) + \epsilon_n \tag{3.105}$$

$$= \frac{1}{n} \sum_{i=1}^{n} I(\tilde{X}_{1i}, \tilde{X}_{2i}; \tilde{Y}_i|Y^{i-1}) + \epsilon_n \tag{3.106}$$

$$\leq \frac{1}{n} \sum_{i=1}^{n} I(\tilde{X}_{1i}, \tilde{X}_{2i}; \tilde{Y}_i) + \epsilon_n \tag{3.107}$$

where

$$\tilde{X}_{ji} := X_{ji} - \mathsf{E}(X_{ji}|Y^{i-1})$$
$$\tilde{Y}_i := \tilde{X}_{1i} + \tilde{X}_{2i} + Z_i$$

and $\epsilon_n \to 0$ as $n \to \infty$.

The equality (3.106) holds since $\mathsf{E}(X_{ji}|Y^{i-1})$ is a function of Y^{i-1}, and the inequality (3.107) follows from the data processing inequality and the fact that Markov chain $\tilde{Y}_i - (\tilde{X}_{1i}, \tilde{X}_{2i}) - Y^{i-1}$ holds.

Notice that by the definition of $\tilde{X}_{ji}$ we have

$$\mathsf{E}(\tilde{X}_{ji}|Y^{i-1}) = 0, \quad i = 1, \ldots, n, \ j = 1, 2. \tag{3.108}$$

Therefore,

$$\begin{aligned}
\mathsf{E}(\tilde{X}_{ji}^2) &= \mathsf{E}\left(\mathsf{E}\left((X_{ji} - \mathsf{E}(X_{ji}|Y^{i-1}))^2 \middle| Y^{i-1}\right)\right) \\
&= \mathsf{E}\left(\mathsf{E}(X_{ji}^2|Y^{i-1}) - \mathsf{E}^2(X_{ji}|Y^{i-1})\right) \\
&\leq \mathsf{E}\left(\mathsf{E}(X_{ji}^2|Y^{i-1})\right) \\
&= \mathsf{E}(X_{ji}^2) \\
&\leq P. \qquad (3.109)
\end{aligned}$$

where the last inequality follows by the assumption of per-symbol power constraints P. Using (3.107), (3.108) and (3.109) we can further upper bound the sum rate R as follows.

$$\begin{aligned}
R &\leq \frac{1}{n}\sum_{i=1}^{n} I(\tilde{X}_{1i}, \tilde{X}_{2i}; \tilde{Y}_i) + \epsilon_n \\
&\leq \frac{1}{2n}\sum_{i=1}^{n} \log\left(1 + 2P + 2P\,\mathsf{E}\left(\rho(\tilde{X}_{1i}, \tilde{X}_{2i})\right)\right) + \epsilon_n \qquad (3.110) \\
&\leq \frac{1}{2n}\sum_{i=1}^{n} \log\left(1 + 2P\left(1 + \rho^*\left(\Theta_{1i}, \Theta_{2i}\middle|Y^{i-1}\right)\right)\right) + \epsilon_n \qquad (3.111)
\end{aligned}$$

where

$$\rho(\tilde{X}_{1i}, \tilde{X}_{2i}) = \mathsf{E}\left(\frac{\tilde{X}_{1i}}{\sqrt{\mathsf{E}(\tilde{X}_{1i}^2)}} \cdot \frac{\tilde{X}_{2i}}{\sqrt{\mathsf{E}(\tilde{X}_{2i}^2)}}\right)$$

is the correlation coefficient between $\tilde{X}_{1i}$ and $\tilde{X}_{2i}$. The inequality (3.110) follows from the maximum entropy theorem [22] and equal per-symbol power constraints $\mathsf{E}(X_{ji}^2) \leq P$. The inequality (3.111) follows from the definition of conditional maximal correlation (3.60), and the fact that $\tilde{X}_{ji}$ is some function of (Θ_j, Y^{i-1}) satisfying the condition (3.108).

Chapter 3, in part, is a reprint of the material in [27]. The dissertation author was the primary investigator and author of this paper.

Chapter 4

Gaussian Broadcast Channel with Feedback

In this chapter, the communication problem over the k-receiver additive white Gaussian noise (AWGN) broadcast channel (BC) with feedback is considered. A linear code for the AWGN-BC with feedback is presented and analyzed using the theory of the linear quadratic Gaussian (LQG) optimal control. The transmitted power required by this code to achieve a given set of rates is determined by the solution to a discrete algebraic Riccati equation (DARE) and the correlation of the noises at the receivers. For the case of independent noises, the symmetric sum rate, where all the receivers have the same rate, is characterized as $1/2\log(1+P\phi)$. Similar to the multiple access channel discussed in Chapter 3, $1 \leq \phi(k,P) \leq k$ captures the improvement due to feedback and for fixed k is increasing in P, that is, more power allows more cooperation among the receivers and the transmitter. For the special case of the two-receiver, the the presented code includes a previous result by Elia and strictly improves upon the Ozarow–Leung code. Next, it is shown that when the noises are correlated, an additional gain in the pre-log factor of the sum rate can be achieved. In particular, for a specific covariance matrix, it is shown that as $P \to \infty$, sum rate $(k/2)\log(1+P)$ is achievable. This generalizes a previous result by Gastpar and Wigger for the two-receiver broadcast channel.

4.1 Introduction

Feedback from the receivers to the sender can improve the performance of the communication over memoryless broadcast channels. Dueck [28] showed that feedback can enlarge the capacity region when the noises at the receivers are correlated. On the other hand, Ozarow and Leung [29] showed that, even when the noises at the receivers are independent, feedback can still improve the performance of the communication by providing a means of cooperation among the receivers and the transmitter.

In this chapter, we study the communication over the k-receiver additive white Gaussian noise (AWGN) broadcast channel (BC) with feedback depicted in Figure 4.1. The sender wishes to communicate independent information to k distinct receivers that observe the transmitted signal corrupted by k, possibly correlated, AWGN noises. The capacity region for this channel is not known even for $k = 2$.

Our contribution is two-fold. First, using the theory of linear quadratic Gaussian (LQG) optimal control, we construct a linear code for the AWGN-BC with feedback, which we refer to as the *LQG code*. The transmitted power required by the LQG code to achieve a given set of rates is determined according to a discrete algebraic Riccati equation (DARE) and depends on the correlation of the noises at the receivers.

For the case of independent noises, we consider the symmetric sum rate $R(P)$, i.e., all the receivers have the same rate $R(P)/k$, achieved by the LQG code under power constraint P. By solving the corresponding DARE, we characterize $R(P)$ as $1/2\log(1 + P\phi)$. Here, $1 \leq \phi(k, P) \leq k$ represents the *power gain* compared to the no feedback sum capacity $1/2\log(1 + P)$. This power gain can be interpreted as the amount of *cooperation* among the receivers established through feedback, which allows the transmitter to align the signals intended for different receivers coherently and use power more efficiently.

Second, we consider the high signal-to-noise ratio (SNR) regime. If the sum rate scales as $(a/2)\log P$ as $P \to \infty$, we refer to the pre-log factor a as *degrees of freedom* (DoF) [30], which captures the number of orthogonal channels that can be

established as the transmit power increases. Degrees of freedom of the AWGN-BC with feedback depends on the correlation among the noises at the receivers. For any noise covariance matrix of rank r, we show that the DoF is upper bounded by $k - r + 1$. Moreover, for any $r \in \{1, \ldots, k\}$, we show that there exists a noise covariance matrix of rank r such that this upper bound on the DoF is achievable by the LQG code. This generalizes a previous result by Gastpar and Wigger [31] for the two-receiver AWGN-BC to the case of k receivers.

The idea of applying tools from optimal control to design communication codes over Gaussian channels with feedback is not new. Elia [32] followed a control-theoretic approach and based on the technique of Youla parameterization presented a linear code for the two-receivers AWGN-BC with independent noises, which outperforms the Ozarow–Leung (OL) code [29]. Our code based on the LQG theory, when specialized to the case of two receivers, provides the same performance as the code in [32]. Wu et al. [19] applied the LQG theory to study Gaussian networks with feedback, where the noises at the receivers are independent, and presented implicit analysis based on Riccati equations. Along the same lines, the Kramer code for the k-sender multiple access channel with feedback, described in Section 3.4, can be obtained by solving an LQG control problem [5].

It is worthwhile to note that the LQG code is derived based on an optimal control for a linear system and hence is optimal among the subclass of linear codes. For the AWGN-BC with feedback, we show that the LQG code provides better performance compared to the OL code for $k = 2$ and hence outperforms the Kramer code [14] for $k \geq 3$, which is an extension of the OL code. However, it is remained to prove whether the LQG code is capacity achieving or not.

The rest of the chapter is organized as follows. Section 4.2 presents the problem definition. Section 4.3 shows how the SK code for the AWGN channel, described in Section 2.3.2, can be derived based on the LQG theory. Section 4.4 presents the LQG code for the AWGN-BC and the analysis for the case of independent noises is provided in Section 4.5. Finally, Section 4.6 presents the degrees of freedom gain when noises are correlated.

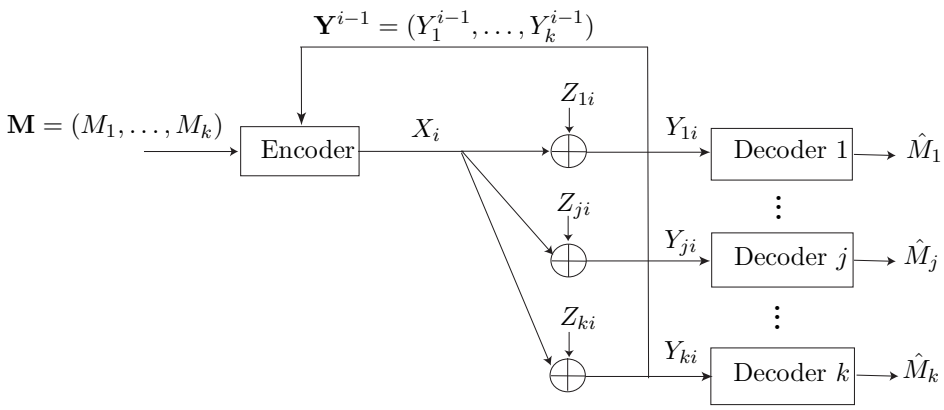


Figure 4.1: The k-receiver Gaussian broadcast channel with feedback

4.2 Problem Setup

Consider the communication problem depicted in Figure 4.1, where a sender wishes to communicate k independent messages $M_1, \ldots, M_k$ to k distinct receivers by n transmissions over an AWGN-BC channel with feedback. At each time $i \in \{1, \ldots, n\}$, the channel outputs are given by

$$Y_{ji} = X_i + Z_{ji}, \quad j = 1, \ldots, k, \tag{4.1}$$

where X_i is the transmitted symbol by the sender, Y_{ji} denotes the received symbol by receiver j, and $Z_{ji} \sim \mathrm{N}(0, 1)$ is the unit variance Gaussian noise at the j-th receiver, which is assumed to be independent of the transmitted messages. The noise vector $\mathbf{Z}_i = (Z_{1i}, \ldots, Z_{ki})$ is drawn independently identically distributed (i.i.d.) from a Gaussian distribution with zero mean and covariance matrix K_z. We assume that the output symbols are causally and noiselessly fed back to the sender such that the transmitted symbol X_i at time i can depend on the messages $\mathbf{M} = (M_1, \ldots, M_k)$ and the previously received channel output sequences $\mathbf{Y}^{i-1} = \{\mathbf{Y}_1, \ldots, \mathbf{Y}_{i-1}\}$, where $\mathbf{Y}_i = (Y_{1i}, \ldots, Y_{ki})^T$ denotes the collection of the k channel outputs at time i.

An n-code for this channel consists of

1. One encoder that assigns a symbol X_i to each $(\mathbf{M}, \mathbf{Y}^{i-1})$, $i = 1, \ldots, n$, and

2. k decoders, where decoder j assigns an estimate $\hat{M}_j$ to each sequence $Y_j^n =$

$(Y_{j1}, \ldots, Y_{jn})$.

For a given n-code, we define the mean square errors $D_1^{(n)}, \ldots, D_k^{(n)}$ at time n as

$$D_j^{(n)} = \mathsf{E}\left((M_j - \hat{M}_j(Y^n))^2\right), \quad j = 1, \ldots, k$$

where the expectation is taken with respect to the distribution of the messages and the channel noises. The probabilities of error $P_{e,1}^{(n)}, \ldots, P_{e,k}^{(n)}$ are defined as

$$P_{e,j}^{(n)} = \mathrm{P}(M_j \neq \hat{M}_j(Y^n))), \quad j = 1, \ldots, k.$$

Definition 4.2.1. *Let $M_1, \ldots, M_k$ be drawn i.i.d. from* $\mathrm{Unif}(0,1)$. *Then, we say that $(E_1, \ldots, E_k)$ is an achievable mean square error (MSE) exponent vector with asymptotic power $\bar{P}$ if there exists a sequence of n-codes such that*

$$E_j = \lim_{n\to\infty} -\frac{1}{2n}\log(D_j^{(n)}), \quad j = 1, \ldots, k$$

and

$$\bar{P} = \limsup_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \mathsf{E}(X_n^2).$$

Definition 4.2.2. *Let $M_1, \ldots, M_k$ be independent random variables and let $M_j \sim$* $\mathrm{Unif}\{1, \ldots, 2^{nR_j}\}$ *for $R_j > 0$. Then, we say that $(R_1, \ldots, R_k)$ is an achievable rate vector under block power constraint P if there exists a sequence of n-codes such that*

$$\lim_{n\to\infty} P_{e,j}^{(n)} = 0, \quad j = 1, \ldots, k$$

and

$$\sum_{i=1}^{n} \mathsf{E}(X_i^2) \leq nP. \tag{4.2}$$

Definition 4.2.3. *The closure of the set of achievable rate vectors $(R_1, \ldots, R_k)$ under block power constraints P is called the capacity region $\mathscr{C}(P, K_z)$. The sum*

capacity $C(P, K_z)$ is defined as

$$C(P, K_z) := \max \left\{ \sum_{j=1}^{k} R_j : (R_1, ..., R_k) \in \mathscr{C}(P, K_z) \right\}.$$

We refer to $R = \sum_{j=1}^{k} R_j$ as the sum rate of an achievable rate vector.

Definition 4.2.4. *The pre-log κ is defined as*

$$\kappa = \limsup_{P \to \infty} \frac{R}{\frac{1}{2}\log(1+P)}.$$

where R is the sum rate achievable under power constraint P.

The definitions of achievable MSE exponent and rate vectors are closely related, as established by the following lemma.

Lemma 4.2.1. *Let $(E_1, \ldots, E_k)$ be an achievable MSE exponent vector with asymptotic power $\bar{P}$, and $(R_1, \ldots, R_k)$ and P be such that*

$$R_j < E_j, \ j = 1, \ldots, k$$

and $P < \bar{P}$. Then, the rate vector $(R_1, \ldots, R_k)$ is achievable under block power constraint P.

Proof. The proof is similar to that of Lemma 2.3.1 considering the power constraint.

4.3 LQG Approach for Gaussian Channel with Feedback

In Section 2.3.3, it was shown that the combination of the system $\{g_i\}_{i=1}^n$ and the control $\{\pi_i\}_{i=1}^n$ for the problem depicted in Figure 2.3 determines an encoder for the feedback communication over an AWGN channel shown in Figure 2.2.

In this section, we consider the linear systems and show that the Schalkwijk–Kailath (SK) code described in Section 2.3.2 can be derived based on the solution

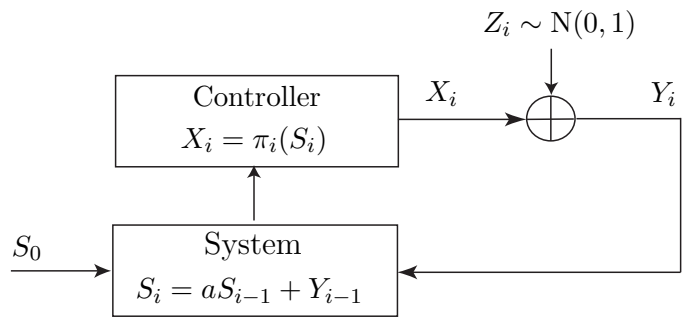


Figure 4.2: Stabilization over the Gaussian channel

to an LQG control problem. This observation was first made by Elia [32]. Let $S_0 \in \mathbb{R}$ be the initial state of an unstable linear system $S_i = aS_{i-1}$ for some $a > 1$, which is stabilized over an AWGN channel (see Figure 4.2). The closed loop system dynamics is then given by

$$S_i = aS_{i-1} + Y_{i-1}, \quad i = 1, 2, \ldots \tag{4.3}$$

where $Y_i = X_i + Z_i$ and

$$X_i = \pi_i(S_i), \quad i = 1, 2, \ldots \tag{4.4}$$

We say that the control $\{\pi_i\}_{i=1}^{\infty}$ is stabilizing if $\limsup_{i\to\infty} \mathsf{E}(S_i^2) < \infty$.

