Network Information Theory

This comprehensive treatment of network information theory and its applications provides the first unified coverage of both classical and recent results. With an approach that balances the introduction of new models and new coding techniques, readers are guided through Shannon's point-to-point information theory, single-hop networks, multihop networks, and extensions to distributed computing, secrecy, wireless communication, and networking. Elementary mathematical tools and techniques are used throughout, requiring only basic knowledge of probability, whilst unified proofs of coding theorems are based on a few simple lemmas, making the text accessible to newcomers. Key topics covered include successive cancellation and superposition coding, MIMO wireless communication, network coding, and cooperative relaying. Also covered are feedback and interactive communication, capacity approximations and scaling laws, and asynchronous and random access channels. This book is ideal for use in the classroom, for self-study, and as a reference for researchers and engineers in industry and academia.

Abbas El Gamal is the Hitachi America Chaired Professor in the School of Engineering and the Director of the Information Systems Laboratory in the Department of Electrical Engineering at Stanford University. In the field of network information theory, he is best known for his seminal contributions to the relay, broadcast, and interference channels; multiple description coding; coding for noisy networks; and energy-efficient packet scheduling and throughput–delay tradeoffs in wireless networks. He is a Fellow of IEEE and the winner of the 2012 Claude E. Shannon Award, the highest honor in the field of information theory.

Young-Han Kim is an Assistant Professor in the Department of Electrical and Computer Engineering at the University of California, San Diego. His research focuses on information theory and statistical signal processing. He is a recipient of the 2008 NSF Faculty Early Career Development (CAREER) Award and the 2009 US–Israel Binational Science Foundation Bergmann Memorial Award.

NETWORK INFORMATION THEORY

Abbas El Gamal
Stanford University

Young-Han Kim
University of California, San Diego

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Tokyo, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9781107008731

First published 2011

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data

ISBN 978-1-107-00873-1 Hardback

Additional resources for this publication at www.cambridge.org/9781107008731

To our families
whose love and support
made this book possible

Contents

Part III Multihop Networks

Appendices

Preface

Network information theory aims to establish the fundamental limits on information flow in networks and the optimal coding schemes that achieve these limits. It extends Shannon's fundamental theorems on point-to-point communication and the Ford–Fulkerson max-flow min-cut theorem for graphical unicast networks to general networks with multiple sources and destinations and shared resources. Although the theory is far from complete, many elegant results and techniques have been developed over the past forty years with potential applications in real-world networks. This book presents these results in a coherent and simplified manner that should make the subject accessible to graduate students and researchers in electrical engineering, computer science, statistics, and related fields, as well as to researchers and practitioners in industry.

The first paper on network information theory was on the two-way channel by Shannon (1961). This was followed a decade later by seminal papers on the broadcast channel by Cover (1972), the multiple access channel by Ahlswede (1971, 1974) and Liao (1972), and distributed lossless compression by Slepian and Wolf (1973a). These results spurred a flurry of research on network information theory from the mid 1970s to the early 1980s with many new results and techniques developed; see the survey papers by van der Meulen (1977) and El Gamal and Cover (1980), and the seminal book by Csiszár and Körner (1981b). However, many problems, including Shannon's two-way channel, remained open and there was little interest in these results from communication theorists or practitioners. The period from the mid 1980s to the mid 1990s represents a "lost decade" for network information theory during which very few papers were published and many researchers shifted their focus to other areas. The advent of the Internet and wireless communication, fueled by advances in semiconductor technology, compression and error correction coding, signal processing, and computer science, revived the interest in this subject and there has been an explosion of activities in the field since the mid 1990s. In addition to progress on old open problems, recent work has dealt with new network models, new approaches to coding for networks, capacity approximations and scaling laws, and topics at the intersection of networking and information theory. Some of the techniques developed in network information theory, such as successive cancellation decoding, multiple description coding, successive refinement of information, and network coding, are being implemented in real-world networks.

Development of the Book

The idea of writing this book started a long time ago when Tom Cover and the first author considered writing a monograph based on their aforementioned 1980 survey paper. The first author then put together a set of handwritten lecture notes and used them to teach a course on multiple user information theory at Stanford University from 1982 to 1984. In response to high demand from graduate students in communication and information theory, he resumed teaching the course in 2002 and updated the early lecture notes with recent results. These updated lecture notes were used also in a course at EPFL in the summer of 2003. In 2007 the second author, who was in the 2002 class, started teaching a similar course at UC San Diego and the authors decided to collaborate on expanding the lecture notes into a textbook. Various versions of the lecture notes have been used since then in courses at Stanford University, UC San Diego, the Chinese University of Hong Kong, UC Berkeley, Tsinghua University, Seoul National University, University of Notre Dame, and McGill University among others. The lecture notes were posted on the arXiv in January 2010. This book is based on these notes. Although we have made an effort to provide a broad coverage of the results in the field, we do not claim to be all inclusive. The explosion in the number of papers on the subject in recent years makes it almost impossible to provide a complete coverage in a single textbook.

Organization of the Book

We considered several high-level organizations of the material in the book, from source coding to channel coding or vise versa, from graphical networks to general networks, or along historical lines. We decided on a pedagogical approach that balances the introduction of new network models and new coding techniques. We first discuss single-hop networks and then multihop networks. Within each type of network, we first study channel coding, followed by their source coding counterparts, and then joint source–channel coding. There were several important topics that did not fit neatly into this organization, which we grouped under Extensions. The book deals mainly with discrete memoryless and Gaussian network models because little is known about the limits on information flow for more complex models. Focusing on these models also helps us present the coding schemes and proof techniques in their simplest possible forms.

The first chapter provides a preview of network information theory using selected examples from the book. The rest of the material is divided into four parts and a set of appendices.

Part I. Background (Chapters 2 and 3). We present the needed basic information theory background, introduce the notion of typicality and related lemmas used throughout the book, and review Shannon's point-to-point communication coding theorems.

Part II. Single-hop networks (Chapters 4 through 14). We discuss networks with single-round one-way communication. Here each node is either a sender or a receiver. The material is divided into three types of communication settings.

- *Independent messages over noisy channels (Chapters 4 through 9).* We discuss noisy

single-hop network building blocks, beginning with multiple access channels (many-to-one communication) in Chapter 4, followed by broadcast channels (one-to-many communication) in Chapters 5 and 8, and interference channels (multiple one-to-one communications) in Chapter 6. We split the discussion on broadcast channels for a pedagogical reason—the study of general broadcast channels in Chapter 8 requires techniques that are introduced more simply through the discussion of channels with state in Chapter 7. In Chapter 9, we study Gaussian vector channels, which model multiple-antenna (multiple-input multiple-output/MIMO) communication systems.

- *Correlated sources over noiseless links (Chapters 10 through 13).* We discuss the source coding counterparts of the noisy single-hop network building blocks, beginning with distributed lossless source coding in Chapter 10, followed by lossy source coding with side information in Chapter 11, distributed lossy source coding in Chapter 12, and multiple description coding in Chapter 13. Again we spread the discussion on distributed coding over three chapters to help develop new ideas gradually.
- *Correlated sources over noisy channels (Chapter 14).* We discuss the general setting of sending uncompressed sources over noisy single-hop networks.

Part III. Multihop networks (Chapters 15 through 20). We discuss networks with relaying and multiple rounds of communication. Here some of the nodes can act as both sender and receiver. In an organization parallel to Part II, the material is divided into three types of settings.

- *Independent messages over graphical networks (Chapter 15).* We discuss coding for networks modeled by graphs beyond simple routing.
- *Independent messages over noisy networks (Chapters 16 through 19).* In Chapter 16, we discuss the relay channel, which is a simple two-hop network with a sender, a receiver, and a relay. We then discuss channels with feedback and the two-way channel in Chapter 17. We extend results on the relay channel and the two-way channel to general noisy networks in Chapter 18. We further discuss approximations and scaling laws for the capacity of large wireless networks in Chapter 19.
- *Correlated sources over graphical networks (Chapter 20).* We discuss source coding counterparts of the channel coding problems in Chapters 15 through 18.

Part IV. Extensions (Chapters 21 through 24). We study extensions of the theory discussed in the first three parts of the book to communication for computing in Chapter 21, communication with secrecy constraints in Chapter 22, wireless fading channels in Chapter 23, and to problems at the intersection of networking and information theory in Chapter 24.

Appendices. To make the book as self-contained as possible, Appendices A, B, and E provide brief reviews of the necessary background on convex sets and functions, probability and estimation, and convex optimization, respectively. Appendices C and D describe techniques for bounding the cardinality of auxiliary random variables appearing in many

capacity and rate region characterizations, and the Fourier–Motzkin elimination procedure, respectively.

Presentation of the Material

Each chapter typically contains both teaching material and advanced topics. Starred sections contain topics that are either too technical to be discussed in detail or are not essential to the main flow of the material. The chapter ends with a bulleted summary of key points and open problems, bibliographic notes, and problems on missing proof steps in the text followed by exercises around the key ideas. Some of the more technical and less central proofs are delegated to appendices at the end of each chapter in order to help the reader focus on the main ideas and techniques.

The book follows the adage "a picture is worth a thousand words." We use illustrations and examples to provide intuitive explanations of models and concepts. The proofs follow the principle of making everything as simple as possible but not simpler. We use elementary tools and techniques, requiring only basic knowledge of probability and some level of mathematical maturity, for example, at the level of a first course on information theory. The achievability proofs are based on joint typicality, which was introduced by Shannon in his 1948 paper and further developed in the 1970s by Forney and Cover. We take this approach one step further by developing a set of simple lemmas to reduce the repetitiveness in the proofs. We show how the proofs for discrete memoryless networks can be extended to their Gaussian counterparts by using a discretization procedure and taking appropriate limits. Some of the proofs in the book are new and most of them are simplified—and in some cases more rigorous—versions of published proofs.

Use of the Book in Courses

As mentioned earlier, the material in this book has been used in courses on network information theory at several universities over many years. We hope that the publication of the book will help make such a course more widely adopted. One of our main motivations for writing the book, however, is to broaden the audience for network information theory. Current education of communication and networking engineers encompasses primarily point-to-point communication and wired networks. At the same time, many of the innovations in modern communication and networked systems concern more efficient use of shared resources, which is the focus of network information theory. We believe that the next generation of communication and networking engineers can benefit greatly from having a working knowledge of network information theory. We have made every effort to present some of the most relevant material to this audience as simply and clearly as possible. In particular, the material on Gaussian channels, wireless fading channels, and Gaussian networks can be readily integrated into an advanced course on wireless communication.

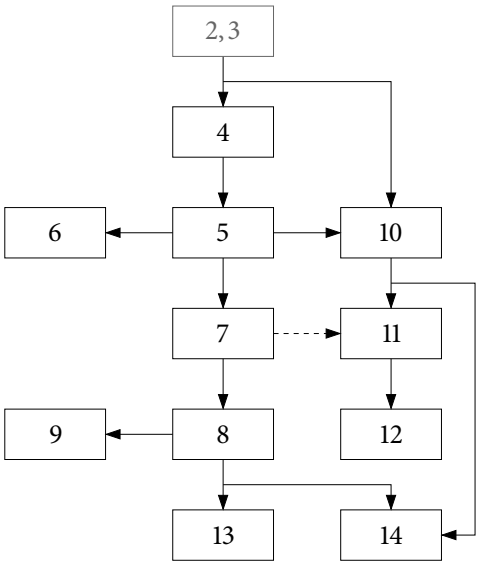
The book can be used as a main text in a one-quarter/semester first course on information theory with emphasis on communication or a one-quarter second course on information theory, or as a supplementary text in courses on communication, networking,

computer science, and statistics. Most of the teaching material in the book can be covered in a two-quarter course sequence. Slides for such courses are posted at http://arxiv.org/abs/1001.3404/.

Dependence Graphs

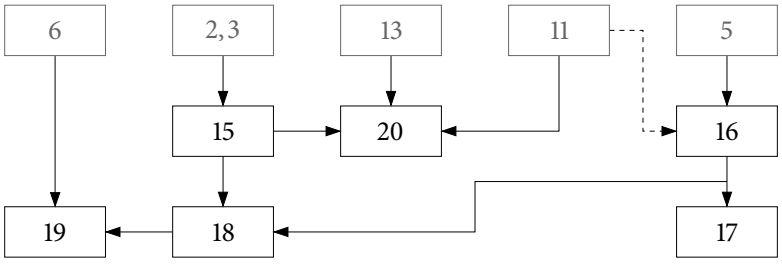
The following graphs depict the dependence of each chapter on its preceding chapters. Each box contains the chapter number and lighter boxes represent dependence on previous parts. Solid edges represent required reading and dashed edges represent recommended reading.

Part II.



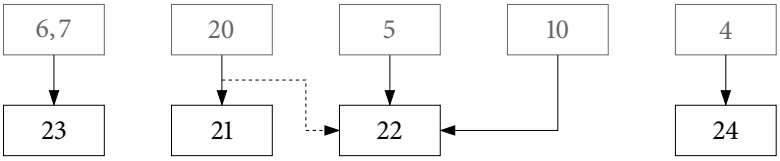
2 Information measures and typicality
3 Point-to-point information theory
4 Multiple access channels
5 Degraded broadcast channels
6 Interference channels
7 Channels with state
8 General broadcast channels
9 Gaussian vector channels
10 Distributed lossless compression
11 Lossy compression with side information
12 Distributed lossy compression
13 Multiple description coding
14 Joint source–channel coding

Part III.



15 Graphical networks
16 Relay channels
17 Interactive channel coding
18 Discrete memoryless networks
19 Gaussian networks
20 Compression over graphical networks

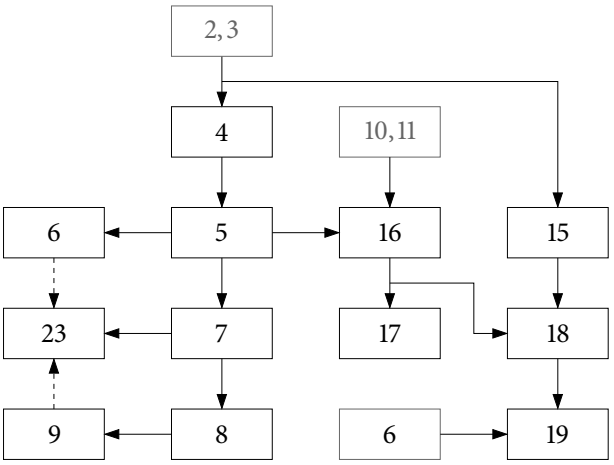
Part IV.



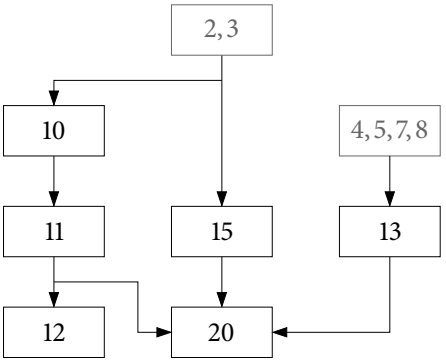
21 Communication for computing
22 Information theoretic secrecy
23 Wireless fading channels
24 Networking and information theory

In addition to the dependence graphs for each part, we provide below some interest-based dependence graphs.

Communication.



Data compression.



Abbas El Gamal
Young-Han Kim

Palo Alto, California
La Jolla, California
July 2011

Acknowledgments

The development of this book was truly a community effort. Many colleagues, teaching assistants of our courses on network information theory, and our postdocs and PhD students provided invaluable input on the content, organization, and exposition of the book, and proofread earlier drafts.

First and foremost, we are indebted to Tom Cover. He taught us everything we know about information theory, encouraged us to write this book, and provided several insightful comments. We are also indebted to our teaching assistants—Ehsan Ardestanizadeh, Chiao-Yi Chen, Yeow-Khiang Chia, Shirin Jalali, Paolo Minero, Haim Permuter, Han-I Su, Sina Zahedi, and Lei Zhao—for their invaluable contributions to the development of this book. In particular, we thank Sina Zahedi for helping with the first set of lecture notes that ultimately led to this book. We thank Han-I Su for his contributions to the chapters on quadratic Gaussian source coding and distributed computing and his thorough proofreading of the entire draft. Yeow-Khiang Chia made invaluable contributions to the chapters on information theoretic secrecy and source coding over graphical networks, contributed several problems, and proofread many parts of the book. Paolo Minero helped with some of the material in the chapter on information theory and networking.

We are also grateful to our PhD students. Bernd Bandemer contributed to the chapter on interference channels and proofread several parts of the book. Sung Hoon Lim contributed to the chapters on discrete memoryless and Gaussian networks. James Mammen helped with the first draft of the lecture notes on scaling laws. Lele Wang and Yu Xiang also provided helpful comments on many parts of the book.

We benefited greatly from discussions with several colleagues. Chandra Nair contributed many of the results and problems in the chapters on broadcast channels. David Tse helped with the organization of the chapters on fading and interference channels. Mehdi Mohseni helped with key proofs in the chapter on Gaussian vector channels. Amin Gohari helped with the organization and several results in the chapter on information theoretic secrecy. Olivier Lévêque helped with some of the proofs in the chapter on Gaussian networks. We often resorted to John Gill for stylistic and editorial advice. Jun Chen, Sae-Young Chung, Amos Lapidoth, Prakash Narayan, Bobak Nazer, Alon Orlitsky, Ofer Shayevitz, Yossi Steinberg, Aslan Tchamkerten, Dimitris Toumpakaris, Sergio Verdú, Mai Vu, Michèle Wigger, Ram Zamir, and Ken Zeger provided helpful input during the writing of this book. We would also like to thank Venkat Anantharam, François Baccelli, Stephen Boyd, Max Costa, Paul Cuff, Suhas Diggavi, Massimo Franceschetti, Michael Gastpar,

Andrea Goldsmith, Bob Gray, Te Sun Han, Tara Javidi, Ashish Khisti, Gerhard Kramer, Mohammad Maddah-Ali, Andrea Montanari, Balaji Prabhakar, Bixio Rimoldi, Anant Sahai, Anand Sarwate, Devavrat Shah, Shlomo Shamai, Emre Telatar, Alex Vardy, Tsachy Weissman, and Lin Zhang.

This book would not have been written without the enthusiasm, inquisitiveness, and numerous contributions of the students who took our courses, some of whom we have already mentioned. In addition, we would like to acknowledge Ekine Akuiyibo, Lorenzo Coviello, Chan-Soo Hwang, Yashodhan Kanoria, Tae Min Kim, Gowtham Kumar, and Moshe Malkin for contributions to some of the material. Himanshu Asnani, Yuxin Chen, Aakanksha Chowdhery, Mohammad Naghshvar, Ryan Peng, Nish Sinha, and Hao Zou provided many corrections to earlier drafts. Several graduate students from UC Berkeley, MIT, Tsinghua, University of Maryland, Tel Aviv University, and KAIST also provided valuable feedback.

We would like to thank our editor Phil Meyler and the rest of the Cambridge staff for their exceptional support during the publication stage of this book. We also thank Kelly Yilmaz for her wonderful administrative support. Finally, we acknowledge partial support for the work in this book from the DARPA ITMANET and the National Science Foundation.

Notation

We introduce the notation and terminology used throughout the book.

Sets, Scalars, and Vectors

We use lowercase letters $x, y, \ldots$ to denote constants and values of random variables. We use $x_i^j = (x_i, x_{i+1}, \ldots, x_j)$ to denote an $(j - i + 1)$-sequence/column vector for $1 \le i \le j$. When $i = 1$, we always drop the subscript, i.e., $x^j = (x_1, x_2, \ldots, x_j)$. Sometimes we write $\mathbf{x}, \mathbf{y}, \ldots$ for constant vectors with specified dimensions and x_j for the j-th component of $\mathbf{x}$. Let $\mathbf{x}(i)$ be a vector indexed by time i and $x_j(i)$ be the j-th component of $\mathbf{x}(i)$. The sequence of these vectors is denoted by $\mathbf{x}^n = (\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(n))$. An all-one column vector $(1, \ldots, 1)$ with a specified dimension is denoted by $\mathbf{1}$.

Let $\alpha, \beta \in [0, 1]$. Then $\bar{\alpha} = (1 - \alpha)$ and $\alpha * \beta = \alpha\bar{\beta} + \beta\bar{\alpha}$.

Let $x^n, y^n \in \{0, 1\}^n$ be binary n-vectors. Then $x^n \oplus y^n$ is the componentwise modulo-2 sum of the two vectors.

Calligraphic letters $\mathcal{X}, \mathcal{Y}, \ldots$ are used exclusively for finite sets and $|\mathcal{X}|$ denotes the cardinality of the set $\mathcal{X}$. The following notation is used for common sets:

- $\mathbb{R}$ is the real line and $\mathbb{R}^d$ is the d-dimensional real Euclidean space.
- $\mathbb{F}_q$ is the finite field GF(q) and $\mathbb{F}_q^d$ is the d-dimensional vector space over GF(q).

Script letters $\mathscr{C}, \mathscr{R}, \mathscr{P}, \ldots$ are used for subsets of $\mathbb{R}^d$.

For a pair of integers $i \le j$, we define the discrete interval $[i : j] = \{i, i + 1, \ldots, j\}$. More generally, for $a \ge 0$ and integer $i \le 2^a$, we define

- $[i : 2^a) = \{i, i + 1, \ldots, 2^{\lfloor a \rfloor}\}$, where $\lfloor a \rfloor$ is the integer part of a, and
- $[i : 2^a] = \{i, i + 1, \ldots, 2^{\lceil a \rceil}\}$, where $\lceil a \rceil$ is the smallest integer $\ge a$.

Probability and Random Variables

The probability of an event $\mathcal{A}$ is denoted by $\mathsf{P}(\mathcal{A})$ and the conditional probability of $\mathcal{A}$ given $\mathcal{B}$ is denoted by $\mathsf{P}(\mathcal{A} \,|\, \mathcal{B})$. We use uppercase letters $X, Y, \ldots$ to denote random variables. The random variables may take values from finite sets $\mathcal{X}, \mathcal{Y}, \ldots$ or from the real line $\mathbb{R}$. By convention, $X = \emptyset$ means that X is a degenerate random variable (unspecified constant) regardless of its support. 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 $X_i^j = (X_i, \ldots, X_j)$ to denote a $(j - i + 1)$-sequence/column vector of random variables for $1 \le i \le j$. When $i = 1$, we always drop the subscript and use $X^j = (X_1, \ldots, X_j)$.