We construct a sequence of n-codes for communicating a message point $\Theta \sim \mathrm{Unif}(0,1)$ over the AWGN channel with feedback according to the system (4.3) with $S_0 = \Theta$ and the control sequence (4.4).

1. Encoder: the encoder transmits $X_i(\Theta, Y^{i-1}) = \pi_i(S_i)$ where

$$S_i = aS_{i-1} + Y_{i-1}, \quad S_1 = \Theta \tag{4.5}$$

2. Decoder: the decoder chooses $\hat{\Theta}_i = -a^{-i} S_i'$ where

$$S_i' = aS_{i-1}' + Y_{i-1}, \quad S_1' = 0 \tag{4.6}$$

Lemma 4.3.1. *For any control* $\{\pi_i\}$ *which stabilizes the unstable system with* $a > 1$*, the code described by* (4.5) *and* (4.6) *achieves the MSE exponent*

$$E = \log a$$

under average power constraint $\limsup_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \mathsf{E}(\pi_i^2(S_i))$.

Proof. Combining (4.5) and (4.6) we have

$$\begin{aligned} S_i &= a^i\Theta + S_i' \\ &= a^i(\Theta - \hat{\Theta}_i) \end{aligned} \tag{4.7}$$

where the last equality follows from the fact that $\hat{\Theta}_i = -a^{-i}S_i'$. From (4.7), the MSE of the estimate $\hat{\Theta}_n$ is $D^{(n)} = \mathsf{E}(\Theta - \hat{\Theta}_n) = a^{-2n}\,\mathsf{E}(S_n^2)$. Since the control is stabilizing we know $\limsup_{n\to\infty} \mathsf{E}(S_n^2) < \infty$ and hence the MSE exponent

$$E = \lim_{n\to\infty} -\frac{1}{2n}\log D^{(n)} = \log a$$

is achievable. □

According to Lemma 4.3.1, any stabilizing control for a given $a > 1$ corresponds to a code which achieves the same MSE exponent $E = \log a$. Next, we find the minimum power required to stabilize the system or equivalently achieve the MSE exponent $E = \log a$. According to the LQG theory the linear stationary control

$$X_i = -cS_i, \quad i = 1, 2, \ldots \tag{4.8}$$

where $c = (a^2 - 1)/a$ attains the minimum average power

$$P^* = a^2 - 1.$$

Hence, according to Lemma 4.3.1, the linear code corresponding to this optimal

LQG control, which we refer to as the LQG code, achieves the MSE exponent

$$\log a = \frac{1}{2}\log(1+P^*)$$

under power constraint P^*. According to Lemma 2.3.1, the LQG code achieves any rate $R < \log a = 1/2\log(1+P^*)$ under power constraint P^* and hence is capacity achieving.

Next, we show that the LQG code corresponds to the SK code. Considering (4.8) we can rewrite (4.5) as

$$X_{i+1} = a(X_i - X_i'(Y_i)) \tag{4.9}$$

$$X_i'(Y_i) = \frac{c}{a}\cdot Y_i \tag{4.10}$$

which becomes equivalent to the recursion in (2.2) if

$$\frac{c}{a} = b = \frac{\mathsf{E}(X_iY_i)}{\mathsf{E}(Y_i^2)}.$$

We show that this equality holds if we consider the asymptotic case where $i \to \infty$. Plugging (4.8) into (4.5) the closed loop is given by

$$S_i = (a-c)S_{i-1} + Z_i.$$

Since $a - c = 1/a < 1$ this recursion converges and it is not hard to see that as $i \to \infty$, $\mathsf{E}(S_i^2) \to a^2/(a^2-1)$ and since $X_i = -cS_i$

$$\mathsf{E}(X_i^2) \to a^2 - 1$$
$$\mathsf{E}(Y_i^2) \to a^2.$$

Therefore,

$$\frac{\mathsf{E}(X_iY_i)}{\mathsf{E}(Y_i^2)} = \frac{\mathsf{E}(X_i^2)}{\mathsf{E}(Y_i^2)} \to \frac{a^2-1}{a^2} = \frac{c}{a}$$

Hence, the LQG code and the SK code are asymptotically equivalent.

4.4 LQG Code for Gaussian Broadcast Channel with Feedback

In this section we extend the LQG approach for the AWGN channel described in Section 4.3 to the k-receiver AWGN-BC by considering the control problem over the AWGN-BC channel depicted in Figure 4.3. In a similar manner as in Section 4.3, we present an n-code for the AWGN-BC with feedback given a general control for an unstable linear system. Considering the stabilizing control with minimum power, which can be derived using the theory of LQG optimal control, we present and analyze the LQG codes for the AWGN-BC.

4.4.1 Code Design Based on a Control Approach

We assume that the channel input and outputs in (4.1) are complex numbers and that the additive noise is drawn i.i.d. from a complex Gaussian distribution with covariance K_z. It is easy to see that if $(R_1, \ldots, R_k)$ is achievable under block power constraint P per each real dimension of the complex channel, then $(R_1, \ldots, R_k)$ is achievable under the same power constraint over the original real channel. In fact, one transmission over the complex channel can be reproduced by two consecutive transmission (of real and imaginary part, respectively) over the real channel.

Let $M_1, \ldots, M_k$ be drawn i.i.d. from a uniform distribution over $(0,1) \times (0,1) \subset \mathbb{C}$,

$$A = \mathrm{diag}(a_1, \ldots, a_k) \in \mathbb{C}^{k \times k}$$
$$B = [1, \ldots, 1]^T \in \mathbb{C}^{k \times 1}$$

where $a_j \in \mathbb{C},\ j = 1 \ldots, k$ are distinct point outside the unit circle, i.e., $|a_j| > 1$. Consider the linear dynamical system

$$\begin{aligned} &\mathbf{S}_0 = \mathbf{M}, \mathbf{Y}_0 = 0 \\ &\mathbf{S}_i = A\mathbf{S}_{i-1} + \mathbf{Y}_{i-1}, \quad i = 1, \ldots, n \end{aligned} \tag{4.11}$$

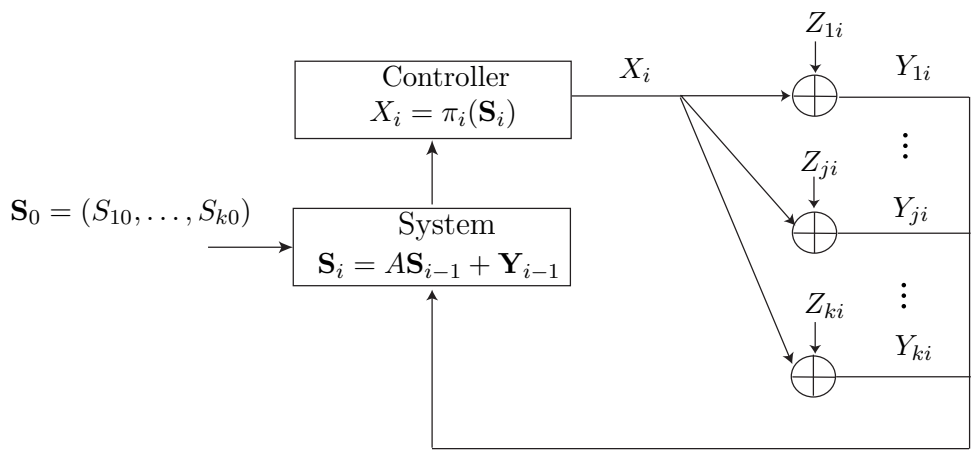


Figure 4.3: Control over the Gaussian broadcast channel

where $\mathbf{S}_i = [S_{1i}, \ldots, S_{ki}]' \in \mathbb{C}^k$ represents the state of the system at time i, $\mathbf{M} = [M_1, \ldots, M_k]'$ is the vector of the messages, and $\mathbf{Y}_i \in \mathbb{C}^k$ denotes the vector of complex channel outputs (4.1), i.e.,

$$\mathbf{Y}_{i-1} = BX_{i-1} + \mathbf{Z}_{i-1}, \quad \mathbf{Z}_{i-1} \sim \mathcal{CN}(0, K_z) \tag{4.12}$$

where $X_i \in \mathbb{C}$ here represents the scalar control signal, and $\mathbf{Z}_{i-1} \in \mathbb{C}^k$ denote the noise vector.

At every discrete time i, the control input can depend only on the state of the system at time i, so

$$X_i = \pi_i(\mathbf{S}_i), \tag{4.13}$$

for some function $\pi_i : \mathbb{C}^k \to \mathbb{C}$. We refer to the sequence $\{\pi_i\}$ as the controller. Since $|a_j| > 1$, the eigenvalues of A are outside the unit circle and the open-loop system (4.11) is unstable. We say that the controller $\{\pi_i\}$ stabilizes the closed-loop system if

$$\limsup_{n\to\infty} \mathsf{E}(|\mathbf{S}_n|^2) < \infty$$

where $|\mathbf{S}_n|^2$ denotes the 2-norm of vector $\mathbf{S}_n$.

Given the system (4.11) and the controller (4.13), we present the following

n-code for the k-receiver AWGN-BC with feedback (4.12).

1. The encoder recursively forms $\mathbf{S}_i$ as in (4.11) and transmits $X_i = \pi_i(\mathbf{S}_i)$ for each $i \in \{1, \ldots, n\}$

2. Decoder j sets
$$\hat{M}_{jn} = -a_j^{-n} S'_{jn},$$
where $\hat{S}_{jn}$ is formed recursively as
$$\begin{aligned} S'_{j0} &= 0, Y_{j0} = 0, \\ S'_{ji} &= AS'_{j(i-1)} + Y_{j(i-1)}, \quad i = 1, \ldots, n, \end{aligned} \tag{4.14}$$
and $Y_{j(i-1)}$ denotes the j-th channel output of the AWGN-BC with feedback at time $i-1$.

The following theorem characterizes the set of MSE exponents vectors that can be achieved by the sequence of n-codes so generated.

Lemma 4.4.1. *Let $\{\pi_i\}$ be a stabilizing control for* (4.11)*. Then, the MSE exponent vector* $(\log|a_1|, \ldots, \log|a_k|)$ *is achievable with asymptotic power*
$$\bar{P} = \limsup_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \mathsf{E}(\pi_i^2(\mathbf{S}_i)). \tag{4.15}$$

Proof. We can rewrite the system dynamics given in (4.11) as
$$\begin{aligned} \mathbf{S}_i &= A\mathbf{S}_{i-1} + \mathbf{Y}_{i-1} \\ &= A^i\mathbf{S}_0 + A\mathbf{S}'_{i-1} + \mathbf{Y}_{i-1} \\ &= A^i\mathbf{S}_0 + \mathbf{S}'_i \end{aligned}$$
where $\mathbf{S}'_i$ is given by
$$\mathbf{S}'_i = A\mathbf{S}'_{i-1} + \mathbf{Y}_{i-1}, \quad \mathbf{S}'_0 = 0, Y_0 = 0$$
Therefore, $\mathbf{S}'_i = \mathbf{S}_i - A^i\mathbf{S}_0 = \mathbf{S}_i - A^i\mathbf{M}$, and $\hat{\mathbf{M}}_n = -A^{-n}\mathbf{S}'_n = \mathbf{M} - A^{-n}\mathbf{S}_n$. Hence,

the error vector $\mathbf{e}_n$ is

$$\mathbf{e}_n := \mathbf{M} - \hat{\mathbf{M}}_n = A^{-n}\mathbf{S}_n.$$

Then we have

$$D_j^{(n)} = \mathsf{E}\left(|\mathbf{e}_n(j)|^2\right) = |a_j|^{-2n}(K_n)_{jj}. \tag{4.16}$$

where $K_n := \mathrm{Cov}(\mathbf{S}_n)$ is the covariance matrix of $\mathbf{S}_n$. By the assumption of stability $\limsup_{n\to\infty}(K_n)_{jj} < \infty$ and achievability of MSE exponent $E_j = \log(|a_j|)$ follows from (4.16) and definition of E_j. □

4.4.2 LQG Code Based on the Optimal LQG Control

According to Lemma 4.4.1, for a given open loop matrix A, any stabilizing controller corresponds to a code which achieves the same MSE exponent vector but with different asymptotic powers. A natural question to ask is what is the minimum asymptotic power required to stabilize the system A or equivalently achieve the MSE exponent vector $(\log|a_1|, \ldots, \log|a_k|)$. The following lemma provides the answer using the theory of the LQG control.

Lemma 4.4.2. *Given a matrix A, there exists a unique controller $\{\pi_i\}$ that stabilizes the closed-loop system* (4.11) *and minimizes the asymptotic average control power*

$$\limsup_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \mathsf{E}(\pi_i^2(\mathbf{S}_i)). \tag{4.17}$$

Such control is stationary and linear, i.e.,

$$X_i = -C\mathbf{S}_i \tag{4.18}$$

where

$$C = (B'GB + 1)^{-1}B'GA \tag{4.19}$$

and G is the unique positive definite solution to the following discrete algebraic Riccati equation (DARE)

$$G = A'GA - A'GB(B'GB + 1)^{-1}B'GA \tag{4.20}$$

and the minimum stationary power is given by

$$\mathrm{tr}(GK_z) \tag{4.21}$$

where K_z is the covariance matrix of the noise vector.

Proof. By plugging (4.12) into (4.11), we have

$$\mathbf{S}_i = A\mathbf{S}_{i-1} + BX_{i-1} + \mathbf{Z}_{i-1}. \tag{4.22}$$

Consider the problem of finding the stabilizing control with minimum average power

$$\frac{1}{n}\sum_{i=1}^{n} \mathsf{E}(\pi_i^2(\mathbf{S}_i)).$$

This is the standard form of the LQG problem of a system with state $\mathbf{S}_i$, disturbance $\mathbf{Z}_i$ and (scalar) control X_i. The optimal controller which minimize the asymptotic average power of the controller then is known [33] to be stationary and linear of the form (4.19). Furthermore, note that we require the controller to stabilize the system in (4.11) (see Lemma 4.4.1), and the stabilizing controller is unique for the following reason. Since the eigenvalues of A are all outside of the unit circle and the elements of B are nonzero we know (A, B) is detectable, that is, there exists a $C \in \mathbb{C}^{1\times k}$ such that $A-BC$ is stable (i.e., every eigenvalue of $A-BC$ lies inside the unit circle). Then, by [25, Lemma 2.4] there exists a unique positive definite solution to (4.20) which stabilizes the closed loop system (4.11). □

Lemma 4.4.2 states that the minimum power required for a control to be stabilizing is given by (4.21) and the optimal control is stationary and linear of the form (4.18). We refer to the linear code for the AWGN-BC with feedback, which is based on the optimal control given in Lemma 4.4.2, as the *LQG code*. The power

of the LQG code to achieve a given rate vector is determined by the solution to the DARE (4.20) and the noise covariance matrix K_z. The following lemma provides the power of a given stabilizing linear controller of the form (4.18). In particular, it provides an alternative representation of the optimal power (4.21).

Lemma 4.4.3. *Let the linear control in* (4.18) *be stabilizing, that is, all eigenvalues of $A - BC$ lies inside the unit circle, then the asymptotic power is given by*

$$CK_sC' \tag{4.23}$$

where K_s is the unique solution to the following discrete algebraic Lyapunov equation (DALE)

$$K_s = (A - BC)K_s(A - BC)' + K_z. \tag{4.24}$$

Remark. From Lemma 4.4.2 and Lemma 4.4.3 it is clear that the performance of the described feedback code depends on the correlation among the noises at the receivers K_z.