Let $(X_1, \ldots, X_k)$ be a tuple of k random variables and $\mathcal{J} \subseteq [1:k]$. The subtuple of random variables with indices from $\mathcal{J}$ is denoted by $X(\mathcal{J}) = (X_j \colon j \in \mathcal{J})$. Similarly, given k random vectors $(X_1^n, \ldots, X_k^n)$,

$$X^n(\mathcal{J}) = (X_j^n \colon j \in \mathcal{J}) = (X_1(\mathcal{J}), \ldots, X_n(\mathcal{J})).$$

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 $\mathbf{X}(i)$. We denote the sequence of these vectors by $\mathbf{X}^n = (\mathbf{X}(1), \ldots, \mathbf{X}(n))$.

The following notation is used to specify random variables and random vectors.

- $X^n \sim p(x^n)$ means that $p(x^n)$ is the probability mass function (pmf) of the discrete random vector X^n. The function $p_{X^n}(\tilde{x}^n)$ denotes the pmf of X^n with argument $\tilde{x}^n$, i.e., $p_{X^n}(\tilde{x}^n) = \mathsf{P}\{X^n = \tilde{x}^n\}$ for all $\tilde{x}^n \in \mathcal{X}^n$. The function $p(x^n)$ without subscript is understood to be the pmf of the random vector X^n defined over $\mathcal{X}_1 \times \cdots \times \mathcal{X}_n$.
- $X^n \sim f(x^n)$ means that $f(x^n)$ is the probability density function (pdf) of the continuous random vector X^n.
- $X^n \sim F(x^n)$ means that $F(x^n)$ is the cumulative distribution function (cdf) of X^n.
- $(X^n, Y^n) \sim p(x^n, y^n)$ means that $p(x^n, y^n)$ is the joint pmf of X^n and Y^n.
- $Y^n \,|\, \{X^n \in \mathcal{A}\} \sim p(y^n \,|\, X^n \in \mathcal{A})$ means that $p(y^n \,|\, X^n \in \mathcal{A})$ is the conditional pmf of Y^n given $\{X^n \in \mathcal{A}\}$.
- $Y^n \,|\, \{X^n = x^n\} \sim p(y^n|x^n)$ means that $p(y^n|x^n)$ is the conditional pmf of Y^n given $\{X^n = x^n\}$.
- $p(y^n|x^n)$ is a collection of (conditional) pmfs on $\mathcal{Y}^n$, one for every $x^n \in \mathcal{X}^n$. $f(y^n|x^n)$ and $F(y^n|x^n)$ are similarly defined.
- $Y^n \sim p_{X^n}(y^n)$ means that Y^n has the same pmf as X^n, i.e., $p(y^n) = p_{X^n}(y^n)$. Similar notation is used for conditional probability distributions.

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 $\mathrm{Var}(X) = \mathsf{E}[(X - \mathsf{E}(X))^2]$ to denote the variance of X and $\mathrm{Var}(X|Y) = \mathsf{E}[(X - \mathsf{E}(X|Y))^2 \,|\, Y]$ to denote the conditional variance of X given Y.

For random vectors $\mathbf{X} = X^n$ and $\mathbf{Y} = Y^k$, $K_{\mathbf{X}} = \mathsf{E}[(\mathbf{X} - \mathsf{E}(\mathbf{X}))(\mathbf{X} - \mathsf{E}(\mathbf{X}))^T]$ denotes the covariance matrix of $\mathbf{X}$, $K_{\mathbf{XY}} = \mathsf{E}[(\mathbf{X} - \mathsf{E}(\mathbf{X}))(\mathbf{Y} - \mathsf{E}(\mathbf{Y}))^T]$ denotes the crosscovariance matrix of $(\mathbf{X}, \mathbf{Y})$, and $K_{\mathbf{X}|\mathbf{Y}} = \mathsf{E}[(\mathbf{X} - \mathsf{E}(\mathbf{X}|\mathbf{Y}))(\mathbf{X} - \mathsf{E}(\mathbf{X}|\mathbf{Y}))^T] = K_{\mathbf{X}-\mathsf{E}(\mathbf{X}|\mathbf{Y})}$ denotes the conditional covariance matrix of $\mathbf{X}$ given $\mathbf{Y}$, that is, the covariance matrix of the minimum mean squared error (MMSE) for estimating $\mathbf{X}$ given $\mathbf{Y}$.

We use the following notation for standard random variables and random vectors:

- $X \sim \text{Bern}(p)$: X is a Bernoulli random variable with parameter $p \in [0, 1]$, i.e.,

$$X = \begin{cases} 1 & \text{with probability } p, \\ 0 & \text{with probability } 1 - p. \end{cases}$$

- $X \sim \text{Binom}(n, p)$: X is a binomial random variable with parameters $n \geq 1$ and $p \in [0, 1]$, i.e.,

$$p_X(k) = \binom{n}{k} p^k (1 - p)^{n-k}, \quad k \in [0 : n].$$

- $X \sim \text{Unif}(\mathcal{A})$: X is a discrete uniform random variable over a finite set $\mathcal{A}$.
  $X \sim \text{Unif}[i : j]$ for integers $j > i$: X is a discrete uniform random variable over $[i : j]$.
- $X \sim \text{Unif}[a, b]$ for $b > a$: X is a continuous uniform random variable over $[a, b]$.
- $X \sim \text{N}(\mu, \sigma^2)$: X is a Gaussian random variable with mean μ and variance σ^2.
  $Q(x) = \mathsf{P}\{X > x\}$, $x \in \mathbb{R}$, where $X \sim \text{N}(0, 1)$.
- $\mathbf{X} = X^n \sim \text{N}(\boldsymbol{\mu}, K)$: $\mathbf{X}$ is a Gaussian random vector with mean vector $\boldsymbol{\mu}$ and covariance matrix K, i.e.,

$$f(\mathbf{x}) = \frac{1}{\sqrt{(2\pi)^n |K|}} e^{-\frac{1}{2}(\mathbf{x}-\boldsymbol{\mu})^T K^{-1} (\mathbf{x}-\boldsymbol{\mu})}.$$

We use the notation $\{X_i\} = (X_1, X_2, \ldots)$ to denote a discrete-time random process. The following notation is used for common random processes:

- $\{X_i\}$ is a $\text{Bern}(p)$ process means that $(X_1, X_2, \ldots)$ is a sequence of independent and identically distributed (i.i.d.) $\text{Bern}(p)$ random variables.
- $\{X_i\}$ is a $\text{WGN}(P)$ process means that $(X_1, X_2, \ldots)$ is a sequence of i.i.d. $\text{N}(0, P)$ random variables. More generally, $\{X_i, Y_i\}$ is a 2-$\text{WGN}(P, \rho)$ process means that (X_1, Y_1), $(X_2, Y_2), \ldots$ are i.i.d. jointly Gaussian random variable pairs with $\mathsf{E}(X_1) = \mathsf{E}(Y_1) = 0$, $\mathsf{E}(X_1^2) = \mathsf{E}(Y_1^2) = P$, and correlation coefficient $\rho = \mathsf{E}(X_1 Y_1)/P$.

We say that $X \to Y \to Z$ form a Markov chain if $p(x, y, z) = p(x)p(y|x)p(z|y)$. More generally, we say that $X_1 \to X_2 \to X_3 \to \cdots$ form a Markov chain if $p(x_i|x^{i-1}) = p(x_i|x_{i-1})$ for $i \geq 2$.

Common Functions

The following functions are used frequently. The logarithm function log is assumed to be base 2 unless specified otherwise.

- Binary entropy function: $H(p) = -p \log p - \bar{p} \log \bar{p}$ for $p \in [0, 1]$.
- Gaussian capacity function: $\mathsf{C}(x) = (1/2) \log(1 + x)$ for $x \geq 0$.
- Quadratic Gaussian rate function: $\mathsf{R}(x) = \max\{(1/2) \log x, \, 0\} = (1/2)[\log x]^+$.

ϵ–δ Notation

We use $\epsilon, \epsilon' > 0$ exclusively to denote "small" constants such that $\epsilon' < \epsilon$. We use $\delta(\epsilon) > 0$ to denote a function of ϵ that tends to zero as $\epsilon \to 0$. When there are multiple such functions $\delta_1(\epsilon), \delta_2(\epsilon), \ldots, \delta_k(\epsilon)$, we denote them all by a generic function $\delta(\epsilon)$ that tends to zero as $\epsilon \to 0$ with the understanding that $\delta(\epsilon) = \max\{\delta_1(\epsilon), \delta_2(\epsilon), \ldots, \delta_k(\epsilon)\}$. Similarly, we use $\epsilon_n \geq 0$ to denote a generic function of n that tends to zero as $n \to \infty$.

We say that $a_n \doteq 2^{nb}$ for some constant b if there exists some $\delta(\epsilon)$ (with ϵ defined in the context) such that for n sufficiently large,

$$2^{n(b-\delta(\epsilon))} \leq a_n \leq 2^{n(b+\delta(\epsilon))}.$$

Matrices

We use uppercase letters $A, B, \ldots$ to denote matrices. The entry in the i-th row and the j-th column of a matrix A is denoted by $A(i, j)$ or A_{ij}. A transpose of a matrix A is denoted by A^T, i.e., $A^T(i, j) = A(j, i)$. We use $\mathrm{diag}(a_1, a_2, \ldots, a_d)$ to denote a $d \times d$ diagonal matrix with diagonal elements $a_1, a_2, \ldots, a_d$. The $d \times d$ identity matrix is denoted by I_d. The subscript d is omitted when it is clear from the context. For a square matrix A, $|A| = \det(A)$ denotes the determinant of A and $\mathrm{tr}(A)$ denotes its trace.

A symmetric matrix A is said to be positive definite (denoted by $A \succ 0$) if $\mathbf{x}^T A \mathbf{x} > 0$ for all $\mathbf{x} \neq 0$. If instead $\mathbf{x}^T A \mathbf{x} \geq 0$ for all $\mathbf{x} \neq 0$, then the matrix A is said to be positive semidefinite (denoted by $A \succeq 0$). For symmetric matrices A and B of the same dimension, $A \succ B$ means that $A - B \succ 0$ and $A \succeq B$ means that $A - B \succeq 0$.

A singular value decomposition of an $r \times t$ matrix G of rank d is given by $G = \Phi \Gamma \Psi^T$, where Φ is an $r \times d$ matrix with $\Phi^T \Phi = I_d$, Ψ is a $t \times d$ matrix with $\Psi^T \Psi = I_d$, and $\Gamma = \mathrm{diag}(\gamma_1, \ldots, \gamma_d)$ is a $d \times d$ positive diagonal matrix.

For a symmetric positive semidefinite matrix K with an eigenvalue decomposition $K = \Phi \Lambda \Phi^T$, we define its symmetric square root as $K^{1/2} = \Phi \Lambda^{1/2} \Phi^T$, where $\Lambda^{1/2}$ is a diagonal matrix with diagonal elements $\sqrt{\Lambda_{ii}}$. Note that $K^{1/2}$ is symmetric positive definite with $K^{1/2} K^{1/2} = K$. We define the symmetric square root inverse $K^{-1/2}$ of a symmetric positive definite matrix K as the symmetric square root of K^{-1}.

Order Notation

Let $g_1(N)$ and $g_2(N)$ be nonnegative functions on natural numbers.

- $g_1(N) = o(g_2(N))$ means that $g_1(N)/g_2(N)$ tends to zero as $N \to \infty$.
- $g_1(N) = O(g_2(N))$ means that there exist a constant a and an integer n_0 such that $g_1(N) \leq a g_2(N)$ for all $N > n_0$.
- $g_1(N) = \Omega(g_2(N))$ means that $g_2(N) = O(g_1(N))$.
- $g_1(N) = \Theta(g_2(N))$ means that $g_1(N) = O(g_2(N))$ and $g_2(N) = O(g_1(N))$.

CHAPTER 1

Introduction

We introduce the general problem of optimal information flow in networks, which is the focus of network information theory. We then give a preview of the book with pointers to where the main results can be found.

1.1 NETWORK INFORMATION FLOW PROBLEM

A networked system consists of a set of information sources and communication nodes connected by a network as depicted in Figure 1.1. Each node observes one or more sources and wishes to reconstruct other sources or to compute a function based on all the sources. To perform the required task, the nodes communicate with each other over the network.

- What is the limit on the amount of communication needed?
- How can this limit be achieved?

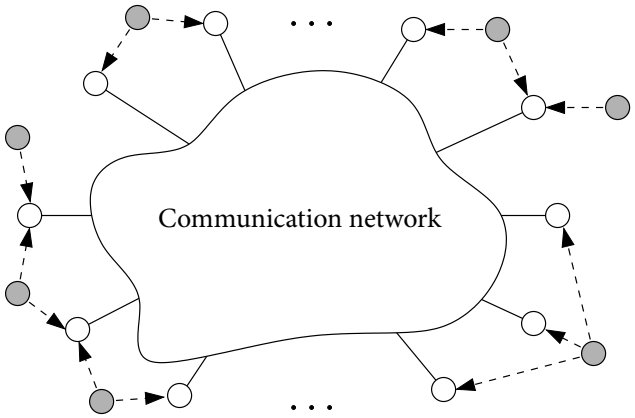


Figure 1.1. Elements of a networked system. The information sources (shaded circles) may be data, video, sensor measurements, or biochemical signals; the nodes (empty circles) may be computers, handsets, sensor nodes, or neurons; and the network may be a wired network, a wireless cellular or ad-hoc network, or a biological network.

These information flow questions have been answered satisfactorily for graphical unicast (single-source single-destination) networks and for point-to-point communication systems.

1.2 MAX-FLOW MIN-CUT THEOREM

Consider a *graphical* (wired) network, such as the Internet or a distributed storage system, modeled by a directed graph $(\mathcal{N}, \mathcal{E})$ with link capacities C_{jk} bits from node j to node k as depicted in Figure 1.2. Assume a unicast communication scenario in which source node 1 wishes to communicate an R-bit message M to destination node N. What is the network capacity C, that is, the maximum number of bits R that can be communicated reliably?

The answer is given by the *max-flow min-cut theorem* due to Ford and Fulkerson (1956) and Elias, Feinstein, and Shannon (1956). They showed that the capacity (maximum flow) is equal to the minimum cut capacity, i.e.,

$$C = \min_{\mathcal{S} \subset \mathcal{N}: 1 \in \mathcal{S},\, N \in \mathcal{S}^c} C(\mathcal{S}),$$

where $C(\mathcal{S}) = \sum_{j \in \mathcal{S},\, k \in \mathcal{S}^c} C_{jk}$ is the capacity of the cut $(\mathcal{S}, \mathcal{S}^c)$. They also showed that the capacity is achieved without errors using simple routing at the intermediate (relay) nodes, that is, the incoming bits at each node are forwarded over its outgoing links. Hence, under this networked system model, information can be treated as a commodity to be shipped over a transportation network or electricity to be delivered over a power grid.

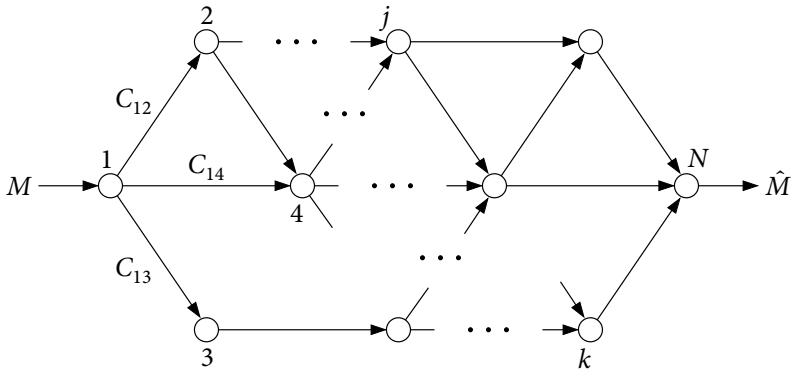


Figure 1.2. Graphical single-source single-destination network.

The max-flow min-cut theorem is discussed in more detail in Chapter 15.

1.3 POINT-TO-POINT INFORMATION THEORY

The graphical unicast network model captures the topology of a point-to-point network with idealized source and communication link models. At the other extreme, Shannon

(1948, 1959) studied communication and compression over a single link with more complex source and link (channel) models. He considered the communication system architecture depicted in Figure 1.3, where a sender wishes to communicate a k-symbol source sequence U^k to a receiver over a noisy channel. To perform this task, Shannon proposed a general *block coding* scheme, where the source sequence is mapped by an encoder into an n-symbol input sequence $X^n(U^k)$ and the received channel output sequence Y^n is mapped by a decoder into an estimate (reconstruction) sequence $\hat{U}^k(Y^n)$. He simplified the analysis of this system by proposing simple discrete memoryless models for the source and the noisy channel, and by using an *asymptotic* approach to characterize the necessary and sufficient condition for reliable communication.

Figure 1.3. Shannon's model of a point-to-point communication system.

Shannon's ingenious formulation of the point-to-point communication problem led to the following four fundamental theorems.

Channel coding theorem. Suppose that the source is a maximally compressed k-bit message M as in the graphical network case and that the channel is discrete and memoryless with input X, output Y, and conditional probability $p(y|x)$ that specifies the probability of receiving the symbol y when x is transmitted. The decoder wishes to find an estimate $\hat{M}$ of the message such that the probability of decoding error $\mathsf{P}\{\hat{M} \neq M\}$ does not exceed a prescribed value P_e. The general problem is to find the tradeoff between the number of bits k, the block length n, and the probability of error P_e.

This problem is intractable in general. Shannon (1948) realized that the difficulty lies in analyzing the system for any given finite block length n and reformulated the problem as one of finding the *channel capacity* C, which is the maximum communication rate $R = k/n$ in bits per channel transmissions such that the probability of error can be made arbitrarily small when the block length n is sufficiently large. He established a simple and elegant characterization of the channel capacity C in terms of the maximum of the mutual information $I(X;Y)$ between the channel input X and output Y:

$$C = \max_{p(x)} I(X;Y) \quad \text{bits/transmission.}$$

(See Section 2.3 for the definition of mutual information and its properties.) Unlike the graphical network case, however, capacity is achieved only *asymptotically* error-free and using sophisticated coding.

Lossless source coding theorem. As a "dual" to channel coding, consider the following lossless data compression setting. The sender wishes to communicate (store) a source sequence *losslessly* to a receiver over a *noiseless* binary channel (memory) with the minimum number of bits. Suppose that the source U is discrete and memoryless, that is, it

generates an i.i.d. sequence U^k. The sender encodes U^k at rate $R = n/k$ bits per source symbol into an n-bit index $M(U^k)$ and sends it over the channel. Upon receiving the index M, the decoder finds an estimate $\hat{U}^k(M)$ of the source sequence such that the probability of error $\mathsf{P}\{\hat{U}^k \neq U^k\}$ is less than a prescribed value. Shannon again formulated the problem as one of finding the minimum lossless compression rate R^* when the block length is arbitrarily large, and showed that it is characterized by the entropy of U:

$$R^* = H(U) \quad \text{bits/symbol.}$$

(See Section 2.1 for the definition of entropy and its properties.)

Lossy source coding theorem. Now suppose U^k is to be sent over the noiseless binary channel such that the receiver can reconstruct it with some distortion instead of losslessly. Shannon assumed the per-letter distortion $(1/k)\sum_{i=1}^{k} \mathsf{E}(d(U_i, \hat{U}_i))$, where $d(u, \hat{u})$ is a measure of the distortion between the source symbol u and the reconstruction symbol $\hat{u}$. He characterized the *rate–distortion function* $R(D)$, which is the optimal tradeoff between the rate $R = n/k$ and the desired distortion D, as the minimum of the mutual information between U and $\hat{U}$:

$$R(D) = \min_{p(\hat{u}|u):\mathsf{E}(d(U,\hat{U}))\le D} I(U; \hat{U}) \quad \text{bits/symbol.}$$

Source–channel separation theorem. Now we return to the general point-to-point communication system shown in Figure 1.3. Let C be the capacity of the discrete memoryless channel (DMC) and $R(D)$ be the rate–distortion function of the discrete memoryless source (DMS), and assume for simplicity that $k = n$. What is the necessary and sufficient condition for communicating the DMS over the DMC with a prescribed distortion D? Shannon (1959) showed that $R(D) \le C$ is necessary. Since $R(D) < C$ is sufficient by the lossy source coding and channel coding theorems, *separate* source coding and channel coding achieves the fundamental limit. Although this result holds only when the code block length is unbounded, it asserts that using bits as a "universal" interface between sources and channels—the basis for digital communication—is essentially optimal.

We discuss the above results in detail in Chapter 3. Shannon's asymptotic approach to network performance analysis will be adopted throughout the book.

1.4 NETWORK INFORMATION THEORY

The max-flow min-cut theorem and Shannon's point-to-point information theory have had a major impact on communication and networking. However, the simplistic model of a networked information processing system as a single source–destination pair communicating over a noisy channel or a graphical network does not capture many important aspects of real-world networks:

- Networked systems have multiple sources and destinations.
- The task of the network is often to compute a function or to make a decision.

- Wireless communication uses a shared broadcast medium.
- Networked systems involve complex tradeoffs between competition for resources and cooperation for the common good.
- Many networks allow for feedback and interactive communication.
- Source–channel separation does not hold for networks in general.
- Network security is often a primary concern.
- Data from the sources is often bursty and network topology evolves dynamically.

Network information theory aims to answer the aforementioned information flow questions while capturing some of these aspects of real-world networks. In the following, we illustrate some of the achievements of this theory using examples from the book.

1.4.1 Multiple Sources and Destinations

Coding for networks with many sources and destinations requires techniques beyond routing and point-to-point source/channel coding. Consider the following settings.

Graphical multicast network. Suppose we wish to send a movie over the Internet to multiple destinations (multicast). Unlike the unicast case, routing is not optimal in general even if we model the Internet by a graphical network. Instead, we need to use *coding* of incoming packets at the relay nodes.

We illustrate this fact via the famous "butterfly network" shown in Figure 1.4, where source node 1 wishes to send a 2-bit message $(M_1, M_2) \in \{0, 1\}^2$ to destination nodes 6 and 7. Assume link capacities $C_{jk} = 1$ for all edges (j, k). Note that using routing only, both M_1 and M_2 must be sent over the edge $(4, 5)$, and hence the message cannot be communicated to both destination nodes.