Proof. Plugging (4.18) into the closed loop system dynamics (4.22) we have

$$\mathbf{S}_i = (A - BC)\mathbf{S}_i + \mathbf{Z}_i.$$

Let $K_{s,i}$ denote the covariance matrix of the state $\mathbf{S}_i$, then we have the following discrete algebraic Lyapunov recursion

$$K_{s,i+1} = (A - BC)K_{s,i}(A - BC)' + K_z.$$

By assumption $(A - BC)$ is stable and $K_{s,0} \succ 0$, hence the above recursion converges to the unique positive-definite solution to the following discrete algebraic Lyapunov equation (DALE)

$$K_s = (A - BC)K_s(A - BC)' + K_z.$$

Since the control signal is $X_i = -C\mathbf{S}_i$, the stationary power of the controller is $\lim_{n\to\infty} \mathsf{E}(X_n^2) = CK_sC'$. $\square$

Combining Lemma 4.2.1, Lemma 4.4.1, Lemma 4.4.2, and Lemma 4.4.3 we have established the following result.

Theorem 4.4.4. *Let $A = \mathrm{diag}(a_1, \ldots, a_k)$ where $a_j \in \mathbb{C},\ j = 1 \ldots, k$ are distinct points outside the unit circle, i.e., $|a_j| > 1$. Then, the LQG code achieves rate vector $(\log|a_1|, \ldots, \log|a_k|)$ under the block power constraint*

$$P(A, K_z) = CK_sC' = \mathrm{tr}(GK_z) \tag{4.25}$$

where G and K_s are unique positive definite solutions to the DARE (4.20) and the DALE (4.24), respectively.

Example 4.4.1. *Consider the special case of a two-receiver AWGN-BC, and let*

$$A = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix},\ K_z = \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix},$$

for $|a_1| > 1$, $|a_2| > 1$, and $-1 < \rho < 1$. By solving (4.20) and plugging the solution into (4.25) we obtain that $(\log|a_1|, \log|a_2|)$ is an achievable rate pair under power constraint

$$\frac{1}{|a_1 - a_2|^2}\Big(|a_1a_2 - 1|^2(|a_1|^2 + |a_2|^2 - 2) \\ - \rho(|a_1|^2 - 1)(|a_2|^2 - 1)(Re(a_1a_2') - 2)\Big).$$

In the special case where the noises at the receivers are independent ($\rho = 0$), the code in [32] has the same performance as the LQG code. However, to achieve the same rate pair, the Ozarow-Leung code [29] requires more power compared to the LQG code.

4.5 Independent Noises: Power Gain

In this section, we consider the case of independent noises, i.e., $K_z = I_{k\times k}$. For the symmetric case

$$a_j = ae^{\frac{2\pi\sqrt{-1}}{k}(j-1)}, \quad j = 1, \ldots, k. \tag{4.26}$$

where $a > 1$ is real, we characterize the sum rate $R(P)$ achievable by the LQG code under power constraint P.

Theorem 4.5.1. *Given A as in* (4.26)*, the LQG code achieves symmetric sum rate $R(k, P)$, i.e., $R_j = R(k, P)/k, j = 1, \ldots, k$, under power constraint P where*

$$R(k, P) = \frac{1}{2}\log(1 + P\phi)$$

and $\phi(k, P)$ is the unique solution to

$$(1 + P\phi)^{k-1} = \left(1 + \frac{P}{k}\phi(k - \phi)\right)^k.$$

Remark. The quantity $\phi(k, P)$ is the power gain compared to the no feedback sum capacity $1/2\log(1 + P)$. This power gain can be interpreted as the amount of cooperation among the receivers established through feedback, which allows the transmitter to align signals intended for different receivers coherently and use power more efficiently.

Proof. For A defined as (4.26), we know by Theorem 4.4.4 that sum rate $R = k\log a$ is achievable under power constraint $P = \mathrm{tr}(G)$ where G is the unique solution to the DARE (4.20). The following lemma characterizes the solution to the DARE (4.20) for the symmetric choice A.

Lemma 4.5.2. *Suppose that the open-loop matrix A is of the form* (4.26)*. Then the unique positive-definite solution G to (4.20) is circulant with real eigenvalues*

$\lambda_1 > \lambda_2 > \ldots > \lambda_k > 0$ *satisfying*

$$\lambda_i = \frac{1}{a^2}\lambda_{i-1}$$

for $i = 2, \ldots, k$. *The largest eigenvalue* λ_1 *satisfies*

$$1 + k\lambda_1 = a^{2k} \tag{4.27}$$

$$\Big(1 + \lambda_1\big(k - \frac{\lambda_1}{G_{jj}}\big)\Big) = a^{2(k-1)}. \tag{4.28}$$

Proof. See Lemma 3.4.5.

From (4.27) and (4.28) we have

$$(1 + k\lambda_1)^{k-1} = \left(1 + \lambda_1(k - \frac{\lambda_1}{G_{jj}})\right)^k. \tag{4.29}$$

The solution to (4.20) is unique and we conclude that (4.29) has a unique solution for G_{jj} given λ_1 and vice-versa. Consider $\lambda_1(k, P)$ corresponding to the case where

$$G_{jj} = \frac{P}{k}, \quad j = 1, \ldots, k.$$

Note that the solution G to (4.20) is circulant and has equal elements on the diagonal. From (4.27) we know the LQG code corresponding to $\lambda_1(k, P)$ achieves sum rate

$$k \log a = \frac{1}{2}\log(1 + k\lambda_1(k, P)).$$

under power constraint $\mathrm{tr}(G) = P$. The following change of variable

$$\phi := \frac{k}{P}\lambda_1$$

completes the proof. □

4.5.1 Comparison to Gaussian Multiple Access Channel

The LQG approach can be also applied to AWGN-MAC with feedback. It is known [5] that the LQG code for AWGN-MAC has the same performance as the

Kramer code [14], which achieves the linear sum capacity as shown in the previous chapter. Let $R_{\mathrm{MAC}}(k, P)$ denotes the symmetric sum rate achievable by the LQG code for the k-sender AWGN-MAC with feedback where each sender has power constraint P [5, Theorem 4]:

$$R_{\mathrm{MAC}}(k, P) = \frac{1}{2}\log(1 + kP\phi)$$

where $\phi(k, P)$ is the unique solution to

$$(1 + kP\phi)^{k-1} = (1 + P\phi(k - \phi))^{k}.$$

Comparing to Theorem 4.5.1, we have

$$R_{\mathrm{BC}}(k, P) = R_{\mathrm{MAC}}(k, P/k).$$

This shows that under the same *sum power* constraint P, the sum rate achievable by the LQG code over MAC and BC are equal.

4.5.2 Comparison to Ozarow–Leung Code for $k = 2$

We compare the LQG code with the Ozarow-Leung (OL) code [29] for $k = 2$ and $K_z = I$. The OL code can be represented as follows [1]:

$$X_i = S_{1i} + S_{2i}$$

where

$$\begin{bmatrix} S_1 \\ S_2 \end{bmatrix}_{k+1} = \begin{bmatrix} a & 0 \\ 0 & -a \end{bmatrix} \left(\begin{bmatrix} S_1 \\ S_2 \end{bmatrix}_{k} - \begin{bmatrix} \frac{\mathsf{E}[S_1 Y]}{\mathsf{E}[Y^2]} & 0 \\ 0 & \frac{\mathsf{E}[S_2 Y]}{\mathsf{E}[Y^2]} \end{bmatrix} \begin{bmatrix} Y_1 \\ Y_2 \end{bmatrix}_{k} \right) \tag{4.30}$$

In the sequel, we present the LQG code in a similar form as (4.30) for comparison. Let the system in (4.11) be generalized as

$$\mathbf{S}_i = A\mathbf{S}_{i-1} + \mathrm{diag}(\tilde{B})\mathbf{Y}_{i-1}.$$

where

$$A = \begin{bmatrix} a & 0 \\ 0 & -a \end{bmatrix}, \quad \tilde{B} = \begin{bmatrix} -b \\ b \end{bmatrix}. \tag{4.31}$$

As we see below choice of $\tilde{B}$ does not affect the performance of the code as the corresponding controller cancels out the effect of $\tilde{B}$ and without loss of generality we can pick $\tilde{B} = [1\ 1]'$ as in (4.11). According to the channel (4.12) the closed loop system is

$$\mathbf{S}_i = A\mathbf{S}_{i-1} + \tilde{B}X_{i-1} + \mathrm{diag}(\tilde{B})\mathbf{Z}_{i-1}. \tag{4.32}$$

Comparing (4.22) and (4.32), the optimal controller is given by Lemma 4.4.2 by substituting B with $\tilde{B}$. Solving the DARE (4.20) for $\tilde{B}$ we have

$$G = -\frac{(a^4-1)}{4a^4b^2}\begin{bmatrix} 1+a^2 & 1-a^2 \\ 1-a^2 & 1+a^2 \end{bmatrix}.$$

which yields the optimal control

$$C = -\frac{(a^4-1)}{2a^3b}\begin{bmatrix} 1 & 1 \end{bmatrix}.$$

Again comparing (4.22) and (4.32), the optimal power is given by (4.21) by substituting $K_z = I$ with

$$Q = \mathrm{diag}(\tilde{B})\,\mathrm{diag}(\tilde{B})' = \begin{bmatrix} b^2 & 0 \\ 0 & b^2 \end{bmatrix}.$$

and we have

$$P = \mathrm{tr}(GQ) = b^2\,\mathrm{tr}(G) = \frac{1}{2a^2}(a^2-1)(a^2+1)^2. \tag{4.33}$$

Notice that (4.33) does not depend on the parameter b. Thus, we can choose b arbitrarily without affecting the overall performance of the scheme. In particular,

by choosing

$$b = \frac{a^4 - 1}{2a^3}$$

we have that $X_i = S_{1i} + S_{2i}$ as in the OL code. However, the state in OL is updated as (4.30) while in the LQG code

$$\begin{bmatrix} S_1 \\ S_2 \end{bmatrix}_{k+1} = \begin{bmatrix} a & 0 \\ 0 & -a \end{bmatrix} \left(\begin{bmatrix} S_1 \\ S_2 \end{bmatrix}_k - \begin{bmatrix} b/a & 0 \\ 0 & b/a \end{bmatrix} \begin{bmatrix} Y_1 \\ Y_2 \end{bmatrix}_k \right) \tag{4.34}$$

To compare (4.34) and (4.30), note that

$$\frac{\mathsf{E}[S_1 Y]}{\mathsf{E}[Y^2]} = \frac{-C_1(K_s)_{11} - C_2(K_s)_{12}}{\mathrm{tr}(GQ) + 1}$$

where K_s denotes the asymptotic covariance matrix of the state. By substituting K_z with Q in the DALE (4.24) in Lemma 4.4.3, K_s is given by

$$K_s = \frac{b^2}{2a^2} \begin{bmatrix} (a^2+1)^2 + \frac{2}{a^2-1} & a^4 + 1 \\ a^4 + 1 & (a^2+1)^2 + \frac{2}{a^2-1} \end{bmatrix}.$$

and

$$\frac{\mathsf{E}[S_1 Y]}{\mathsf{E}[Y^2]} = \frac{-C_1(K_s)_{11} - C_2(K_s)_{12}}{\mathrm{tr}(GQ) + 1} = b \cdot \frac{a^3(a^2-1)}{a^6 + a^4 + a^2 - 1}.$$

Notice that

$$b \cdot \frac{a^3(a^2-1)}{a^6 + a^4 + a^2 - 1} < \frac{b}{a}$$

so we conclude that the weight given to the channel outputs by the Ozarow and Leung code is strictly smaller than the weight in the LQG code.

4.6 Correlated Noises: Degrees of Freedom Gain

As shown in Theorem 4.4.4, the performance of the LQG code depends on the noise covariance matrix K_z. In this section, we show that when the noises

are correlated we can get pre-log gain in addition to the power gain introduced in Section 4.5. We also refer to pre-log as degrees of freedom as it captures the number of independent channels which can be established as power increases. For the LQG code, let the achievable degrees of freedom (pre-log) be

$$\kappa(K_z) = \limsup_{P\to\infty} \frac{R(P, K_z)}{\frac{1}{2}\log(1+P)}$$

where $R(P, K_z)$ is the achievable sum rate by the LQG code under power constraint P and noise covariance K_z. According to Theorem 4.5.1, when the noises are independent, i.e., $K_z = I_{k\times k}$, the degrees of freedom is one:

$$\kappa(I) = \limsup_{P\to\infty} \frac{\frac{1}{2}\log(1+P\phi)}{\frac{1}{2}\log(1+P)} = 1$$

since $\phi \in [1, k]$. However, we show that the LQG code can achieve degrees of freedom more than one depending on the correlation among noises at the receivers. In particular, there exists K_z such that the LQG code achieves the full degrees of freedom, i.e., $\kappa(K_z) = k$.

Theorem 4.6.1. *For all K_z of rank $r \in \{1, \ldots, k\}$*

$$\kappa(K_z) \leq k - r + 1.$$

Moreover, for any $r \in \{1, \ldots, k\}$, there exists K_z such that $\mathrm{rank}(K_z) = r$ *and*

$$\kappa(K_z) = k - r + 1.$$

Proof. First, we prove the upper bound by induction. By assumption K_z contains r linearly independent rows, let us assume, without loss of generality, the last r rows. Assume that receivers $k-r+1, \cdots, k$ share their received signals and form a single receiver equipped with r receive antennas and let $\mathbf{Y}_{k-r+1} := (Y_{k-r+1}, \ldots, Y_k)^T$ denotes the vector of received signals by this multiple antenna receiver. The cor-

responding Gaussian vector BC with feedback is specified by

$$Y_j = X + Z_j, \qquad j = 1, \cdots, k-r,$$
$$\mathbf{Y}_{k-r+1} = \mathbf{1}_{r\times 1} X + \mathbf{Z}_{k-r+1}$$

where $(Z_1, \cdots, Z_{k-r}, \mathbf{Z_{k-r+1}}) \sim \mathcal{N}(0, K_z)$, $\mathbf{Z_{k-r+1}} \sim \mathcal{N}(0, \tilde{K}_z)$, and by assumption $\tilde{K}_z$ is full rank and invertible. Suppose that the sender of this channel wishes to send message M_j to receiver j, $j = 1, \cdots, k-r+1$, and assume the expected average transmit power constraint

$$\sum_{i=1}^{n} \mathsf{E}[X_i^2(m_1, \cdots, m_{k-r+1}, Y_1^{i-1}, \cdots, Y_{k-r}^{i-1}, \mathbf{Y}_{k-r+1}^{i-1})] \leq nP, \quad m_j \in [1 : 2^{nR_j}].$$

Since we made the optimistic assumption that a subset of receiver can cooperate, the sum capacity of this channel is an outer bound on the sum capacity of the original AWGN-BC. Note that for every $j = 1, \cdots, k-r$ the rate

$$R_j < \frac{1}{2}\log(1+P)$$

is upper bounded by the capacity of a point-to-point Gaussian channel. Since $\tilde{K}$ is invertible, the rate R_{k-r+1} is upper bounded by the capacity of a single input multiple output (SIMO) [30] channel:

$$R_{k-r+1} \leq \frac{1}{2}\log(1 + P|\tilde{K}^{-\frac{1}{2}}\mathbf{1}_{r\times 1}|^2)$$

Thus, the sum capacity of this channel is upper bounded by $(k-r)/2\log(1+P) + 1/2\log(1+P|\tilde{K}^{-\frac{1}{2}}\mathbf{1}_{r\times 1}|^2)$, and there can be at most $k-r+1$ degrees of freedom.