However, if we allow the nodes to perform simple modulo-2 sum operations in addition to routing, the 2-bit message can be communicated to both destinations. As illustrated in Figure 1.5, relay nodes 2, 3, and 5 forward multiple copies of their incoming bits,

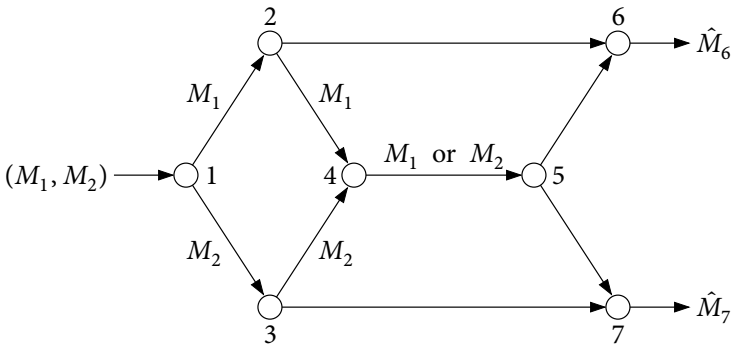


Figure 1.4. Butterfly network. The 2-bit message (M_1, M_2) cannot be sent using routing to both destination nodes 6 and 7.

and relay node 4 sends the modulo-2 sum of M_1 and M_2. Using this simple scheme, both destination nodes 6 and 7 can recover the message error-free.

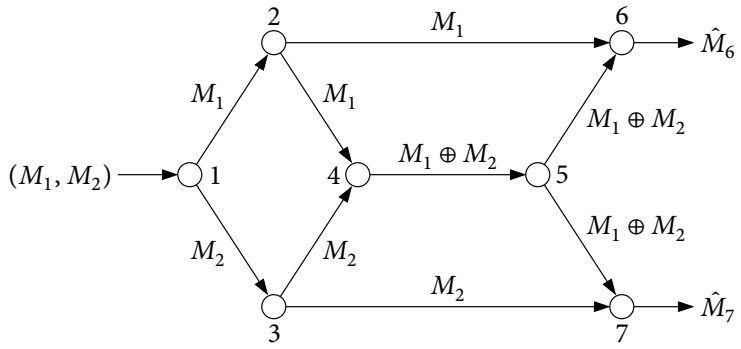


Figure 1.5. The 2-bit message can be sent to destination nodes 6 and 7 using linear network coding.

In Chapter 15, we show that linear network coding, which is a generalization of this simple scheme, achieves the capacity of an arbitrary graphical multicast network. Extensions of this multicast setting to lossy source coding are discussed in Chapters 13 and 20.

Distributed compression. Suppose that a sensor network is used to measure the temperature over a geographical area. The output from each sensor is compressed and sent to a base station. Although compression is performed separately on each sensor output, it turns out that using point-to-point compression is not optimal when the sensor outputs are *correlated*, for example, because the sensors are located close to each other.

Consider the distributed lossless compression system depicted in Figure 1.6. Two sequences X_1^n and X_2^n are drawn from correlated discrete memoryless sources $(X_1, X_2) \sim p(x_1, x_2)$ and compressed separately into an nR_1-bit index M_1 and an nR_2-bit index M_2, respectively. A receiver (base station) wishes to recover the source sequences from the index pair (M_1, M_2). What is the minimum sum-rate R_{sum}^*, that is, the minimum over $R_1 + R_2$ such that both sources can be reconstructed losslessly?

If each sender uses a point-to-point code, then by Shannon's lossless source coding theorem, the minimum lossless compression rates for the individual sources are $R_1^* = H(X_1)$ and $R_2^* = H(X_2)$, respectively; hence the resulting sum-rate is $H(X_1) + H(X_2)$. If instead the two sources are jointly encoded, then again by the lossless source coding theorem, the minimum lossless compression sum-rate is $H(X_1, X_2)$, which can be much smaller than the sum of the individual entropies. For example, let X_1 and X_2 be binary-valued sources with $p_{X_1,X_2}(0,0) = 0.495$, $p_{X_1,X_2}(0,1) = 0.005$, $p_{X_1,X_2}(1,0) = 0.005$, and $p_{X_1,X_2}(1,1) = 0.495$; hence, the sources have the same outcome 0.99 of the time. From the joint pmf, we see that X_1 and X_2 are both Bern(1/2) sources with entropy $H(X_1) = H(X_2) = 1$ bit per symbol. By comparison, their joint entropy $H(X_1, X_2) = 1.0808 \ll 2$ bits per symbol pair.

Slepian and Wolf (1973a) showed that $R_{\text{sum}}^* = H(X_1, X_2)$ and hence that the minimum

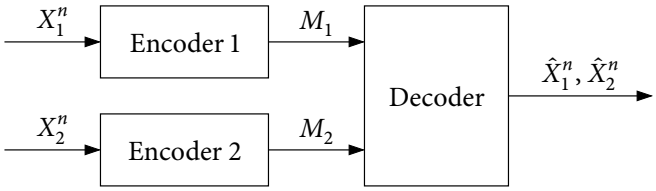


Figure 1.6. Distributed lossless compression system. Each source sequence X_j^n, $j = 1, 2$, is encoded into an index $M_j(X_j^n) \in [1 : 2^{nR_j}]$, and the decoder wishes to reconstruct the sequences losslessly from (M_1, M_2).

sum-rate for distributed compression is asymptotically the same as for centralized compression! This result is discussed in Chapter 10. Generalizations to distributed lossy compression are discussed in Chapters 11 and 12.

Communication for computing. Now suppose that the base station in the temperature sensor network wishes to compute the *average* temperature over the geographical area instead of the individual temperature values. What is the amount of communication needed?

While in some cases the rate requirement for computing a function of the sources is the same as that for recovering the sources themselves, it is sometimes significantly smaller. As an example, consider an n-round online game, where in each round Alice and Bob each select one card without replacement from a virtual hat with three cards labeled 1, 2, and 3. The one with the larger number wins. Let X^n and Y^n be the sequences of numbers on Alice and Bob's cards over the n rounds, respectively. Alice encodes her sequence X^n into an index $M \in [1 : 2^{nR}]$ and sends it to Bob so that he can find out who won in each round, that is, find an estimate $\hat{Z}^n$ of the sequence $Z_i = \max\{X_i, Y_i\}$ for $i \in [1 : n]$, as shown in Figure 1.7. What is the minimum communication rate R needed?

By the aforementioned Slepian–Wolf result, the minimum rate needed for Bob to reconstruct X is the conditional entropy $H(X|Y) = H(X, Y) - H(Y) = 2/3$ bit per round. By exploiting the structure of the function $Z = \max\{X, Y\}$, however, it can be shown that only 0.5409 bit per round is needed.

This card game example as well as general results on communication for computing are discussed in Chapter 21.

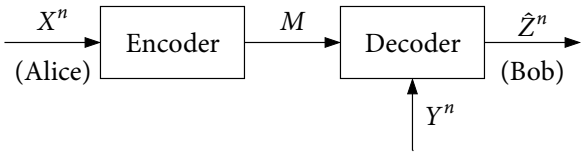


Figure 1.7. Online game setup. Alice has the card number sequence X^n and Bob has the card number sequence Y^n. Alice encodes her card number sequence into an index $M \in [1 : 2^{nR}]$ and sends it to Bob, who wishes to losslessly reconstruct the winner sequence Z^n.

1.4.2 Wireless Networks

Perhaps the most important practical motivation for studying network information theory is to deal with the special nature of wireless channels. We study models for wireless communication throughout the book.

The first and simplest wireless channel model we consider is the point-to-point Gaussian channel $Y = gX + Z$ depicted in Figure 1.8, where $Z \sim \mathrm{N}(0, N_0/2)$ is the receiver noise and g is the channel gain. Shannon showed that the capacity of this channel under a prescribed average transmission power constraint P on X, i.e., $\sum_{i=1}^{n} X_i^2 \le nP$ for each codeword X^n, has the simple characterization

$$C = \frac{1}{2}\log(1 + S) = \mathsf{C}(S),$$

where $S = 2g^2P/N_0$ is the received signal-to-noise ratio (SNR).

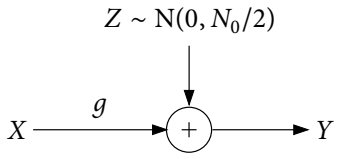


Figure 1.8. Gaussian point-to-point channel.

A wireless network can be turned into a set of separate point-to-point Gaussian channels via time or frequency division. This traditional approach to wireless communication, however, does not take full advantage of the broadcast nature of the wireless medium as illustrated in the following example.

Gaussian broadcast channel. The downlink of a wireless system is modeled by the Gaussian broadcast channel

$$Y_1 = g_1X + Z_1,$$
$$Y_2 = g_2X + Z_2,$$

as depicted in Figure 1.9. Here $Z_1 \sim \mathrm{N}(0, N_0/2)$ and $Z_2 \sim \mathrm{N}(0, N_0/2)$ are the receiver noise components, and $g_1^2 > g_2^2$, that is, the channel to receiver 1 is stronger than the channel to receiver 2. Define the SNRs for receiver $j = 1, 2$ as $S_j = 2g_j^2P/N_0$. Assume average power constraint P on X.

The sender wishes to communicate a message M_j at rate R_j to receiver j for $j = 1, 2$. What is the *capacity region* $\mathscr{C}$ of this channel, namely, the set of rate pairs (R_1, R_2) such that the probability of decoding error at both receivers can be made arbitrarily small as the code block length becomes large?

If we send the messages M_1 and M_2 in different time intervals or frequency bands, then we can reliably communicate at rate pairs in the "time-division region" $\mathscr{R}$ shown in Figure 1.9. Cover (1972) showed that higher rates can be achieved by adding the codewords for the two messages and sending this sum over the entire transmission block. The

stronger receiver 1 decodes for both codewords, while the weaker receiver 2 treats the other codeword as noise and decodes only for its own codeword. Using this *superposition coding* scheme, the sender can reliably communicate the messages at any rate pair in the capacity region $\mathscr{C}$ shown in Figure 1.9b, which is strictly larger than the time-division region $\mathscr{R}$.

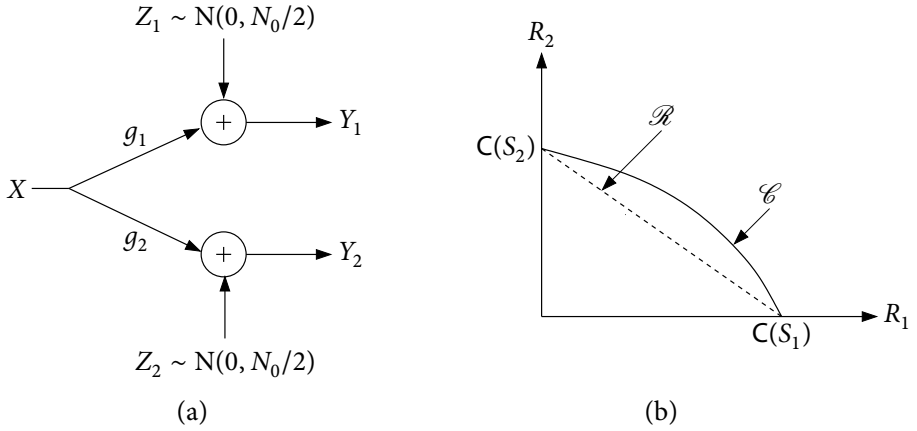


Figure 1.9. (a) Gaussian broadcast channel with SNRs $S_1 = g_1^2 P > g_2^2 P = S_2$. (b) The time-division inner bound $\mathscr{R}$ and the capacity region $\mathscr{C}$.

This superposition scheme and related results are detailed in Chapter 5. Similar improvements in rates can be achieved for the uplink (multiple access channel) and the intercell interference (interference channel), as discussed in Chapters 4 and 6, respectively.

Gaussian vector broadcast channel. Multiple transmitter and receiver antennas are commonly used to enhance the performance of wireless communication systems. Coding for these multiple-input multiple-output (MIMO) channels, however, requires techniques beyond single-antenna (scalar) channels. For example, consider the downlink of a MIMO wireless system modeled by the Gaussian vector broadcast channel

$$\mathbf{Y}_1 = G_1\mathbf{X} + \mathbf{Z}_1,$$
$$\mathbf{Y}_2 = G_2\mathbf{X} + \mathbf{Z}_2,$$

where G_1, G_2 are r-by-t channel gain matrices and $\mathbf{Z}_1 \sim \mathrm{N}(0, I_r)$ and $\mathbf{Z}_2 \sim \mathrm{N}(0, I_r)$ are noise components. Assume average power constraint P on $\mathbf{X}$. Note that unlike the single-antenna broadcast channel shown in Figure 1.9, in the vector case neither receiver is necessarily stronger than the other. The optimum coding scheme is based on the following *writing on dirty paper* result. Suppose we wish to communicate a message over a Gaussian vector channel,

$$\mathbf{Y} = G\mathbf{X} + \mathbf{S} + \mathbf{Z}$$

where $\mathbf{S} \sim \mathrm{N}(0, K_\mathbf{S})$ is an *interference* signal, which is independent of the Gaussian noise

$\mathbf{Z} \sim \mathrm{N}(0, I_r)$. Assume average power constraint P on $\mathbf{X}$. When the interference sequence $\mathbf{S}^n$ is available at the receiver, it can be simply subtracted from the received sequence and hence the channel capacity is the same as when there is no interference. Now suppose that the interference sequence is available only at the sender. Because of the power constraint, it is not always possible to presubtract the interference from the transmitted codeword. It turns out, however, that the *effect* of interference can still be completely canceled via judicious precoding and hence the capacity is again the same as that with no interference!

This scheme is applied to the Gaussian vector broadcast channel as follows.

- To communicate the message M_2 to receiver 2, consider the channel $\mathbf{Y}_2 = G_2\mathbf{X}_2 + G_2\mathbf{X}_1 + \mathbf{Z}_2$ with input $\mathbf{X}_2$, Gaussian interference $G_2\mathbf{X}_1$, and additive Gaussian noise $\mathbf{Z}_2$. Receiver 2 recovers M_2 while treating the interference signal $G_2\mathbf{X}_1$ as part of the noise.
- To communicate the message M_1 to receiver 1, consider the channel $\mathbf{Y}_1 = G_1\mathbf{X}_1 + G_1\mathbf{X}_2 + \mathbf{Z}_1$, with input $\mathbf{X}_1$, Gaussian interference $G_1\mathbf{X}_2$, and additive Gaussian noise $\mathbf{Z}_1$, where the interference sequence $G_1\mathbf{X}_2^n(M_2)$ is available at the sender. By the writing on dirty paper result, the transmission rate of M_1 can be as high as that for the channel $\mathbf{Y}_1' = G_1\mathbf{X}_1 + \mathbf{Z}_1$ without interference.

The writing on dirty paper result is discussed in detail in Chapter 7. The optimality of this scheme for the Gaussian vector broadcast channel is established in Chapter 9.

Gaussian relay channel. An ad-hoc or a mesh wireless network is modeled by a Gaussian *multihop* network in which nodes can act as relays to help other nodes communicate their messages. Again reducing such a network to a set of links using time or frequency division does not take full advantage of the shared wireless medium, and the rate can be greatly increased via node cooperation.

As a canonical example, consider the 3-node relay channel depicted in Figure 1.10a. Here node 2 is located on the line between nodes 1 and 3 as shown in Figure 1.10b. We assume that the channel gain from node k to node j is $g_{jk} = r_{jk}^{-3/2}$, where r_{jk} is the distance between nodes k and j. Hence $g_{31} = r_{31}^{-3/2}$, $g_{21} = r_{21}^{-3/2}$, and $g_{32} = (r_{31} - r_{21})^{-3/2}$. Assume average power constraint P on each of X_1 and X_2.

Suppose that sender node 1 wishes to communicate a message M to receiver node 3 with the help of relay node 2. On the one extreme, the sender and the receiver can communicate *directly* without help from the relay. On the other extreme, we can use a *multihop* scheme where the relay plays a pivotal role in the communication. In this commonly used scheme, the sender transmits the message to the relay in the first hop and the relay recovers the message and transmits it to the receiver concurrently in the second hop, causing interference to the first-hop communication. If the receiver is far away from the sender, that is, the distance r_{31} is large, this scheme performs well because the interference due to the concurrent transmission is weak. However, when r_{31} is not large, the interference can adversely affect the communication of the message.

In Chapter 16, we present several coding schemes that outperform both direct transmission and multihop.

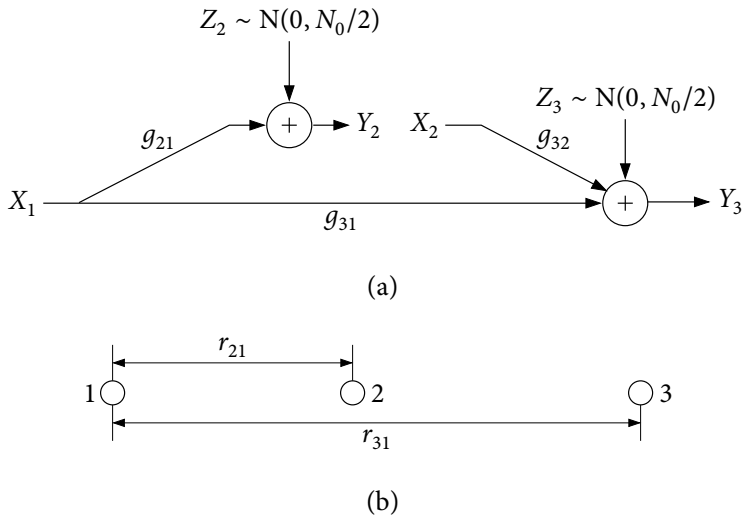


Figure 1.10. (a) Gaussian relay channel. (b) Node placements: relay node 2 is placed along the lines between sender node 1 and receiver node 2.

- *Decode–forward*. The direct transmission and multihop schemes are combined and further enhanced via coherent transmission by the sender and the relay. The receiver decodes for the signals from both hops instead of treating the transmission from the first hop as interference. Decode–forward performs well when the relay is closer to the sender, i.e., $r_{21} < (1/2)r_{31}$.
- *Compress–forward*. As an alternative to the "digital-to-digital" relay interface used in multihop and decode–forward, the compress–forward scheme uses an "analog-to-digital" interface in which the relay compresses the received signal and sends the compression index to the receiver. Compress–forward performs well when the relay is closer to the receiver.
- *Amplify–forward*. Decode–forward and compress–forward require sophisticated operations at the nodes. The amplify–forward scheme provides a much simpler "analog-to-analog" interface in which the relay scales the incoming signal and transmits it to the receiver. In spite of its simplicity, amplify–forward can outperform decode–forward when the relay is closer to the receiver.

The performance of the above relaying schemes are compared in Figure 1.11. In general, it can be shown that both decode–forward and compress–forward achieve rates within 1/2 bit of the capacity, while amplify–forward achieves rates within 1 bit of the capacity.

We extend the above coding schemes to general multihop networks in Chapters 18 and 19. In particular, we show that extending compress–forward leads to a noisy network coding scheme that includes network coding for graphical multicast networks as a special case. When applied to Gaussian multihop multicast networks, this noisy network coding scheme achieves within a constant gap of the capacity independent of network topology,

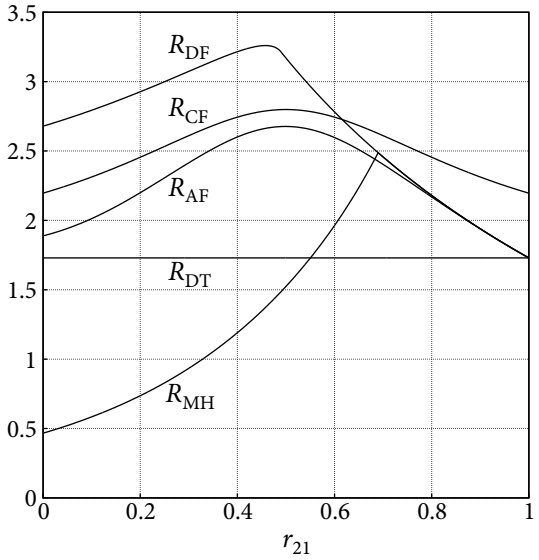


Figure 1.11. Comparison of the achievable rates for the Gaussian relay channel using direct transmission (R_{DT}), multihop (R_{MH}), decode–forward (R_{DF}), compress–forward (R_{CF}), and amplify–forward (R_{AF}) for $N_0/2 = 1$, $r_{31} = 1$ and $P = 10$.

channel parameters, and power constraints, while extensions of the other schemes do not yield such performance guarantees.

To study the effect of interference and path loss in large wireless networks, in Chapter 19 we also investigate how capacity scales with the network size. We show that relaying and spatial reuse of frequency/time can greatly increase the rates over naive direct transmission with time division.

Wireless fading channels. Wireless channels are *time varying* due to scattering of signals over multiple paths and user mobility. In Chapter 23, we study fading channel models that capture these effects by allowing the gains in the Gaussian channels to vary randomly with time. In some settings, channel capacity in the Shannon sense is not well defined. We introduce different coding approaches and corresponding performance metrics that are useful in practice.

1.4.3 Interactive Communication

Real-world networks allow for feedback and node interactions. Shannon (1956) showed that feedback does not increase the capacity of a memoryless channel. Feedback, however, can help simplify coding and improve reliability. This is illustrated in the following example.

Binary erasure channel with feedback. The binary erasure channel is a DMC with binary input $X \in \{0, 1\}$ and ternary output $Y \in \{0, 1, \mathrm{e}\}$. Each transmitted bit (0 or 1) is erased

(Y = e) with probability p. The capacity of this channel is $1 - p$ and achieving it requires sophisticated block coding. Now suppose that noiseless causal feedback from the receiver to the sender is present, that is, the sender at each time i has access to all previous received symbols Y^{i-1}. Then we can achieve the capacity simply by retransmitting each erased bit. Using this simple feedback scheme, on average $n = k/(1 - p)$ transmissions suffice to reliably communicate k bits of information.

Unlike point-to-point communication, feedback can achieve higher rates in networks with multiple senders/receivers.

Binary erasure multiple access channel with feedback. Consider the multiple access channel (MAC) with feedback depicted in Figure 1.12, where the channel inputs X_1 and X_2 are binary and the channel output $Y = X_1 + X_2$ is ternary, i.e., $Y \in \{0, 1, 2\}$. Suppose that senders 1 and 2 wish to communicate independent messages M_1 and M_2, respectively, to the receiver at the same rate R. Without feedback, the *symmetric capacity*, which is the maximum rate R, is $\max_{p(x_1)p(x_2)} H(Y) = 3/4$ bits/transmission.

Noiseless causal feedback allows the senders to *cooperate* in communicating their messages and hence to achieve higher symmetric rates than with no feedback. To illustrate such cooperation, suppose that each sender first transmits its k-bit message uncoded. On average $k/2$ bits are "erased" (that is, $Y = 0 + 1 = 1 + 0 = 1$ is received). Since the senders know through feedback the exact locations of the erasures as well as the corresponding message bits from both messages, they can cooperate to send the erased bits from the first message (which is sufficient to recover both messages). This cooperative retransmission requires $k/(2 \log 3)$ transmissions. Hence we can increase the symmetric rate to $R = k/(k + k/(2 \log 3)) = 0.7602$. This rate can be further increased to 0.7911 by using a more sophisticated coding scheme that sends new messages simultaneously with cooperative retransmissions.