For the direct part, we show $\kappa(K_z) = k$ is achievable by the LQG code for some K_z of rank one, i.e., $r = 1$. For $r = 2, \ldots, k$ similar argument holds. Suppose that the open-loop matrix A is as in (4.26). By Theorem 4.4.4, the symmetric rate vector $(\log a, \ldots, \log a)$ is achievable under block power constraint $\mathrm{tr}(GK_z)$, where G is the circulant matrix in Lemma 4.5.2. Suppose that the covariance matrix K_z

is also circulant, so

$$K_z = \begin{pmatrix} q_1 & q_k & q_{k-1} & \cdots & q_2 \\ q_2 & q_1 & q_k & \cdots & q_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ q_k & q_{k-1} & q_{k-2} & \cdots & q_1 \end{pmatrix},$$

for $q_1 = 1$ and some $-1 \leq q_i \leq 1$, $i = 2, \ldots, k$. Let the first row of G be $\mathbf{g} := [g_1, g_2, \ldots, g_k]$ and first column of K_z be $\mathbf{q} := [q_1, \ldots, q_k]'$. Then, we have

$$\mathrm{tr}(GQ) = k(\mathbf{g} \cdot \mathbf{q}). \tag{4.35}$$

Since G is circulant it can be diagonalized by the discrete Fourier transform (DFT) matrix, i.e,

$$G = F \Lambda F'$$

where F is the k point DFT matrix with

$$F_{jl} = \frac{1}{\sqrt{k}} e^{-2\pi\sqrt{-1}(j-1)(l-1)/k},$$

and $F' = F^{-1}$ is the inverse DFT matrix,

$$F'_{jl} = \frac{1}{\sqrt{k}} e^{2\pi\sqrt{-1}(l-1)(j-1)/k},$$

and $\Lambda = \mathrm{diag}([\lambda_1, \ldots, \lambda_k])$ is a matrix having the eigenvalues of G on its diagonal. Let $\lambda := [\lambda_1, \ldots, \lambda_k]^T$ be the eigenvalues vector. The first row of G can be written in terms of its eigenvalues as follows,

$$\mathbf{g} = \frac{1}{\sqrt{k}} (F'\lambda)^T = \frac{1}{\sqrt{k}} \lambda^T F'$$

where the last equality comes from the fact that $F' = (F')^T$. plugging into (4.35)

we have

$$\mathrm{tr}(GK_z) = \lambda^T(\sqrt{k}F'\mathbf{q}).$$

Let $\mathbf{q}$ be a multiple of the last column of the DFT matrix

$$\mathbf{q} = \sqrt{k}F \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \tag{4.36}$$

such that

$$\sqrt{k}F'\mathbf{q} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ k \end{pmatrix}$$

Then,

$$\mathrm{tr}(GK_z) = \lambda^T(\sqrt{k}F'\mathbf{q}) = k\lambda_k$$

where by Lemma 4.5.2,

$$\lambda_k = \frac{k\lambda_1}{a^{2(k-1)}} = \frac{a^{2k}-1}{a^{2(k-1)}}.$$

Therefore, for the symmetric choice of A in (4.26), the LQG code achieves sum rate $R = k\log a$ under power constraint

$$P = \mathrm{tr}(GK_z) = k \cdot \frac{a^{2k}-1}{a^{2(k-1)}}$$

and we have

$$\begin{aligned} \kappa(K_z) &= \lim_{P\to\infty} \frac{R(P, K_z)}{\frac{1}{2}\log(1+P)} \\ &= \lim_{a\to\infty} \frac{k\log a}{\frac{1}{2}\log\left(k\frac{a^{2k}-1}{a^{2(k-1)}}\right)} \end{aligned}$$

$$= \lim_{a \to \infty} \frac{k \log a}{\frac{1}{2} \log a^2} = k.$$

Hence, the LQG code achieves pre-log k for this covariance matrix K_z.

For rank $r = 2, \ldots, k$, consider K_z such that it contains a $(k-r+1) \times (k-r+1)$ sub-matrix of rank one. We can use a similar argument as above to show that degrees of freedom $k - r + 1$ can be achieved for some K_z. $\square$

Chapter 4, in part, is a reprint of the material in [34]. The dissertation author was the primary investigator and author of this paper.

Chapter 5

Wiretap Channel with Rate-limited Feedback

This chapter studies the benefits of a feedback link of rate R_f for secure communication over the wiretap channel. The *secrecy* capacity is defined as the maximum data rate of reliable communication while the intended message is not revealed to the eavesdropper. An upper bound on the secrecy capacity is presented as a function of the feedback rate R_f. The proof is based on a recursive argument which is used to obtain the single-letter characterization. This upper bound is shown to be tight for the class of physically degraded wiretap channels. A capacity-achieving coding scheme is presented for this case, in which the receiver securely feeds back fresh randomness with rate R_f, generated *independent* of the received channel output symbols. The transmitter then uses this shared randomness as a secret key on top of Wyner's coding scheme for wiretap channels without feedback. Hence, when a feedback link is available, the receiver should allocate all resources to convey a new key rather than sending back information about the channel output.

5.1 Introduction

In his pioneering work [35] that opened up the era of modern cryptography, Shannon modeled a secrecy system as a communication system consisting of a legitimate transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper (Eve), in which Alice wishes to transmit a message M to Bob secret from Eve. If Eve has complete access to what Bob receives, Shannon showed that in order to achieve *perfect secrecy*, a secret key K of entropy $H(K) \geq H(M)$ has to be shared between Alice and Bob. This fundamental yet strongly negative result has been extended—and in a sense overcome—in many directions. In the direction of mathematical communication theory, Wyner [36] introduced the degraded wiretap channel, in which Bob receives the message through a discrete memoryless channel (DMC) $p(y|x)$, and Eve has access to what Bob receives through an additional discrete memoryless channel $p(z|y)$ such that $p(y, z|x) = p(y|x)p(z|y)$, as depicted in Figure 5.1. By relaxing the secrecy requirement mildly while exploiting the better quality of the Alice–Bob channel $p(y|x)$ than that of the Alice–Eve channel $p(z|x)$, Wyner showed that information can be transmitted securely at a positive rate, and characterized the secrecy capacity C_s, the supremum of all achievable rates of secure communication, as

$$C_s = \max_{p(x)} I(X;Y|Z) = \max_{p(x)} (I(X;Y) - I(X;Z)). \tag{5.1}$$

This result was later extended by Csiszár and Körner [37] to general broadcast channels with confidential messages. In particular, they showed that the secrecy capacity of the general (not necessarily degraded) wiretap channel $p(y, z|x)$ is

$$C_s = \max_{p(u,x)} (I(U;Y) - I(U;Z)). \tag{5.2}$$

Furthermore, it was shown that if the channel from Alice to Bob is *more capable* [38] than the channel from Alice to Eve, that is, if $I(X;Y) \geq I(X;Z)$ for all $p(x)$, then

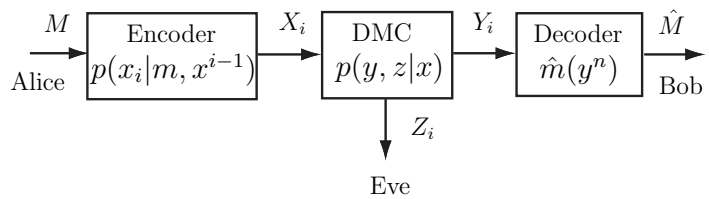


Figure 5.1: The wiretap channel.

the secrecy capacity is simplified to

$$C_s = \max_{p(x)}(I(X;Y) - I(X;Z)). \tag{5.3}$$

All the scenarios described above deal with one-way communication between Alice and Bob. However, many common communication arise over inherently two-way channels, such as telephone systems, digital subscriber lines (DSL), cellular networks, satellite communications, and the Internet. Hence, it is natural to ask how possible interactions between Alice and Bob can increase the secrecy of their communication.

As a canonical model to study this question, in this chapter we extend the wiretap channel model by introducing a secure feedback link of rate R_f from Bob to Alice as depicted in Figure 5.2. The secure feedback link can be viewed as a primitive form of the backward channel from Bob to Alice with secrecy capacity R_f, independent of the forward channel. Thus this model can provide insights into the value of two-way interactions in secure communication.

There are several concrete scenarios in which this model is applicable. For instance, consider the communication between a satellite (Alice) and a base station (Bob) on the ground. The satellite broadcasts its signal to the ground, so any (unintended) station can receive it. On the other hand, the base station can beamform some data back to the satellite securely, which can be used to enhance the secret data rate sent from the satellite to the base station.

The main purpose of this chapter is to investigate the secrecy capacity $C_s(R_f)$ as a function of the secure feedback rate R_f. In Theorem 5.2.1, we show the following upper bound for a general wiretap channel $p(y, z|x)$ with secure rate-

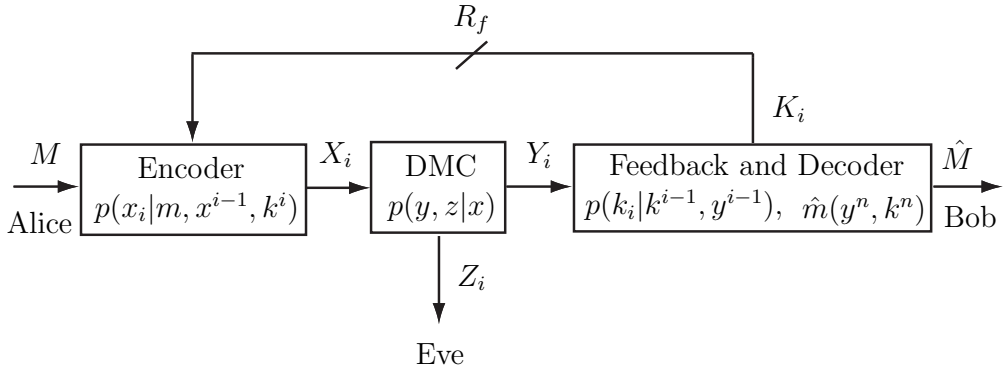


Figure 5.2: The wiretap channel with secure rate-limited feedback.

limited feedback:

$$C_s(R_f) \leq \max_{p(x)} \min\{I(X;Y),\ I(X;Y|Z) + R_f\}. \tag{5.4}$$

Due to the dependencies introduced by the feedback, proving the upper bound (5.4) requires a less standard treatment. We use a *recursive* argument, which helps to track the causal dependencies step by step and to obtain the desired single-letter characterization. Exploiting the recursive structure to find the single-letter characterization might be a powerful tool for similar proofs.

For the case of a physically degraded wiretap channel in which Eve receives a degraded version of what Bob receives, i.e., $p(y, z|x) = p(y|x)p(z|y)$, we show that the upper bound (5.4) is tight, establishing the secrecy capacity as

$$C_s(R_f) = \max_{p(x)} \min\{I(X;Y),\ I(X;Y|Z) + R_f\}. \tag{5.5}$$

Interestingly, we show that in order to achieve the secrecy capacity for the physically degraded wiretap channel Bob can simply ignore what he receives and sends "fresh" randomness. This fresh randomness plays the role of a secret key, which bridges Shannon's original result with Wyner's wiretap model. Accordingly, we use a variation of Wyner's original coding scheme which allows the use of a shared key (sent from Bob to Alice via rate-limited feedback). It should be noted that this modification has been already proposed by Yamamoto [39] and Merhav [40], who characterized the secrecy capacity of wiretap channels with a shared key (which is

already given prior to the communication) and also considered additional effects of having distortion or side information.

In closely related work, Ahlswede and Cai [41] studied wiretap channels with secure *output* feedback, in which the channel output symbols received by Bob are fed back secretly to Alice. They showed that the secrecy capacity of the physically degraded wiretap channel with secure output feedback is

$$\max_{p(x)} \min\{I(X;Y),\ I(X;Y|Z) + H(Y|X,Z)\} \tag{5.6}$$

which is in general larger than the nonfeedback secrecy capacity (5.1). At a first glance, it might seem contradictory that the optimal receiver should ignore the channel outputs completely when feedback is rate-limited (in the current chapter) while the output feedback (in the Ahlswede–Cai setup) boosts the secrecy capacity as in (5.6). A closer look, however, reveals that the Ahlswede–Cai coding scheme essentially extracts fresh randomness in the fed back output symbols hidden from Eve and uses that randomness as a key. Hence, the role of feedback for secure communication is providing shared randomness. Our result shows explicitly that when Bob has a means of interacting with Alice, he should allocate all resources to convey a key rather than sending back the channel output.

Recently, additional studies have been conducted on characterizing the secrecy capacity of various two-way communication systems. Lai, El Gamal, and Poor [42] studied the case of the modulo-additive DMC, where Eve receives the modulo-sum of the source signal, the feedback signal, and the noise. They showed that if Bob jams Eve completely, then Alice can send messages securely at the capacity of the channel to Bob. Tekin and Yener [43] presented an achievable rate region for the two-way Gaussian wiretap channel. Similar to [42], the model presented in [43] assumes that Eve receives the sum of signals from both transmitters corrupted by an additive Gaussian noise. They showed that due to the multiple access nature of Eve's channel, each transmitter can simultaneously help to hide the other user's message from Eve and send some data secretly to the other user. In both studies, the additive nature of Eve's channel gives the opportunity for jamming, in addition to possible backward information transfer. In comparison, our

model decouples the forward and backward communication channels, eliminating the possible use of jamming, and focuses on the "inherent" value of the backward communication link. It also seems that having independent forward and backward communication links fits better the current practice of two-way communications over orthogonal media such as different frequency bands or time slots.

The rest of the chapter is organized as follows. First, we give a formal statement of our result in Section 5.2. Then, we show the upper bound on the secrecy capacity and the coding scheme in Sections 5.3 and 5.4, respectively.

5.2 Problem Setup and the Main Result

We consider the communication problem depicted in Figure 5.2. Here Alice wishes to communicate a message index $M \in [1 : 2^{nR}] := \{1, 2, \ldots, 2^{\lceil nR \rceil}\}$ reliably to the legitimate receiver Bob over a wiretap channel $p(y, z|x)$, while keeping it secret from the eavesdropper Eve, where the channel input $X_i \in \mathcal{X}$ at time i is received as $Y_i \in \mathcal{Y}$ and $Z_i \in \mathcal{Z}$ by Bob and Eve, respectively. To enhance the secrecy of the communication, Bob can send back symbols $K_i \in \mathcal{K}_i$, $i = 1, 2, \ldots, n$, over a feedback link of rate R_f secret from Eve. The feedback symbol K_i at time i can depend causally on previous channel outputs $Y^{i-1} := (Y_1, \ldots, Y_{i-1})$ and previous feedback symbols $K^{i-1} := (K_1, \ldots, K_{i-1})$. We assume that the channel alphabets $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$, and the feedback alphabets $\mathcal{K}_1, ..., \mathcal{K}_n$ are finite, and Eve has complete knowledge about them as well as the coding scheme used by Alice and Bob. The wiretap channel $p(y, z|x)$ is memoryless, i.e.,

$$p(y_i, z_i|x^i, y^{i-1}, z^{i-1}) = p(y_i, z_i|x_i)$$

for $i = 1, 2, ..., n$.

More formally, we define a $(2^{nR}, 2^{nR_f}, n)$ code as

1. feedback alphabets $\mathcal{K}_1, \ldots, \mathcal{K}_n$ such that their cardinalities satisfy

$$\frac{1}{n} \sum_{i=1}^{n} \log(|\mathcal{K}_i|) \leq R_f, \tag{5.7}$$

2. stochastic encoding maps consisting of conditional probability distributions $p(x_i|m, x^{i-1}, k^i)$, $i = 1, 2, \ldots, n$, defined for each $x_i \in \mathcal{X}$, $k^i \in \mathcal{K}^i := \mathcal{K}_1 \times \cdots \times \mathcal{K}_i$, $x^{i-1} \in \mathcal{X}^{i-1}$, and $m \in [1 : 2^{nR}]$ (in other words, $p(x_i|m, x^{i-1}, k^i)$ denotes the probability that the message m, the previous sent symbols x^{i-1} and the previously received feedback symbols k^i are mapped to the channel input x_i at time i),

3. stochastic feedback maps consisting of conditional probability distributions $p(k_i|y^{i-1}, k^{i-1})$ (by convention, $K_1 \sim p(k_1)$ independent of M), and

4. a decoding map $\hat{m} : \mathcal{Y}^n \times \mathcal{K}^n \to [1 : 2^{nR}]$ resulting in the decoded message

$$\hat{M} = \hat{m}(Y^n, K^n). \tag{5.8}$$

We assume throughout that the message M is a random variable uniformly distributed over $[1 : 2^{nR}]$. Given a $(2^{nR}, 2^{nR_f}, n)$ code, we define the probability of error $P_e^{(n)}$ as

$$P_e^{(n)} := \mathsf{P}(\hat{M} \neq M),$$

and the secrecy measure $L^{(n)}$ as

$$L^{(n)} := \frac{1}{n} I(M; Z^n).$$

Definition 5.2.1. *A* secrecy rate R *is achievable if there exists a sequence of* $(2^{nR}, 2^{nR_f}, n)$ *codes such that as* $n \to \infty$,

$$P_e^{(n)} \to 0, \tag{5.9}$$

$$L^{(n)} \to 0. \tag{5.10}$$

Note that $L^{(n)} = R(1 - \Delta^{(n)})$, where

$$\Delta^{(n)} = \frac{H(M|Z^n)}{H(M)} = \frac{H(M|Z^n)}{nR},$$

is the *equivocation* as was defined originally by Wyner, and the condition $L^{(n)} \to 0$

in Definition 5.2.1 is equivalent to the condition $\Delta^{(n)} \to 1$, which was used by Wyner as the requirement for secure communication. The secrecy capacity $C_s(R_f)$ at feedback rate R_f is the supremum of all achievable secrecy rates.

We are now ready to state our main results.

Theorem 5.2.1. *The secrecy capacity $C_s(R_f)$ of the wiretap channel with rate-limited feedback R_f is upper bounded as*

$$C_s(R_f) \leq \max_{p(x)} \min\{I(X;Y),\ I(X;Y|Z) + R_f\}.$$

The proof is given in Section 5.3.

Theorem 5.2.2. *The secrecy capacity of the physically degraded wiretap channel $p(y,z|x) = p(y|x)p(z|y)$ with rate-limited feedback R_f is*

$$C_s(R_f) = \max_{p(x)} \min\{I(X;Y),\ I(X;Y|Z) + R_f\}. \tag{5.11}$$

The converse follows immediately from Theorem 5.2.1. A capacity-achieving coding scheme is presented in Section 5.4, in which Bob sends back pure randomness securely at rate R_f, and Alice uses that shared randomness as a secret key to increase the secrecy rate.

Example 5.2.1. *Consider the degraded wiretap channel shown in Figure 5.3, which is a cascade of two binary symmetric channels, BSC(β_1) and BSC(β_2). By symmetry, the distribution $\mathsf{P}(X=0) = \mathsf{P}(X=1) = 1/2$ achieves the maximization in $C_s(R_f)$, and with this distribution we have*

$$\begin{aligned} I(X;Y) &= 1 - h(\beta_1) \\ I(X;Y|Z) &= I(X;Y) - I(X;Z) = h(\beta_1 * \beta_2) - h(\beta_1), \end{aligned}$$

where $\beta_1 * \beta_2 = \beta_1(1-\beta_2) + (1-\beta_1)\beta_2$ and $h(\beta) := -\beta\log\beta - (1-\beta)\log(1-\beta)$ is the binary entropy function.

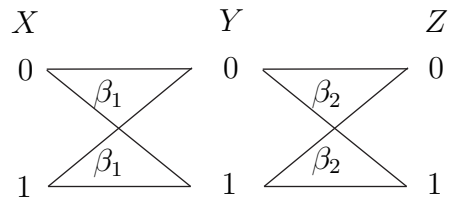


Figure 5.3: The physically degraded binary symmetric wiretap channel.

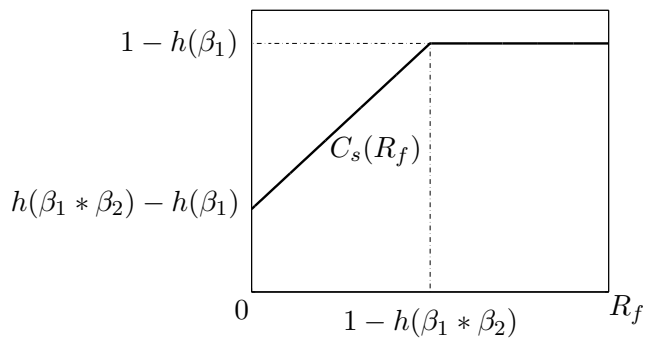


Figure 5.4: Plot of $C_s(R_f)$ for Example 5.2.1.

From Theorem 5.2.2, we have

$$C_s(R_f) = \min\{1 - h(\beta_1),\ h(\beta_1 * \beta_2) - h(\beta_1) + R_f\}.$$

Figure 5.4 shows the plot of $C_s(R_f)$, which starts from $C_s(0) = h(\beta_1 * \beta_2) - h(\beta_1)$ and increases linearly with R_f until it gets saturated at $C = 1 - h(\beta_1)$, for feedback rate $R_f \geq 1 - h(\beta_1 * \beta_2)$.

Example 5.2.2. *In this example we look at the physically degraded Gaussian wiretap channel shown in Figure 5.5. Here E_1 and E_2 are assumed to be independent from each other, i.i.d. over time, and distributed as $E_1 \sim \mathrm{N}(0, N_1)$ and $E_2 \sim \mathrm{N}(0, N_2)$, where $\mathrm{N}(0, N)$ denotes the Gaussian distribution with zero mean and variance N.*

Let P be the input power constraint. Then we know [22]

$$C = \max_{EX^2 \leq P} I(X;Y) = \frac{1}{2}\log\left(1 + \frac{P}{N_1}\right), \tag{5.12}$$

where the maximum is attained by $X \sim \mathrm{N}(0, P)$. For the secrecy capacity without

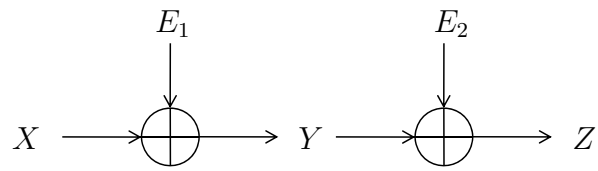


Figure 5.5: The physically degraded Gaussian wiretap channel.

feedback we know [44] that

$$\begin{aligned} C_s(0) &= \max_{EX^2 \leq P} I(X;Y|Z) \\ &= \frac{1}{2}\log\left(1+\frac{P}{N_1}\right) - \frac{1}{2}\log\left(1+\frac{P}{N_1+N_2}\right), \end{aligned} \tag{5.13}$$

where the maximum is attained again with $X \sim \mathrm{N}(0,P)$. *While we will not provide a detailed argument, it is straightforward to show that Theorem 5.2.2 can be modified for additive Gaussian noise channels to give*

$$C_s(R_f) = \max_{EX^2 \leq P} \min\{I(X;Y),\ I(X;Y|Z) + R_f\}. \tag{5.14}$$

Since the maximizations in (5.12) and (5.13) are achieved by the same distribution, it can be verified that the maximization in (5.14) is also achieved by $X \sim \mathrm{N}(0,P)$ *and the secrecy capacity with rate-limited feedback is*

$$C_s(R_f) = \min\{C, C_s(0) + R_f\}. \tag{5.15}$$

Similar to Figure 5.4 in the previous example, $C_s(R_f)$ *starts from*

$$C_s(0) = \frac{1}{2}\log\left(1+\frac{P}{N_1}\right) - \frac{1}{2}\log\left(1+\frac{P}{N_1+N_2}\right)$$

and increases linearly with R_f *until it gets saturated at*

$$C = \frac{1}{2}\log\left(1+\frac{P}{N_1}\right)$$

for feedback rate $R_f \geq 1/2\log(1+P/(N_1+N_2))$.

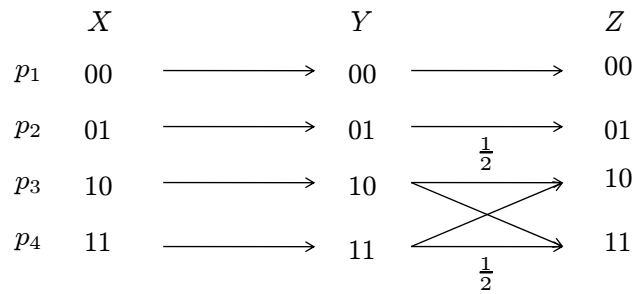


Figure 5.6: An example of a degraded wiretap channel whose secrecy capacity is sublinear in the feedback rate.

As we saw in the previous examples, when the same input distribution maximizes $I(X;Y)$ and $I(X;Y|Z)$, the maximization and the minimization in $C_s(R_f)$ can be exchanged. Therefore,

$$C_s(R_f) = \min\{C,\ C_s(0) + R_f\},$$

and one bit secure feedback is worth one bit in the secrecy capacity until we get saturated by the capacity of the channel between Alice and Bob. However, this is not always true. In fact, $C_s(R_f)$ could be strictly sublinear in R_f; namely,

$$C_s(R_f) < \min\{C,\ C_s(0) + R_f\},$$

as shown in the following example.

Example 5.2.3. *Consider the degraded wiretap channel shown in Figure 5.6. By symmetry, the distribution $p_1 = p_2 = p/2$ and $p_3 = p_4 = (1-p)/2$ achieves the maximization in (5.11). It is easy to verify that with this input distribution we have*

$$I(X;Y) = h(p) + 1 \tag{5.16}$$

$$I(X;Y|Z) = p \tag{5.17}$$

where $h(p) = -p\log p - (1-p)\log(1-p)$ is the binary entropy function.

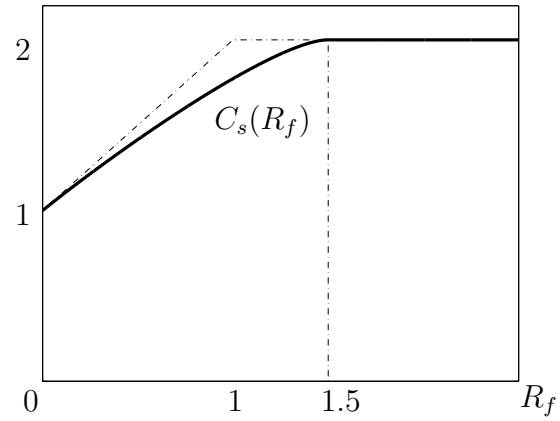


Figure 5.7: Plot of $C_s(R_f)$ for Example 5.2.3.

It follows that

$$C_s(R_f) = \max_p \min\{h(p) + 1,\ p + R_f\}. \tag{5.18}$$

Figure 5.7 shows the plot of $C_s(R_f)$, which increases sublinearly with R_f until it gets saturated at $C = 2$, for feedback rate $R_f \geq 1.5$.

5.3 Proof of the Upper Bound

In this section we show that if the secrecy rate R is achievable, then R must satisfy

$$R \leq \max_{p(x)} \min\{I(X;Y),\ I(X;Y|Z) + R_f\}. \tag{5.19}$$

To show (5.19) we prove the following two upper bounds for any achievable secrecy rate R.

$$R \leq \frac{1}{n}\sum_{i=1}^{n} I(X_i;Y_i) + \epsilon_n \tag{5.20}$$

$$R \leq R_f + \frac{1}{n}\sum_{i=1}^{n} I(X_i;Y_i|Z_i) + \delta_n, \tag{5.21}$$

where $\epsilon_n, \delta_n \to 0$ as $n \to \infty$. Then we use the usual technique of introducing a time sharing random variable [22], and concavity of mutual information in $p(x)$ to obtain (5.19).

First, (5.20) follows easily from Fano's inequality as in the standard converse proof of the channel coding theorem [22, Theorem 7.7.1].

We now prove (5.21) using Fano's inequality, the secrecy constraint (5.10), and the feedback rate-limit constraint (5.7). A recursive argument (Lemma 5.3.1) is then used to obtain the single-letter characterization.

By Fano's inequality, we have

$$H(M|\hat{M}) \leq 1 + P_e^{(n)} nR =: n\epsilon_n.$$

By the assumption that $P_e^{(n)} \to 0$, we have $\epsilon_n \to 0$ as $n \to \infty$. From (5.8) and the data processing inequality, we have

$$H(M|K^n, Y^n) \leq H(M|\hat{M}) \leq n\epsilon_n.$$

By the assumption that $L^{(n)} \to 0$, we have

$$I(M; Z^n) = n\gamma_n, \tag{5.22}$$

where $\gamma_n \to 0$ as $n \to \infty$. It then follows that

$$\begin{aligned}
nR &= H(M) \\
&= H(M|Z^n) + I(M; Z^n) \\
&= H(M|Z^n) + n\gamma_n && (5.23) \\
&= I(M; Y^n, K^n|Z^n) + H(M|Y^n, Z^n, K^n) + n\gamma_n \\
&\leq I(M; Y^n, K^n|Z^n) + n\epsilon_n + n\gamma_n && (5.24) \\
&= I(M; K^n|Z^n) + I(M; Y^n|K^n, Z^n) + n\delta_n && (5.25) \\
&\leq H(K^n|Z^n) + I(M, X^n; Y^n|K^n, Z^n) + n\delta_n, && (5.26)
\end{aligned}$$

where (5.23) follows from (5.22), (5.24) follows from Fano's inequality, and (5.25)

follows by defining $\delta_n = \epsilon_n + \gamma_n$.

The following lemma provides a recursive expression, which is crucial to single-letterize (5.26).

Lemma 5.3.1. *For each $j = 1, 2, \ldots, n$, we have*

$$\begin{aligned}
&H(K^j|Z^j) + I(M, X^j; Y^j|K^j, Z^j) \\
&\quad \le H(K^{j-1}|Z^{j-1}) + I(M, X^{j-1}; Y^{j-1}|K^{j-1}, Z^{j-1}) \\
&\qquad + H(K_j|M, X^{j-1}, K^{j-1}, Z^{j-1}) + I(X_j; Y_j|Z_j).
\end{aligned}$$

Proof. We have the following chain of inequalities:

$$\begin{aligned}
&H(K^j|Z^j) + I(M, X^j; Y^j|K^j, Z^j) \\
&\quad = H(K^j|Z^j) + I(M, X^j; Y^{j-1}|K^j, Z^j) + I(M, X^j; Y_j|Y^{j-1}, K^j, Z^j) \\
&\quad \le H(K^j|Z^j) + I(M, X^j; Y^{j-1}|K^j, Z^j) + I(M, Y^{j-1}, K^j, Z^{j-1}, X^j; Y_j|Z_j) \\
&\quad = H(K^j|Z^j) + I(M, X^j; Y^{j-1}|K^j, Z^j) + I(X_j; Y_j|Z_j) \qquad (5.27) \\
&\quad \le H(K^j|Z^j) + I(M, X^j, Z_j; Y^{j-1}|K^j, Z^{j-1}) + I(X_j; Y_j|Z_j) \\
&\quad = H(K^j|Z^j) + I(M, X^j; Y^{j-1}|K^j, Z^{j-1}) + I(X_j; Y_j|Z_j) \qquad (5.28) \\
&\quad = H(K^j|Z^j) + I(M, X^{j-1}; Y^{j-1}|K^j, Z^{j-1}) \\
&\qquad\qquad + I(X_j; Y^{j-1}|M, X^{j-1}, K^j, Z^{j-1}) + I(X_j; Y_j|Z_j) \\
&\quad = H(K^j|Z^j) + I(M, X^{j-1}; Y^{j-1}|K^j, Z^{j-1}) + I(X_j; Y_j|Z_j) \qquad (5.29) \\
&\quad = H(K^j|Z^j) + I(M, X^{j-1}, K_j; Y^{j-1}|K^{j-1}, Z^{j-1}) \\
&\qquad\qquad - I(K_j; Y^{j-1}|K^{j-1}, Z^{j-1}) + I(X_j; Y_j|Z_j) \\
&\quad = H(K^j|Z^j) + I(M, X^{j-1}; Y^{j-1}|K^{j-1}, Z^{j-1}) \\
&\qquad + I(K_j; Y^{j-1}|M, X^{j-1}, K^{j-1}, Z^{j-1}) - I(K_j; Y^{j-1}|K^{j-1}, Z^{j-1}) + I(X_j; Y_j|Z_j) \\
&\quad = H(K^{j-1}|Z^j) + H(K_j|K^{j-1}, Z^j) + I(M, X^{j-1}; Y^{j-1}|K^{j-1}, Z^{j-1}) \\
&\qquad\qquad + I(K_j; Y^{j-1}|M, X^{j-1}, K^{j-1}, Z^{j-1}) + H(K_j|Y^{j-1}, K^{j-1}, Z^{j-1}) \\
&\qquad\qquad - H(K_j|K^{j-1}, Z^{j-1}) + I(X_j; Y_j|Z_j) \\
&\quad \le H(K^{j-1}|Z^j) + I(M, X^{j-1}; Y^{j-1}|K^{j-1}, Z^{j-1})
\end{aligned}$$

$$+ I(K_j; Y^{j-1}|M, X^{j-1}, K^{j-1}, Z^{j-1}) + H(K_j|Y^{j-1}, K^{j-1}, Z^{j-1}) + I(X_j; Y_j|Z_j) \tag{5.30}$$