In Chapter 17, we discuss the *iterative refinement* approach illustrated in the binary erasure channel example; the cooperative feedback approach for multiuser channels illustrated in the binary erasure MAC example; and the two-way channel. In Chapters 20

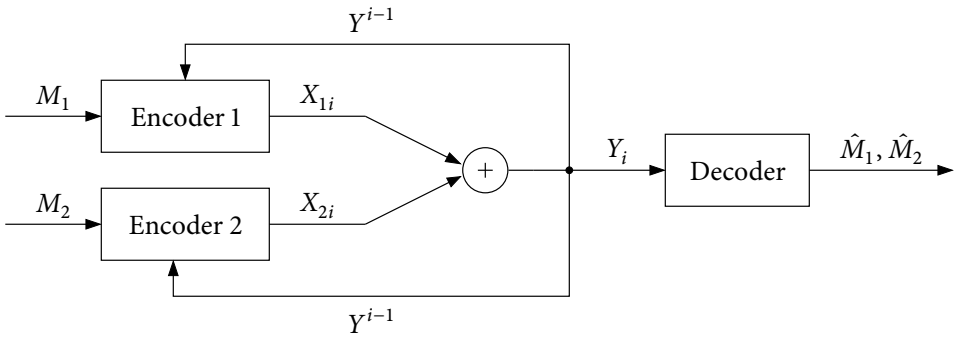


Figure 1.12. Feedback communication over a binary erasure MAC. The channel inputs X_{1i} and X_{2i} at time $i \in [1 : n]$ are functions of (M_1, Y^{i-1}) and (M_2, Y^{i-1}), respectively.

through 22, we show that interaction can also help in distributed compression, distributed computing, and secret communication.

1.4.4 Joint Source–Channel Coding

As we mentioned earlier, Shannon showed that separate source and channel coding is asymptotically optimal for point-to-point communication. It turns out that such separation does not hold in general for sending correlated sources over multiuser networks. In Chapter 14, we demonstrate this breakdown of separation for lossless communication of correlated sources over multiple access and broadcast channels. This discussion yields natural definitions of various notions of *common information* between two sources.

1.4.5 Secure Communication

Confidentiality of information is a crucial requirement in networking applications such as e-commerce. In Chapter 22, we discuss several coding schemes that allow a legitimate sender (Alice) to communicate a message reliably to a receiver (Bob) while keeping it secret (in a strong sense) from an eavesdropper (Eve). When the channel from Alice to Bob is stronger than that to Eve, a confidential message with a positive rate can be communicated reliably without a shared secret key between Alice and Bob. By contrast, when the channel from Alice to Bob is weaker than that to Eve, no confidential message can be communicated reliably. We show, however, that Alice and Bob can still agree on a secret key through interactive communication over a public (nonsecure) channel that Eve has complete access to. This key can then be used to communicate a confidential message at a nonzero rate.

1.4.6 Network Information Theory and Networking

Many aspects of real-world networks such as bursty data arrivals, random access, asynchrony, and delay constraints are not captured by the standard models of network information theory. In Chapter 24, we present several examples for which such networking issues have been successfully incorporated into the theory. We present a simple model for random medium access control (used for example in the ALOHA network) and show that a higher throughput can be achieved using a broadcasting approach instead of encoding the packets at a fixed rate. In another example, we establish the capacity region of the asynchronous multiple access channel.

1.4.7 Toward a Unified Network Information Theory

The above ideas and results illustrate some of the key ingredients of network information theory. The book studies this fascinating subject in a systematic manner, with the ultimate goal of developing a unified theory. We begin our journey with a review of Shannon's point-to-point information theory in the next two chapters.

CHAPTER 2

Information Measures and Typicality

We define entropy and mutual information and review their basic properties. We introduce basic inequalities involving these information measures, including Fano's inequality, Mrs. Gerber's lemma, the maximum differential entropy lemma, the entropy power inequality, the data processing inequality, and the Csiszár sum identity. We then introduce the notion of typicality adopted throughout the book. We discuss properties of typical sequences and introduce the typical average lemma, the conditional typicality lemma, and the joint typicality lemma. These lemmas as well as the aforementioned entropy and mutual information inequalities will play pivotal roles in the proofs of the coding theorems throughout the book.

2.1 ENTROPY

Let X be a discrete random variable with probability mass function (pmf) $p(x)$ (in short $X \sim p(x)$). The uncertainty about the outcome of X is measured by its *entropy* defined as

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log p(x) = -\mathsf{E}_X(\log p(X)).$$

For example, if X is a Bernoulli random variable with parameter $p = \mathsf{P}\{X = 1\} \in [0, 1]$ (in short $X \sim \text{Bern}(p)$), the entropy of X is

$$H(X) = -p \log p - (1 - p) \log(1 - p).$$

Since the Bernoulli random variable will be frequently encountered, we denote its entropy by the *binary entropy function* $H(p)$. The entropy function $H(X)$ is a nonnegative and concave function in $p(x)$. Thus, by Jensen's inequality (see Appendix B),

$$H(X) \le \log |\mathcal{X}|,$$

that is, the uniform pmf over $\mathcal{X}$ maximizes the entropy.

Let X be a discrete random variable and $g(X)$ be a function of X. Then

$$H(g(X)) \le H(X),$$

where the inequality holds with equality if g is one-to-one over the support of X, i.e., the set $\{x \in \mathcal{X} \colon p(x) > 0\}$.

Conditional entropy. Let $X \sim F(x)$ be an arbitrary random variable and $Y|\{X = x\} \sim p(y|x)$ be discrete for every x. Since $p(y|x)$ is a pmf, we can define the entropy function $H(Y|X = x)$ for every x. The *conditional entropy* (or *equivocation*) $H(Y|X)$ of Y given X is the average of $H(Y|X = x)$ over X, i.e.,

$$\begin{aligned} H(Y|X) &= \int H(Y|X = x)\, dF(x) \\ &= -\mathsf{E}_{X,Y}\big(\log p(Y|X)\big). \end{aligned}$$

Conditional entropy is a measure of the remaining uncertainty about the outcome of Y given the "observation" X. Again by Jensen's inequality,

$$H(Y|X) \le H(Y) \tag{2.1}$$

with equality if X and Y are independent.

Joint entropy. Let $(X, Y) \sim p(x, y)$ be a pair of discrete random variables. The *joint entropy* of X and Y is defined as

$$H(X, Y) = -\mathsf{E}\big(\log p(X, Y)\big).$$

Note that this is the same as the entropy of a single "large" random variable (X, Y). The chain rule for pmfs, $p(x, y) = p(x)p(y|x) = p(y)p(x|y)$, leads to a *chain rule* for joint entropy

$$H(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y).$$

By (2.1), it follows that

$$H(X, Y) \le H(X) + H(Y) \tag{2.2}$$

with equality if X and Y are independent.

The definition of entropy extends to discrete random vectors. Let $X^n \sim p(x^n)$. Then again by the chain rule for pmfs,

$$\begin{aligned} H(X^n) &= H(X_1) + H(X_2|X_1) + \cdots + H(X_n|X_1, \ldots, X_{n-1}) \\ &= \sum_{i=1}^{n} H(X_i|X_1, \ldots, X_{i-1}) \\ &= \sum_{i=1}^{n} H(X_i|X^{i-1}). \end{aligned}$$

Using induction and inequality (2.2), it follows that $H(X^n) \le \sum_{i=1}^{n} H(X_i)$ with equality if $X_1, X_2, \ldots, X_n$ are mutually independent.

Next, we consider the following two results that will be used in the converse proofs of many coding theorems. The first result relates equivocation to the "probability of error."

Fano's Inequality. Let $(X, Y) \sim p(x, y)$ and $P_e = \mathsf{P}\{X \neq Y\}$. Then

$$H(X|Y) \leq H(P_e) + P_e \log |\mathcal{X}| \leq 1 + P_e \log |\mathcal{X}|.$$

The second result provides a lower bound on the entropy of the modulo-2 sum of two binary random vectors.

Mrs. Gerber's Lemma (MGL). Let $H^{-1}\colon [0, 1] \to [0, 1/2]$ be the inverse of the binary entropy function, i.e., $H(H^{-1}(v)) = v$.

- Scalar MGL: Let X be a binary random variable and let U be an arbitrary random variable. If $Z \sim \text{Bern}(p)$ is independent of (X, U) and $Y = X \oplus Z$, then

$$H(Y|U) \geq H\big(H^{-1}(H(X|U)) * p\big).$$

- Vector MGL: Let X^n be a binary random vector and U be an arbitrary random variable. If Z^n is a vector of independent and identically distributed Bern(p) random variables independent of (X^n, U) and $Y^n = X^n \oplus Z^n$, then

$$\frac{H(Y^n|U)}{n} \geq H\left(H^{-1}\left(\frac{H(X^n|U)}{n}\right) * p\right).$$

The proof of this lemma follows by the convexity of the function $H(H^{-1}(v) * p)$ in v and using induction; see Problem 2.5.

Entropy rate of a stationary random process. Let $X = \{X_i\}$ be a stationary random process with X_i taking values in a finite alphabet $\mathcal{X}$. The *entropy rate* $\overline{H}(X)$ of the process X is defined as

$$\overline{H}(X) = \lim_{n\to\infty} \frac{1}{n} H(X^n) = \lim_{n\to\infty} H(X_n|X^{n-1}).$$

2.2 DIFFERENTIAL ENTROPY

Let X be a continuous random variable with probability density function (pdf) $f(x)$ (in short $X \sim f(x)$). The *differential entropy* of X is defined as

$$h(X) = -\int f(x) \log f(x)\, dx = -\mathsf{E}_X\big(\log f(X)\big).$$

For example, if $X \sim \text{Unif}[a, b]$, then

$$h(X) = \log(b - a).$$

As another example, if $X \sim \text{N}(\mu, \sigma^2)$, then

$$h(X) = \frac{1}{2} \log(2\pi e \sigma^2).$$

The differential entropy $h(X)$ is a concave function of $f(x)$. However, unlike entropy it is not always nonnegative and hence should not be interpreted directly as a measure of information. Roughly speaking, $h(X) + n$ is the entropy of the quantized version of X using equal-size intervals of length 2^{-n} (Cover and Thomas 2006, Section 8.3).

The differential entropy is invariant under translation but not under scaling.

- Translation: For any constant a, $h(X + a) = h(X)$.
- Scaling: For any nonzero constant a, $h(aX) = h(X) + \log |a|$.

The maximum differential entropy of a continuous random variable $X \sim f(x)$ under the average power constraint $\mathsf{E}(X^2) \le P$ is

$$\max_{f(x):\mathsf{E}(X^2)\le P} h(X) = \frac{1}{2}\log(2\pi e P)$$

and is attained when X is Gaussian with zero mean and variance P, i.e., $X \sim \mathrm{N}(0, P)$; see Remark 2.1 and Problem 2.6. Thus, for any $X \sim f(x)$,

$$h(X) = h(X - \mathsf{E}(X)) \le \frac{1}{2}\log(2\pi e \operatorname{Var}(X)). \tag{2.3}$$

Conditional differential entropy. Let $X \sim F(x)$ be an arbitrary random variable and $Y|\{X = x\} \sim f(y|x)$ be continuous for every x. The *conditional differential entropy* $h(Y|X)$ of Y given X is defined as

$$\begin{aligned} h(Y|X) &= \int h(Y|X = x)\, dF(x) \\ &= -\mathsf{E}_{X,Y}\big(\log f(Y|X)\big). \end{aligned}$$

As for the discrete case in (2.1), conditioning reduces entropy, i.e.,

$$h(Y|X) \le h(Y) \tag{2.4}$$

with equality if X and Y are independent.