$$\begin{aligned}
&= H(K^{j-1}|Z^j) + I(M, X^{j-1}; Y^{j-1}|K^{j-1}, Z^{j-1}) \\
&\qquad + H(K_j|M, X^{j-1}, K^{j-1}, Z^{j-1}) - H(K_j|Y^{j-1}, M, X^{j-1}, K^{j-1}, Z^{j-1}) \\
&\qquad + H(K_j|Y^{j-1}, K^{j-1}, Z^{j-1}) + I(X_j; Y_j|Z_j) \\
&= H(K^{j-1}|Z^j) + I(M, X^{j-1}; Y^{j-1}|K^{j-1}, Z^{j-1}) \\
&\qquad + H(K_j|M, X^{j-1}, K^{j-1}, Z^{j-1}) + I(X_j; Y_j|Z_j) \qquad (5.31) \\
&\leq H(K^{j-1}|Z^{j-1}) + I(M, X^{j-1}; Y^{j-1}|K^{j-1}, Z^{j-1}) \\
&\qquad + H(K_j|M, X^{j-1}, K^{j-1}, Z^{j-1}) + I(X_j; Y_j|Z_j), \qquad (5.32)
\end{aligned}$$

where

- (5.27) holds because the channel is memoryless and therefore $Y_j \to (X_j, Z_j) \to (M, X^{j-1}, K^j, Y^{j-1}, Z^{j-1})$ form a Markov chain,
- (5.28) holds because $Z_j \to (M, X^j, K^j, Z^{j-1}) \to Y^{j-1}$ form a Markov chain,
- (5.29) holds because $Y^{j-1} \to (M, X^{j-1}, K^j, Z^{j-1}) \to X_j$ form a Markov chain,
- (5.30) and (5.32) follow from $H(K_j|K^{j-1}, Z^j) \leq H(K_j|K^{j-1}, Z^{j-1})$ and $H(K_j|Z^j) \leq H(K_j|Z^{j-1})$ respectively, and
- (5.31) holds because of the following Markov chain $(M, X^{j-1}, Z^{j-1}) \to (Y^{j-1}, K^{j-1}) \to K_j$,

which completes the proof. □

Starting from (5.26), we apply Lemma 5.3.1 recursively to find the single-letter characterization as follows:

$$\begin{aligned}
nR &\leq H(K^n|Z^n) + I(M, X^n; Y^n|K^n, Z^n) + n\delta_n \\
&\leq H(K^{n-1}|Z^{n-1}) + I(M, X^{n-1}; Y^{n-1}|K^{n-1}, Z^{n-1}) \\
&\qquad + I(X_n; Y_n|Z_n) + H(K_n) + n\delta_n
\end{aligned}$$

$$
\begin{aligned}
&\leq H(K^{n-2}|Z^{n-2}) + I(M, X^{n-2}; Y^{n-2}|K^{n-2}, Z^{n-2}) \\
&\quad + I(X_{n-1}; Y_{n-1}|Z_{n-1}) + H(K_{n-1}) \\
&\quad + I(X_n; Y_n|Z_n) + H(K_n) + n\delta_n \\
&\quad \vdots \\
&\leq \sum_{i=1}^{n} I(X_i; Y_i|Z_i) + \sum_{i=1}^{n} H(K_i) + n\delta_n. \qquad (5.33)
\end{aligned}
$$

Dividing (5.33) by n and applying the feedback rate-limit constraint (5.7) we obtain (5.21) as follows:

$$
\begin{aligned}
R &\leq \frac{1}{n}\sum_{i=1}^{n} I(X_i; Y_i|Z_i) + \frac{1}{n}\sum_{i=1}^{n} H(K_i) + \delta_n \\
&\leq \frac{1}{n}\sum_{i=1}^{n} I(X_i; Y_i|Z_i) + R_f + \delta_n.
\end{aligned}
$$

To complete the proof, let Q be a time-sharing random variable distributed uniformly over $\{1, 2, ..., n\}$ and independent of X^n, Y^n, Z^n. Then (5.21) can be written as

$$
\begin{aligned}
R &\leq R_f + \frac{1}{n}\sum_{i=1}^{n} I(X_i; Y_i|Z_i) + \delta_n \\
&= R_f + \frac{1}{n}\sum_{i=1}^{n} I(X_i; Y_i|Z_i, Q = i) + \delta_n \\
&= R_f + I(X_Q; Y_Q|Z_Q, Q) + \delta_n \\
&= R_f + I(X; Y|Z, Q) + \delta_n,
\end{aligned}
$$

where $X := X_Q$, $Y := Y_Q$, $Z := Z_Q$. Now letting $n \to \infty$, $\delta_n \to 0$ and hence

$$
R \leq R_f + I(X; Y|Z, Q). \qquad (5.34)
$$

Similarly, (5.20) can be written as

$$
R \leq I(X; Y|Q) + \epsilon_n,
$$

where as $n \to \infty$, $\epsilon_n \to 0$ and we have

$$R \leq I(X;Y|Q). \tag{5.35}$$

Note that $\mathsf{P}(Y_Q = y, Z_Q = z|X_Q = x)$ is consistent with the given wiretap channel $p(y,z|x)$ and is independent of Q. Since $Q \to X \to Y \to Z$ form a Markov chain, it follows from (5.34),

$$\begin{aligned} R &\leq R_f + I(X;Y|Z,Q) \\ &\leq R_f + I(X,Q;Y|Z) \\ &= R_f + I(X;Y|Z). \end{aligned} \tag{5.36}$$

Similarly from (5.35),

$$R \leq I(X;Y|Q) \leq I(X,Q;Y) = I(X;Y). \tag{5.37}$$

Combining (5.36) and (5.37), we have

$$R \leq \min[I(X;Y), I(X;Y|Z) + R_f]$$

for some (X,Y,Z) consistent with the given channel $p(y,z|x)$. Therefore, we conclude that

$$R \leq \max_{p(x)} \min[I(X;Y),\ I(X;Y|Z) + R_f],$$

which completes the proof of Theorem 5.2.1.

5.4 A Capacity Achieving Code for Degraded Channels

In this section, for the sake of completeness, we present a coding scheme for the degraded wiretap channel with rate-limited feedback that achieves any secrecy

rate R satisfying

$$R < \max_{p(x)} \min\ [I(X;Y),\ I(X;Y|Z) + R_f]. \tag{5.38}$$

The coding scheme is based on a variation of Wyner's original scheme which allows the use of a shared key, and originally was proposed by Yamamoto [39]. Ahlswede and Cai [41] use a similar idea to enhance the secrecy rate after generating secret common randomness through feedback.

We assume Bob uses the feedback link only to send back a secret key of rate R_f at the first instance; i.e., send K_1 with $|\mathcal{K}_1| = 2^{nR_f}$, so that Alice and Bob have a shared key prior to their communication as shown in Figure 5.8. In the remainder, we will provide a coding scheme for the wiretap channel with shared key of rate R_f that achieves any secrecy rate R satisfying (5.38).

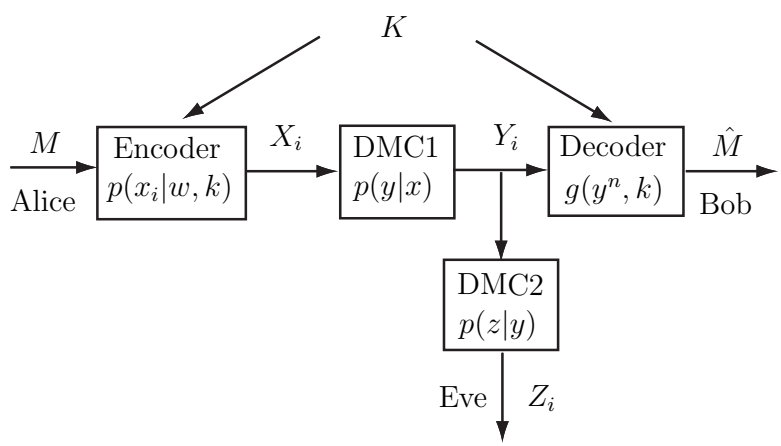


Figure 5.8: The degraded wiretap channel with shared key.

Fix any distribution $p(x)$ and define

$$R' = I(X;Y|Z) = I(X;Y) - I(X;Z), \tag{5.39}$$

and

$$R'_f = R - R'. \tag{5.40}$$

Let $M = (M_1, M_2)$, where M_1 and M_2 are independent random variables uniformly

distributed over $[1 : 2^{nR'}]$ and $[1 : 2^{nR'_f}]$, respectively. As shown below, the message M_1 will be transmitted securely using Wyner's original coding scheme while the security of M_2 will be guaranteed by using a key of rate R'_f. Note that from (5.38), (5.39) and (5.40) we have

$$R'_f < \min[I(X;Z),\ R_f].$$

The codebook is a collection of codewords $X^n \in \mathcal{X}^n$, from which the specific codeword $X^n(M_1, M_2, K)$ is picked randomly so as to confuse the eavesdropper. Therefore, there is no pre-defined codeword for a specific message.

Codebook generation. Pick $R_{\mathcal{C}} \geq R$, such that $R_{\mathcal{C}} = I(X;Y) - \epsilon$ for some $\epsilon > 0$. Such $(R_{\mathcal{C}}, \epsilon)$ always exists since $R < I(X;Y)$. Generate a random codebook $\mathcal{C}$ containing i.i.d. random codewords $X^n(\ell) \in \mathcal{X}^n$, $\ell \in [1 : 2^{nR_{\mathcal{C}}}]$, each drawn according to $\mathsf{P}(X^n = x^n) = \prod_{i=1}^n p(x_i)$. Divide the codebook into $2^{nR'}$ disjoint *sub-codebooks*, each of which has $2^{n(R_{\mathcal{C}} - R')}$ codewords. Label the sub-codebooks $\mathcal{C}_1, ..., \mathcal{C}_{2^{nR'}}$. Now, divide each sub-codebook $\mathcal{C}_i$ into $T = 2^{n(R_{\mathcal{C}} - R' - R'_f)}$ *sections* $\mathcal{C}_{i1}, ..., \mathcal{C}_{iT}$, each of which has $2^{nR'_f}$ codewords. Enumerate the codewords in each section from 1 to $2^{nR'_f}$, so the codewords in the j-th section of the i-th sub-codebook can be called as $X^n_{\mathcal{C}_{ij}}(1), \ldots, X^n_{\mathcal{C}_{ij}}(2^{nR'_f})$ (see Figure 5.9).

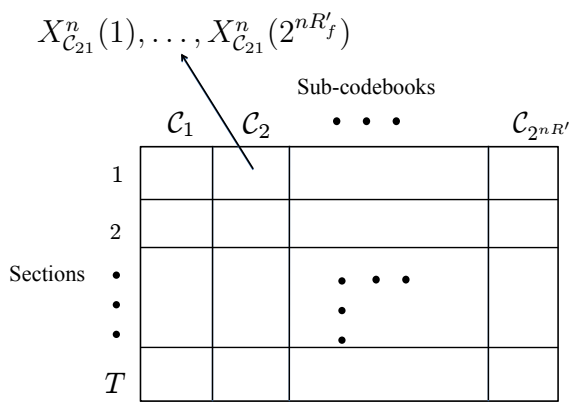


Figure 5.9: Structure of the codebook.

Feedback. Let K be uniform over $[1 : 2^{nR'_f}]$. Bob sends $K_1 = K$ at time 1.

Encoding. We use K as a key shared between Alice and Bob. Generate a

new variable $M_2' = M_2 \oplus K \in [1 : 2^{nR_f'}]$, where $\oplus$ is the modulo addition over the set $[1 : 2^{nR_f'}]$. Note that K and M_2 are uniformly distributed and independent, so M_2' is uniformly distributed and independent of both K and M_2.

We pick $X^n(M_1, M_2, K)$ as follows. According to M_1 we pick the corresponding sub-codebook among $2^{nR'}$ ones. In that sub-codebook we pick one of the sections uniformly at random and in that section we pick the corresponding codeword among the $2^{nR_f'}$ codewords according to M_2'. We denote by $J \in [1 : 2^{n(R_{\mathcal{C}} - R')}]$ the index of the picked codeword in the sub-codebook corresponding to M_1.

Decoding. Decoder looks for a unique index $\hat{\ell} \in [1 : 2^{nR_{\mathcal{C}}}]$ such that $(X^n(\hat{\ell}), Y^n) \in A_\epsilon^{(n)}$, where $A_\epsilon^{(n)}$ is the set of jointly typical (X^n, Y^n) sequences. If no such $\hat{\ell}$ exists or if there is more than one such, an error is declared. Having found $\hat{\ell}$, the decoder finds the reconstructed message $(\hat{M}_1, \hat{M}_2)$ as follows. It chooses $\hat{M}_1$ as the index of the sub-codebook $X^n(\hat{\ell})$ belongs to. For $\hat{M}_2$, the decoder first finds $\hat{M}_2'$, the index of $X^n(\hat{\ell})$ in the section it belongs to, and then it finds $\hat{M}_2 = \hat{M}_2' \ominus K$, where $\ominus$ is the modulo subtraction over $[1 : 2^{nR_f'}]$.

Analysis of the error probability and the secrecy. We show that there exists a codebook in the random collection of codebooks for which (5.9) and (5.10) are simultaneously satisfied; i.e., $P_e^{(n)} \to 0$ and $L^{(n)} = \frac{1}{n} I(M; Z^n) \to 0$.

Let $P_e^{(n)}(\mathcal{C}_0)$ and $L^{(n)}(\mathcal{C}_0)$ be the probability of error and the secrecy measure corresponding to a specific codebook $\mathcal{C}_0$. Since $R_{\mathcal{C}} < I(X; Y)$, by channel coding theorem [22, Theorem 7.7.1] we have

$$\mathsf{E}_{\mathcal{C}}[P_e^{(n)}(\mathcal{C})] \to 0 \quad \text{as} \quad n \to \infty, \tag{5.41}$$

where the expectation is over all random codebooks. As shown below,

$$\mathsf{E}_{\mathcal{C}}[L^{(n)}(\mathcal{C})] \to 0 \quad \text{as} \quad n \to \infty. \tag{5.42}$$

Combining (5.41) and (5.42), we have

$$\mathsf{E}_{\mathcal{C}}[P_e^{(n)}(\mathcal{C}) + L^{(n)}(\mathcal{C})] \to 0 \quad \text{as} \quad n \to \infty. \tag{5.43}$$

Therefore, there exists at least one codebook for which conditions (5.9) and (5.10) are simultaneously satisfied.

Now, it remains to show that (5.42) holds. Let

$$L_1^{(n)}(\mathcal{C}_0) = \frac{1}{n} I(M_1; Z^n | \mathcal{C} = \mathcal{C}_0)$$
$$L^{(n)}(\mathcal{C}_0) = \frac{1}{n} I(M_1, M_2; Z^n | \mathcal{C} = \mathcal{C}_0).$$

For the rest of the chapter all expectations are with respect to $\mathcal{C}$, so we omit the subscript $\mathcal{C}$. From the definition of the conditional mutual information we have

$$\mathsf{E}[L_1^{(n)}(\mathcal{C})] = \frac{1}{n} I(M_1; Z^n | \mathcal{C})$$
$$\mathsf{E}[L^{(n)}(\mathcal{C})] = \frac{1}{n} I(M_1, M_2; Z^n | \mathcal{C}). \tag{5.44}$$

With these definitions we have the following lemma.

Lemma 5.4.1. *Suppose* $\mathsf{E}[L_1^{(n)}(\mathcal{C})] \to 0$ *as* $n \to \infty$. *Then* $\mathsf{E}[L^{(n)}(\mathcal{C}))] \to 0$ *as* $n \to \infty$.

Proof. Consider

$$\begin{aligned}
&\mathsf{E}[L^{(n)}(\mathcal{C})] \\
&= \frac{1}{n} I(M_1, M_2; Z^n | \mathcal{C}) \\
&= \frac{1}{n} [I(M_1; Z^n | \mathcal{C}) + I(M_2; Z^n | \mathcal{C}, M_1)] \\
&= \frac{1}{n} [I(M_1; Z^n | \mathcal{C})] \qquad (5.45) \\
&= \mathsf{E}[L_1^{(n)}(\mathcal{C})],
\end{aligned}$$

where (5.45) follows from the fact that M_2 is independent of (M_1, Z^n) for any choice of $\mathcal{C}$. This follows since M_2 is independent of M_2' due to the independent and uniformly distributed key K, and $M_2 \to M_2' \to (M_1, Z^n)$ form a Markov chain. □

To complete the analysis, we show that $\mathsf{E}[L_1^{(n)}(\mathcal{C})] \to 0$ as $n \to \infty$. Recall J

is a random variable over $[1 : 2^{n(R_{\mathcal{C}}-R')}]$ that denotes the index of the picked codeword X^n in the sub-codebook $\mathcal{C}_{M_1}$. Based on the encoding scheme, J is uniformly distributed and independent of $(M_1, \mathcal{C})$. Then it follows that

$$
\begin{aligned}
&\mathsf{E}[L_1^{(n)}(\mathcal{C})] \\
&= \frac{1}{n}[I(M_1; Z^n|\mathcal{C})] \\
&= \frac{1}{n}[I(M_1, J; Z^n|\mathcal{C}) - I(J; Z^n|M_1, \mathcal{C})] \\
&\leq \frac{1}{n}[I(X^n; Z^n|\mathcal{C}) - I(J; Z^n|M_1, \mathcal{C})] && (5.46) \\
&= \frac{1}{n}[I(X^n; Z^n|\mathcal{C}) - H(J|M_1, \mathcal{C}) + H(J|Z^n, M_1, \mathcal{C})] \\
&= \frac{1}{n}[I(X^n; Z^n|\mathcal{C}) - n(I(X; Z) - \epsilon) + H(J|Z^n, M_1, \mathcal{C})] && (5.47) \\
&\leq \frac{1}{n}[I(X^n; Z^n|\mathcal{C}) - n(I(X; Z) - \epsilon) + n\epsilon_n] && (5.48) \\
&\leq \frac{1}{n}[I(X^n; Z^n) - nI(X; Z) + n\epsilon + n\epsilon_n] && (5.49) \\
&= \frac{1}{n}[nI(X; Z) - nI(X; Z) + n\epsilon + n\epsilon_n], && (5.50)
\end{aligned}
$$

which tends to zero as $n \to \infty$ and $\epsilon \to 0$. Here

- inequality (5.46) follows from the fact that $(M_1, J) \to X^n \to Z^n$ form a Markov chain,
- equality (5.47) follows since J is uniformly distributed over $[1 : 2^{n(R_{\mathcal{C}}-R')}] = [1 : 2^{n(I(X;Z)-\epsilon)}]$ and is independent of $(M_1, \mathcal{C})$,
- inequality (5.48) follows from Fano's inequality and the fact that $\mathsf{E}[\tilde{P}_e(\mathcal{C})] \to 0$ as $n \to \infty$, where

$$\tilde{P}_e(\mathcal{C}_0) = \min_{\tilde{X}^n} \mathsf{P}(\tilde{X}^n(Z^n) \neq X^n|\mathcal{C} = \mathcal{C}_0),$$

  where the minimization is taken over all functions $\tilde{X}^n : Z^n \to \mathcal{X}^n$. This can be easily seen if one consider the sub-codebook $\mathcal{C}_{M_1}$ with $2^{n(I(X;Z)-\epsilon)}$ elements as a code for Eve's channel given M_1 is sent, and apply the channel coding

theorem [22, Theorem 7.7.1]. Here, we have used the notation ϵ_n to show a sequence such that $\epsilon_n \to 0$ as $n \to \infty$,

- inequality (5.49) comes from the fact that $\mathcal{C} \to X^n \to Z^n$ form a Markov chain, and

- equality (5.50) comes from the fact that X_i's are i.i.d and the channel is memoryless, therefore, $I(X^n; Z^n) = nI(X; Z)$.

To summarize, we showed that $\mathsf{E}[L_1^{(n)}(\mathcal{C})] \to 0$ as $n \to \infty$, and hence by Lemma 5.4.1, condition (5.42) holds. Putting (5.41) and (5.42) together, we can conclude that there exists at least one codebook which satisfies conditions (5.9) and (5.10) simultaneously. This completes the proof.

Remark. This coding scheme can be easily modified to the case in which the feedback channel has a time-invariant rate constraint $\log(|\mathcal{K}_i|) < R_f$ for all i. By using block Markov coding, we can send the key in the L-th block that will be used in the $(L+1)$-th block.

Chapter 5, in part, is a reprint of the material in [45]. The dissertation author was the primary investigator and author of this paper.

Chapter 6

Binary Multiplying Channel

The feedback communication settings discussed in the previous chapters are special cases of interactive communication systems where each user is assumed to be either a sender (with some messages) or a receiver (without any message). Two-way channels generalize point-to-point channels with feedback discussed in Chapter 2, by letting each user be both a sender and a receiver, and model the communication scenario where two users wish to exchange their messages interactively over some channel. This chapter studies the *binary multiplying channel* (BMC), a simple two-way channel introduced by Shannon and Blackwell, for which the characterization of the capacity region is still open. In such a two-way channel, each user can help the other user at the price of communicating less information and the problem is characterization of the optimal trade-off between these two competing roles. This two-way communication problem is formulated as a decentralized control problem, and using dynamic programming, an optimality condition for the codes over this channel is provided. Moreover, a code for the BMC presented by Schalkwijk is analyzed based on the *Massey directed information*, a natural extension of the mutual information which captures causality.

6.1 Introduction

Consider the two-way communication problem over the binary multiplying channel (BMC) depicted in Figure 6.1, where each user wishes to reliably communicate its message $M_j, j = 1, 2$, to the other user. The BMC is a discrete channel with two binary inputs and a binary output, $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y} \in \{0, 1\}$, such that at each time $i = 1, ..., n$, the output of the channel

$$Y_i = X_{1i} \cdot X_{2i} \tag{6.1}$$

is observed by both users. A $(2^{nR_1}, 2^{nR_2}, n)$ code consists of

1. two message sets $[1 : 2^{nR_1}]$ and $[1 : 2^{nR_2}]$,
2. two encoders, where encoder 1 assigns a symbol $x_{1i}(m_1, y^{i-1})$ to each pair (m_1, y^{i-1}) and encoder 2 assigns a symbol $x_{2i}(m_2, y^{i-1})$ to each pair (m_2, y^{i-1}) for $i \in [1 : n]$, and
3. two decoders, where decoder 1 assigns an estimate $\hat{m}_2$ to each pair (m_1, y^{i-1}) and decoder 2 assigns an estimate $\hat{m}_1$ to each pair (m_2, y^{i-1}).

We assume that the pair (M_1, M_2) is uniformly distributed over $[1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$. The average probability of error is defined as

$$P_e^{(n)} := \mathsf{P}\{(\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)\}.$$

A rate pair (R_1, R_2) is said to be achievable for the BMC if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that $P_e^{(n)} \to 0$ as $n \to \infty$. The capacity region $\mathscr{C}$ of the BMC is the closure of the set of achievable rate pairs (R_1, R_2). The capacity region of the BMC is not known.

6.2 Markov Decision Problem Formulation

In Chapter 4, we saw an application of control theory in designing codes for communication networks. This section presents an example where tools from

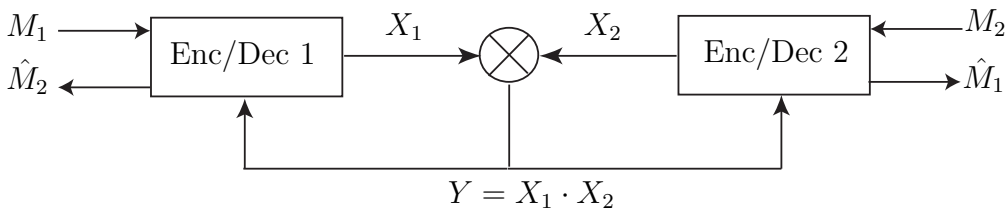


Figure 6.1: Binary multiplying channel

control theory can potentially be useful in deriving optimality conditions for communication codes over multi-user networks. In particular, we formulate the two-way communication over the binary multiplying channel as an average-cost infinite horizon Markov decision problem (MDP) and derive an optimality condition using dynamic programming.

Consider the following distributed control problem. Let the two controllers (encoders) 1 and 2 have access to random variables $M_1 \sim \text{Unif}[1 : 2^{nR_1}]$ and $M_2 \sim \text{Unif}[1 : 2^{nR_1}]$, respectively. At each time i, controllers 1 and 2 take actions (send symbols) $X_{1i} \in \{0, 1\}$ and $X_{2i} \in \{0, 1\}$ which are inputs to the BMC and the output of the channel $Y_i = X_{1i} \cdot X_{2i}$ is observed by both controllers. For a given cost function $c_i(M_1, M_2, Y^{i-1})$, one wishes to design controllers so as to minimize the asymptotic average expected cost

$$J := \limsup_{n\to\infty} \mathsf{E}\left(\frac{1}{n}\sum_{i=1}^{n} c_i(M_1, M_2, Y^{i-1})\right)$$

where the expectation is with respect to the probability measure induced by the choice of the controllers.

The distributed control problem above can be transformed to a centralized one by considering a fictitious central agent, who causally observes the channel outputs y^{i-1}, and controls the next symbols transmitted by the separated controllers through action $a_i = (a_{1i}, a_{2i})$, where $a_{1i} : (0, 1) \to \{0, 1\}$, and $a_{2i} : (0, 1) \to \{0, 1\}$ are functions such that

$$x_{1i} = a_{1i}(m_1), x_{2i} = a_{2i}(m_2). \tag{6.2}$$

With slight abuse of notation we use $A_i = (A_{1i}, A_{2i})$ to denote random functions. Note that the problem becomes centralized at the cost of expanding the space of actions from binary symbols to functions from unit interval to binary symbols. Let (M_1, M_2, Y^{i-1}) denote the state of the system, then this centralized problem can be viewed as a partially observable Markov decision problem (POMDP) since the central agent does not have access to (M_1, M_2). However, it is well-known [9] that we can transform POMDPs to fully observed MDPs as follows.

State: Let the state space be $\mathcal{S} = \{F : F \text{ is a probability distribution over } [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]\}$, and the state at time i be $s_i = F_{M_1,M_2}(\cdot|y^{i-1}, a^{i-1})$. We use S_i to denote a random distribution.

Action: At time i, action a_i generally depends on (y^{i-1}, a^{i-1}). Then, it follows that

$$\begin{aligned}
s_{i+1} &= F_{M_1,M_2}(\cdot|y^i, a^i) \\
&= \frac{F_{M_1,M_2}(\cdot|y^{i-1}, a^i)\,\mathsf{P}(y_i|\cdot, y^{i-1}, a^i)}{\mathsf{P}(y_i|y^{i-1}, a^i)} \\
&= \frac{F_{M_1,M_2}(\cdot|y^{i-1}, a^i)\,\mathsf{P}(y_i|\cdot, y^{i-1}, a^i)}{\sum_{m_1,m_2} \mathsf{P}(y_i|m_1, m_2, y^{i-1}, a^i) F_{M_1,M_2}(m_1, m_2|y^{i-1}, a^i)} \\
&= \frac{F_{M_1,M_2}(\cdot|y^{i-1}, a^i)\,\mathsf{P}(y_i|\cdot, a_i)}{\sum_{m_1,m_2} \mathsf{P}(y_i|m_1, m_2, a_i) F_{M_1,M_2}(m_1, m_2|y^{i-1}, a^i)} \qquad (6.3) \\
&= \frac{F_{M_1,M_2}(\cdot|y^{i-1}, a^{i-1})\,\mathsf{P}(y_i|\cdot, a_i)}{\sum_{m_1,m_2} \mathsf{P}(y_i|m_1, m_2, a_i) F_{M_1,M_2}(m_1, m_2|y^{i-1}, a^{i-1})}, \qquad (6.4)
\end{aligned}$$

where equality (6.3) comes from the fact that Y_i is a deterministic function of (M_1, M_2, A_i) according to the action (6.2) and the channel (6.1) such that $Y_i \to (M_1, M_2, A_i) \to (Y^{i-1}, A^{i-1})$ form a Markov chain. Equality (6.4) comes from the fact that $(M_1, M_2) \to (A^{i-1}, Y^{i-1}) \to A_i$ form a Markov chain since the common agent picks A_i only based on (A^{i-1}, Y^{i-1}). From (6.4) it can be verified that S_{i+1} is a deterministic function of (S_i, A_i, Y_i). Moreover, the distribution of Y_i is determined by (S_i, A_i) through (6.2). Therefore $(Y^{i-1}, A^{i-1}, S^{i-1}) \to (S_i, A_i) \to (S_{i+1}, Y_i)$ form a Markov chain and we conclude that S_i is an *information state* [9, Chapter 6] for the the purpose of control. Hence, there is no loss of optimality if we consider only Markov policies such that the action at time i depends on (Y^{i-1}, A^{i-1})

only through the information state S_i as follows

$$A_i = \pi_i(S_i),$$

where π_i is a mapping from the state S_i to the action A_i. We refer to the sequence $\{\pi_i\}$ as the policy π.

Cost: The mapping described above could be useful for different problems depending on the cost function. We define the cost at time i as

$$c(s, a) = -I(M_1, M_2; Y|S = s, A = a), \tag{6.5}$$

The input symbols to the channel are determined by action $A = a$ according to (6.2) and the distribution on M is given by $S = s$. Therefore, the distribution of Y can be computed given (s, a), and the cost at time i will be

$$\begin{aligned} c(s_i, a_i) &= -I(M_1, M_2; Y_i|S = s_i, A = a_i) \\ &= -I(M_1, M_2; Y_i|S = s_i, Y^{i-1} = y^{i-1}, A^i = a^i) \qquad (6.6) \\ &= -I(M_1, M_2; Y_i|Y^{i-1} = y^{i-1}, A^i = a^i), \end{aligned}$$

where equality (6.6) comes from the Markov chain $(Y^{i-1}, A^{i-1}) \to (S_i, A_i) \to (M_1, M_2, Y_i)$, and the last equality holds since s_n is a function of (y^{n-1}, a^{n-1}). Then, the expected average cost up to time n is

$$\begin{aligned} \frac{1}{n}\sum_{i=1}^{n} \mathsf{E}(c(S_i, A_i)) &= \frac{1}{n}\sum_{i=1}^{n} -I(M_1, M_2; Y_i|Y^{i-1}, A^i) \\ &= -\frac{1}{n}\sum_{i=1}^{n} I(M_1, M_2; Y_i, A_i|Y^{i-1}, A^{i-1}) \\ &= -\frac{1}{n} I(M_1, M_2; Y^n, A^n) \\ &= -\frac{1}{n} I(M_1, M_2; Y^n). \end{aligned}$$

Now, define the expected average cost incurred by policy π as

$$\begin{aligned} J(\pi) &:= \limsup_{n\to\infty} \mathsf{E}_\pi \left(\frac{1}{n} \sum_{i=1}^{n} c_i(S_i, A_i) \right) \\ &= \limsup_{n\to\infty} -\frac{1}{n} I_\pi(M_1, M_2; Y^n) \end{aligned}$$

where E_π denotes the expectation according to the probability measure determined by policy π when the initial state is $S_1 = F_{M_1,M_2}(\cdot) = \text{Unif}[1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$. Define J^* as follows

$$J^* := \inf_\pi J(\pi).$$

This problem is known as the average cost problem. To find the average cost optimality equation (ACOE) for this problem we use the following theorem which follows from [46, Theorem 6.1].

Theorem 6.2.1. *If there exists a $\tilde{J} \in \mathbb{R}$, a bounded function $V(s) \in \mathbb{R}$, $s \in \mathcal{S}$, and a stationary deterministic policy π^* such that $a = \pi^*(s)$ attains the infimum in*

$$\tilde{J} + V(s) = \inf \left(c(s,a) + \int_{\mathcal{S}} V(x) P(x|s,a) dx \right) \tag{6.7}$$

for all $s \in \mathcal{S}$, then the stationary deterministic policy π^* is optimal and $J^* = \tilde{J}$.

This theorem provides a sufficient condition for optimality of a policy, or equivalently, a code for the BMC. However, this sufficient condition is hard to verify since it has to hold for all $s \in \mathcal{S}$ and the state space is growing with n.

The mapping described above illustrates a potential application of techniques from control theory in characterizing the optimal information trade-off in multi-user communication settings. This is yet another example, in addition to the one discussed in Chapter 4, of how control theory can be useful in analyzing the performance of cooperative communication schemes.

6.3 Directed Information

Directed information, introduced by Massey [47], is a natural extension of mutual information to capture causality. More precisely, the directed information from a random vector X^n to another random vector Y^n of the same length is defined as

$$I(X^n \to Y^n) = \sum_{i=1}^{n} I(X^i, Y_i | Y^{i-1}) = H(Y^n) - \sum_{i=1}^{n} H(Y_i | Y^{i-1}, X^i).$$

Comparing with the mutual information between X^n and Y^n

$$I(X^n; Y^n) = \sum_{i=1}^{n} I(X^n, Y_i | Y^{i-1}) = H(Y^n) - \sum_{i=1}^{n} H(Y_i | Y^{i-1}, X^n),$$

one can see that X^n in the mutual information is replaced by X^i in the directed information. Similar to the conditional mutual information, the directed information from X^n to Y^n causally conditioned on Z^n is defined as

$$I(X^n \to Y^n || Z^n) = \sum_{i=1}^{n} I(X^i; Y_i | Y^{i-1}, Z^i).$$

We know [48] that the capacity region of a general two-way channel $p(y|x_1, x_2)$ with common output is $\mathscr{C} = \bigcup_n \mathscr{C}_n$, where $\mathscr{C}_n$ is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq \frac{1}{n} I(X_1^n \to Y^n || X_2^n) \\ R_2 &\leq \frac{1}{n} I(X_2^n \to Y^n || X_1^n) \end{aligned} \tag{6.8}$$

for some joint distribution of the form

$$\prod_{i=1}^{n} p(x_{1i}, x_{2i} | x_1^{i-1}, x_2^{i-1}, y^{i-1}) = \prod_{i=1}^{n} p(x_{1i} | x_1^{i-1}, y^{i-1}) p(x_{2i} | x_2^{i-1}, y^{i-1}). \tag{6.9}$$

Note that this characterization of the capacity region is not computable. However, for a given distribution of the form (6.9), an inner bound on the capacity region

can be derived based on (6.8).

6.4 Schalkwijk Code

In this section we evaluate (6.8) according to the probability distributions induced by the Schalkwijk code [49], a constructive code for the BMC, and show that symmetric rate pair $(R_1, R_2) = (0.6191, 0.6191)$ is achievable. This rate pair is strictly outside the Shannon inner bound [50], which is obtained based on random point-to-point codebooks generated independent of the received outputs.

The distribution induced by the Schalkwijk code is as follows. Let the output symbols Y^i be summarized in the state $S_i = f(Y^i) \in \{0, 1, 2\}$, where $s_0 = 0$ and

$$\begin{aligned} s_i &= 0 \quad \text{if} \;\; (s_{i-1} = 0, y_i = 1) \;\; \text{or} \;\; (s_{i-1} = 1, y_i = 0) \;\; \text{or} \;\; s_i = 2 \\ s_i &= 1 \quad \text{if} \;\; (s_{i-1} = 0, y_i = 0) \\ s_i &= 2 \quad \text{if} \;\; (s_{i-1} = 1, y_i = 1). \end{aligned} \tag{6.10}$$

The probability distribution $p(x_{1i}|x_1^{i-1}, y^{i-1})$ is given by

$$\begin{aligned} &p(x_{1i} = 1|s_{i-1} = 0) = \alpha \\ &p(x_{1i} = 0|s_{i-1} = 1, x_{1(i-1)} = 1) = \beta \\ &p(x_{1i} = 1|s_{i-1} = 1, x_{1(i-1)} = 0) = 1 \\ &p(x_{1i} = 0|s_{i-1} = 2, x_{1(i-2)} = 1) = 1 \\ &p(x_{1i} = 1|s_{i-1} = 2, x_{1(i-2)} = 0) = 1. \end{aligned} \tag{6.11}$$

for some $\alpha, \beta \in [0, 1]$. Substituting x_2 for x_1 in (6.11) we get $p(x_{2i}|x_2^{i-1}, y^{i-1})$. Note that X_{1i} and X_{2i} depends on Y^{i-1} only through the state S_{i-1}. Also, given the state S_{i-1} the memory is 2, i.e., the transmission at each time depends on at most 2 previous transmissions.

One can show that S_i is a Markov chain with the following transition matrix:

$$\mathbf{P_S} = \begin{pmatrix} \alpha^2 & \frac{2\alpha\beta}{1+\alpha} & 1 \\ 1-\alpha^2 & 0 & 0 \\ 0 & 1-\frac{2\alpha\beta}{1+\alpha} & 0 \end{pmatrix}. \tag{6.12}$$

This Markov chain is finite, irreducible, and aperiodic. Therefore, it has a unique stationary distribution which is also the limiting distribution. Next, we compute the achievable symmetric rate pair (R, R) from (6.8) considering the distribution induced by (6.10) and (6.11).

$$\begin{aligned} R = \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} H(Y_i|Y^{i-1}, X_2^i) &= \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} H(Y_i|Y^{i-1}, X_1^i) \\ &= \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} H(Y_i|Y^{i-1}, S^{i-1}, X_1^i) \qquad (6.13) \\ &= \lim_{i\to\infty} H(Y_i|Y^{i-1}, S^{i-1}, X_1^i), \qquad (6.14) \end{aligned}$$

where (6.13) comes from the fact that $S_i = f(Y^i)$. Note that

$$H(Y_i|X_{1i} = 0, X_1^{i-1}, Y^{i-1}, S^{i-1}).$$

Also, from the structure of the Schalkwijk code given in (6.10) and (6.11) the following Markov chains hold:

$$\begin{aligned} &X_{2i} \to (S_{i-1} = 0, X_{1i}) \to (X_1^{i-1}, Y^{i-1}, S^{i-1}) \\ &X_{2i} \to (S_{i-1} = 1, X_{1i}, X_{1(i-1)}) \to (X_1^{i-2}, Y^{i-1}, S^{i-1}) \\ &X_{2i} \to (S_{i-1} = 2, X_{1i}, X_{1(i-1)}, X_{1(i-2)}) \to (X_1^{i-3}, Y^{i-1}, S^{i-1}). \end{aligned}$$

and we can write (6.14) as

$$\begin{aligned} R &= \lim_{n\to\infty} H(Y_i|Y^{i-1}, S^{i-1}, X_1^i) \\ &= \lim_{n\to\infty} \Big[H(X_{2i}|X_{1i} = 1, S_{i-1} = 0).\, \mathsf{P}(X_{1i} = 1, S_{i-1} = 0) \end{aligned}$$

$$
\begin{aligned}
&+ \sum_{x_{1(i-1)}} H(X_{2i}|X_{1(i-1)} = x_{1(i-1)}, X_{1i} = 1, S_{i-1} = 1) \\
&\qquad\qquad \times \mathsf{P}(X_{1(i-1)} = x_{1(i-1)}, X_{1i} = 1, S_{i-1} = 1) \\
&+ \sum_{x_{1(i-1)}, x_{1(i-2)}} H(X_{2i}|X_{1(i-2)} = x_{1(i-2)}, X_{1(i-1)} = x_{1(i-1)}, X_{1i} = 1, S_{i-1} = 2) \\
&\qquad \times \mathsf{P}(X_{1(i-2)} = x_{1(i-2)}, X_{1(i-1)} = x_{1(i-1)}, X_{1i} = 1, S_{i-1} = 2)\Big] \\
&= a_1 \cdot p_1 + a_2 \cdot p_2 + a_3 \cdot p_3 \qquad (6.15)
\end{aligned}
$$

where p_1, p_2, p_3 denote the the stationary distribution of the Markov chain with transition matrix (6.12), that is, $p_j = \lim_{i\to\infty} \mathsf{P}(S_i = j-1)$, $j = 1, 2, 3$, and a_1, a_2, a_3 are

$$
\begin{aligned}
a_1 &= H(X_{2i}|X_{1i} = 1, S_{i-1} = 0).\,\mathsf{P}(X_{1i} = 1|S_{i-1} = 0) \\
a_2 &= \sum_{x_{1(i-1)}} H(X_{2i}|X_{1(i-1)} = x_{1(i-1)}, X_{1i} = 1, S_{i-1} = 1) \\
&\qquad\qquad \times \mathsf{P}(X_{1(i-1)} = x_{1(i-1)}, X_{1i} = 1|S_{i-1} = 1) \\
a_3 &= \sum_{x_{1(i-1)}, x_{1(i-2)}} H(X_{2i}|X_{1(i-2)} = x_{1(i-2)}, X_{1(i-1)} = x_{1(i-1)}, X_{1i} = 1, S_{i-1} = 2) \\
&\qquad \times \mathsf{P}(X_{1(i-2)} = x_{1(i-2)}, X_{1(i-1)} = x_{1(i-1)}, X_{1i} = 1|S_{i-1} = 2).
\end{aligned}
$$

According to (6.10) and (6.11) we have

$$
\begin{aligned}
a_1 &= \alpha \cdot h(\alpha) \\
a_2 &= \frac{1}{(1+\alpha)} \cdot h(\alpha\beta) \\
a_3 &= \frac{1-\alpha\beta}{1+\alpha-2\alpha\beta} \cdot h\left(\frac{1-\alpha}{1-\alpha\beta}\right).
\end{aligned}
$$

Given a_1, a_2, a_3 and the stationary distribution of (6.12), the expression (6.15) is maximized for

$$
\begin{aligned}
\alpha^* &= 0.6757 \\
\beta^* &= 0.7023,
\end{aligned}
$$

and we can conclude that the corresponding symmetric rate pair $(0.6191, 0.6191)$ is achievable.

Chapter 6 is based on a research project in collaboration with Professors T. Javidi and Y.-H. Kim. The dissertation author was the primary investigator.

Bibliography

[1] A. El Gamal and Y.-H. Kim. *Lecture Notes on Network Information Theory*. Stanford University and University of California San Diego, 2010.

[2] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948.

[3] C. E. Shannon. The zero error capacity of a noisy channel. *IRE Trans. Inf. Theory*, 2:8–19, 1956.

[4] C. E. Shannon. Coding theorems for a discrete source with a fidelity criterion. *IRE Int. Conv. Rec., part 4*, 7:142–163, 1959.

[5] E. Ardestanizadeh and M. Franceschetti. Control-theoretic approach to communication with feedback: Fundamental limits and code design. arXiv:1006.5265, Jun. 2010, submitted for publication in *IEEE Trans. Automatic Control*.

[6] J. P. M. Schalkwijk and T. Kailath. A coding scheme for additive noise channels with feedback–I: No bandlimited constraint. *IEEE Trans. Inf. Theory*, 12:172–182, 1966.

[7] J. P. M. Schalkwijk. A coding scheme for additive noise channels with feedback–II: Band-limited signals. *IEEE Trans. Inf. Theory*, 12:183–189, 1966.

[8] O. Shayevitz and M. Feder. Optimal feedback communication via posterior matching. Preprint, http://arxiv.org/abs/0909.4828.

[9] P. R. Kumar and P. Varaiya. *Stochastic Control: Estimation, Identification, and Adaptive Control*. Prentice Hall, 1986.

[10] L. H. Ozarow. The capacity of the white Gaussian multiple-access channel with feedback. *IEEE Trans. Inf. Theory*, 30:623–629, 1984.

[11] J. A. Thomas. Feedback can at most double Gaussain multiple access channel capacity. *IEEE Trans. Inf. Theory*, 33:711–716, 1987.

[12] E. Ordentlich. On the factor-of-two bound for Gaussian multiple access channel with feedback. *IEEE Trans. Inf. Theory*, 42:2231–2235, 1996.

[13] S. Pombra and T. M. Cover. Non white Gaussian multiple access channels with feedback. *IEEE Trans. Inf. Theory*, 40:885–892, 1994.

[14] G. Kramer. Feedback strategies for white Gaussian interference networks. *IEEE Trans. Inf. Theory*, 48:1423–1438, 2002.

[15] T. M. Cover and S. Pombra. Gaussian feedback capacity. *IEEE Trans. Inf. Theory*, 35:37–43, 1989.

[16] A. P. Hekstra and F. M. J. Willems. Dependence balance bounds for single-output two-way channels. *IEEE Trans. Inf. Theory*, 35:44–53, 1989.

[17] G. Kramer and M. Gastpar. Dependece balance and the gaussian multiaccess channel with feedback. In *Proc. IEEE Information Theory Workshop*, 2006.

[18] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[19] W. Wu, S. Vishwanath, and A. Arapostathis. Gaussian interference networks with feedback: Duality, sum capacity and dynamic team problem. In *Proc. 44th Allerton Conference on Communication, Control, and Computation*, 2005.

[20] A. Réyni. On measures of dependence. *Acta Mathematica Hungarica*, 10:441–451, 1959.

[21] Y.-H. Kim, A. Lapidoth, and T. Weissman. On the reliability of gaussian channels with noisy feedback. In *Proc. 44th Allerton Conference on Communication, Control, and Computation*, 2006.

[22] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. 2nd ed. New York: Wiley, 2006.

[23] T. Kailath, A. H. Sayed, and B. Hassibi. *Linear Estimation*. 2nd ed. New York: Wiley, 2006.

[24] P. Lancaster and L. Rodman. *Algebraic Riccati Equations*. New York: Oxford University Press, 1995.

[25] Y.-H. Kim. Feedback capacity of stationary Gaussian channels. *IEEE Trans. Inf. Theory*, 56:57–85, 2010.

[26] H. O. Lancaster. Some properties of the bivariate normal distribution considered in the form of a contingency table. *Biometrika*, 44:289–292, 1957.

[27] E. Ardestanizadeh, M. A. Wigger, T. Javidi, and Y.-H. Kim. Linear sum capacity for Gaussian multiple access channel with feedback. arXiv:1002.1781, Feb. 2010, submitted for publication in *IEEE Trans. Inf. Theory*.

[28] G. Dueck. Partial feedback for two-way and broadcast channels. *Inform. Contr.*, 46:1–15, 1980.

[29] L. H. Ozarow and C. S. K. Leung. An achievable region and outer bound for the gaussian broadcast channel with feedback. *IEEE Trans. Inf. Theory*, 30:667–671, 1984.

[30] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[31] M. A. Wigger and M. Gastpar. The pre-log of gaussian broadcast with feedback can be two. In *Proc. IEEE International Symposium on Information Theory*, 2008.

[32] N. Elia. When Bode meets Shannon: Control oriented feedback communication schemes. *IEEE Trans. Automatic Control*, 47:1477–1488, 2004.

[33] G. Chen and S. Hsu. *Linear Stochastic Control Systems*. 2nd ed. CRC Press, 1995.

[34] E. Ardestanizadeh, P. Minero, and M. Franceschetti. LQG control approach to Gaussian broadcast channels with feedback. Preprint, 2010, to be submitted for publication in *IEEE Trans. Inf. Theory*.

[35] C. E. Shannon. Communication theory of secrecy systems. *Bell System Tech. J.*, 28:656–715, 1949.

[36] A. D. Wyner. The wire-tap channel. *Bell System Tech. J.*, 54:1355–1387, 1975.

[37] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24:339–348, 1978.

[38] A. El Gamal. The capacity of a class of broadcast channels. *IEEE Trans. Inf. Theory*, 25:166–169, 1979.

[39] H. Yamamoto. Rate-distortion theory for the Shannon cipher system. *IEEE Trans. Inf. Theory*, 43:827–835, 1997.

[40] N. Merhav. Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels. *IEEE Trans. Inf. Theory*, 54:2723–2734, June 2008.

[41] R. Ahlswede and N. Cai. Transmission, identification, and common randomness capacities for wire-tape channels with secure feedback from the decoder. In *Book chapter in General Theory of Information Transfer and Combinatorics*, pages 258–275, 2006.

[42] L. Lai, H. El Gamal, and V. Poor. The wiretap channel with feedback: Encryption over the channel. *IEEE Trans. Inf. Theory*, 54:5059–5067, 2008.

[43] E. Tekin and A. Yener. The general Gaussian multiple access channel and two-way wire-tap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory*, 54:2735–2751, 2008.

[44] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wiretap channel. *IEEE Trans. Inf. Theory*, 24:451–456, 1978.

[45] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim. Wiretap channel with secure rate-limited feedback. *IEEE Trans. Inf. Theory*, 55:5353–5361, 2009.

[46] A. Araposthathis, V. Borkar, E. Fernández-Gaucherand, M. Ghost, and S. Marcels. Discrete-time controlled Markov processes with average cost criterion: A survey. *SIAM J. Control Optim.*, 31:282–344, 1993.

[47] J. L. Massey. Causality, feedback, and directed information. In *Proc. International Symposium on Information Theory and its Applications*, 1990.

[48] G. Kramer. Capacity results for discrete memoryless network. *IEEE Trans. Inf. Theory*, 49:4–21, 2003.

[49] J. P. M. Schalkwijk. The binary multiplying channel: A coding scheme that operates beyond shannon's inner bound region. *IEEE Trans. Inf. Theory*, 28:107–110, 1982.

[50] C. E. Shannon. Two-way communication channels. *Proc. 4th Berkeley Sympos. Math. Statist. Prob.*, 1961.