We will often be interested in the sum of two random variables $Y = X + Z$, where X is an arbitrary random variable and Z is an independent continuous random variable with bounded pdf $f(z)$, for example, a Gaussian random variable. It can be shown in this case that the sum Y is a continuous random variable with well-defined density.

Joint differential entropy. The definition of differential entropy can be extended to a continuous random vector X^n with joint pdf $f(x^n)$ as

$$h(X^n) = -\mathsf{E}\big(\log f(X^n)\big).$$

For example, if X^n is a Gaussian random vector with mean $\boldsymbol{\mu}$ and covariance matrix K, i.e., $X^n \sim \mathrm{N}(\boldsymbol{\mu}, K)$, then

$$h(X^n) = \frac{1}{2}\log\big((2\pi e)^n |K|\big).$$

By the chain rule for pdfs and (2.4), we have

$$h(X^n) = \sum_{i=1}^{n} h(X_i|X^{i-1}) \le \sum_{i=1}^{n} h(X_i) \tag{2.5}$$

with equality if $X_1, \ldots, X_n$ are mutually independent. The translation and scaling properties of differential entropy continue to hold for the vector case.

- Translation: For any real-valued vector a^n, $h(X^n + a^n) = h(X^n)$.
- Scaling: For any real-valued nonsingular $n \times n$ matrix A,

$$h(AX^n) = h(X^n) + \log|\det(A)|\,.$$

The following lemma will be used in the converse proofs of Gaussian source and channel coding theorems.

Maximum Differential Entropy Lemma. Let $\mathbf{X} \sim f(x^n)$ be a random vector with covariance matrix $K_{\mathbf{X}} = \mathsf{E}[(\mathbf{X} - \mathsf{E}(\mathbf{X}))(\mathbf{X} - \mathsf{E}(\mathbf{X}))^T] \succ 0$. Then

$$h(\mathbf{X}) \le \frac{1}{2}\log\big((2\pi e)^n|K_{\mathbf{X}}|\big) \le \frac{1}{2}\log\big((2\pi e)^n|\mathsf{E}(\mathbf{X}\mathbf{X}^T)|\big), \tag{2.6}$$

where $\mathsf{E}(\mathbf{X}\mathbf{X}^T)$ is the correlation matrix of X^n. The first inequality holds with equality if and only if $\mathbf{X}$ is Gaussian and the second inequality holds with equality if and only if $\mathsf{E}(\mathbf{X}) = 0$. More generally, if $(\mathbf{X}, \mathbf{Y}) = (X^n, Y^k) \sim f(x^n, y^k)$ is a pair of random vectors $K_{\mathbf{X}|\mathbf{Y}} = \mathsf{E}[(\mathbf{X} - \mathsf{E}(\mathbf{X}|\mathbf{Y}))(\mathbf{X} - \mathsf{E}(\mathbf{X}|\mathbf{Y}))^T]$ is the covariance matrix of the error vector of the minimum mean squared error (MMSE) estimate of $\mathbf{X}$ given $\mathbf{Y}$, then

$$h(\mathbf{X}|\mathbf{Y}) \le \frac{1}{2}\log\big((2\pi e)^n|K_{\mathbf{X}|\mathbf{Y}}|\big) \tag{2.7}$$

with equality if $(\mathbf{X}, \mathbf{Y})$ is jointly Gaussian.

The proof of the upper bound in (2.6) is similar to the proof for the scalar case in (2.3); see Problem 2.7. The upper bound in (2.7) follows by applying (2.6) to $h(\mathbf{X}|\mathbf{Y} = \mathbf{y})$ for each $\mathbf{y}$ and Jensen's inequality using the concavity of $\log|K|$ in K. The upper bound on differential entropy in (2.6) can be further relaxed to

$$h(X^n) \le \frac{n}{2}\log\Big(2\pi e\Big(\frac{1}{n}\sum_{i=1}^{n}\mathrm{Var}(X_i)\Big)\Big) \le \frac{n}{2}\log\Big(2\pi e\Big(\frac{1}{n}\sum_{i=1}^{n}\mathsf{E}(X_i^2)\Big)\Big). \tag{2.8}$$

These inequalities can be proved using Hadamard's inequality or more directly using (2.5), (2.3), and Jensen's inequality.

The quantity $2^{2h(X^n)/n}/(2\pi e)$ is often referred to as the *entropy power* of the random vector X^n. The inequality in (2.8) shows that the entropy power is upper bounded by the average power. The following inequality shows that the entropy power of the sum of two

independent random vectors is lower bounded by the sum of their entropy powers. In a sense, this inequality is the continuous analogue of Mrs. Gerber's lemma.

Entropy Power Inequality (EPI).

- Scalar EPI: Let $X \sim f(x)$ and $Z \sim f(z)$ be independent random variables and $Y = X + Z$. Then
$$2^{2h(Y)} \geq 2^{2h(X)} + 2^{2h(Z)}$$
with equality if both X and Z are Gaussian.
- Vector EPI: Let $X^n \sim f(x^n)$ and $Z^n \sim f(z^n)$ be independent random vectors and $Y^n = X^n + Z^n$. Then
$$2^{2h(Y^n)/n} \geq 2^{2h(X^n)/n} + 2^{2h(Z^n)/n}$$
with equality if X^n and Z^n are Gaussian with $K_{\mathbf{X}} = aK_{\mathbf{Z}}$ for some scalar $a > 0$.
- Conditional EPI: Let X^n and Z^n be conditionally independent given an arbitrary random variable U, with conditional pdfs $f(x^n|u)$ and $f(z^n|u)$, and $Y^n = X^n + Z^n$. Then
$$2^{2h(Y^n|U)/n} \geq 2^{2h(X^n|U)/n} + 2^{2h(Z^n|U)/n}.$$

The scalar EPI can be proved, for example, using a sharp version of Young's inequality or de Bruijn's identity; see Bibliographic Notes. The proofs of the vector and conditional EPIs follow by the scalar EPI, the convexity of the function $\log(2^v + 2^w)$ in (v, w), and induction.

Differential entropy rate of a stationary random process. Let $X = \{X_i\}$ be a stationary continuous-valued random process. The *differential entropy rate* $\bar{h}(X)$ of the process X is defined as
$$\bar{h}(X) = \lim_{n\to\infty} \frac{1}{n} h(X^n) = \lim_{n\to\infty} h(X_n|X^{n-1}).$$

2.3 MUTUAL INFORMATION

Let $(X, Y) \sim p(x, y)$ be a pair of discrete random variables. The information about X obtained from the observation Y is measured by the *mutual information* between X and Y defined as
$$\begin{aligned} I(X;Y) &= \sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} \\ &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X) \\ &= H(X) + H(Y) - H(X,Y). \end{aligned}$$

The mutual information $I(X;Y)$ is a nonnegative function of $p(x, y)$, and $I(X;Y) = 0$ if and only if (iff) X and Y are independent. It is concave in $p(x)$ for a fixed $p(y|x)$, and convex in $p(y|x)$ for a fixed $p(x)$. Mutual information can be defined also for a pair of continuous random variables $(X, Y) \sim f(x, y)$ as

$$\begin{aligned} I(X;Y) &= \int f(x,y) \log \frac{f(x,y)}{f(x)f(y)}\, dxdy \\ &= h(X) - h(X|Y) \\ &= h(Y) - h(Y|X) \\ &= h(X) + h(Y) - h(X,Y). \end{aligned}$$

Similarly, let $X \sim p(x)$ be a discrete random variable and $Y|\{X = x\} \sim f(y|x)$ be continuous for every x. Then

$$I(X;Y) = h(Y) - h(Y|X) = H(X) - H(X|Y).$$

In general, mutual information can be defined for an *arbitrary* pair of random variables (Pinsker 1964) as

$$I(X;Y) = \int \log \frac{d\mu(x,y)}{d(\mu(x)\times\mu(y))}\, d\mu(x,y),$$

where $d\mu(x, y)/d(\mu(x)\times\mu(y))$ is the *Radon–Nikodym derivative* (see, for example, Royden 1988) of the joint probability measure $\mu(x, y)$ with respect to the product probability measure $\mu(x)\times\mu(y)$. Equivalently, it can be expressed as

$$I(X;Y) = \sup_{\hat{x},\hat{y}} I(\hat{x}(X); \hat{y}(Y)),$$

where $\hat{x}(x)$ and $\hat{y}(y)$ are finite-valued functions, and the supremum is over all such functions. These definitions can be shown to include the above definitions of mutual information for discrete and continuous random variables as special cases (Gray 1990, Section 5) by considering

$$I(X;Y) = \lim_{j,k\to\infty} I([X]_j; [Y]_k),$$

where $[X]_j = \hat{x}_j(X)$ and $[Y]_k = \hat{y}_k(Y)$ can be any sequences of finite quantizations of X and Y, respectively, such that the quantization errors $(x - \hat{x}_j(x))$ and $(y - \hat{y}_k(y))$ tend to zero as $j, k \to \infty$ for every x, y.

Remark 2.1 (Relative entropy). Mutual information is a special case of the *relative entropy* (*Kullback–Leibler divergence*). Let P and Q be two probability measures such that P is absolutely continuous with respect to Q, then the relative entropy is defined as

$$D(P||Q) = \int \log \frac{dP}{dQ}\, dP,$$

where dP/dQ is the Radon–Nikodym derivative. Thus, mutual information $I(X;Y)$ is the relative entropy between the joint and product measures of X and Y. Note that by the convexity of $\log(1/x)$, $D(P||Q)$ is nonnegative and $D(P||Q) = 0$ iff $P = Q$.

Conditional mutual information. Let $(X, Y)|\{Z = z\} \sim F(x, y|z)$ and $Z \sim F(z)$. Denote the mutual information between X and Y given $\{Z = z\}$ by $I(X; Y|Z = z)$. Then the *conditional mutual information* $I(X; Y|Z)$ between X and Y given Z is defined as

$$I(X; Y|Z) = \int I(X; Y|Z = z)\, dF(z).$$

For $(X, Y, Z) \sim p(x, y, z)$,

$$\begin{aligned} I(X; Y|Z) &= H(X|Z) - H(X|Y, Z) \\ &= H(Y|Z) - H(Y|X, Z) \\ &= H(X|Z) + H(Y|Z) - H(X, Y|Z). \end{aligned}$$

The conditional mutual information $I(X; Y|Z)$ is nonnegative and is equal to zero iff X and Y are conditionally independent given Z, i.e., $X \to Z \to Y$ form a Markov chain. Note that unlike entropy, no general inequality relationship exists between the conditional mutual information $I(X; Y|Z)$ and the mutual information $I(X; Y)$. There are, however, two important special cases.

- Independence: If $p(x, y, z) = p(x)p(z)p(y|x, z)$, that is, if X and Z are independent, then
$$I(X; Y|Z) \geq I(X; Y).$$
This follows by the convexity of $I(X; Y)$ in $p(y|x)$ for a fixed $p(x)$.
- Conditional independence: If $Z \to X \to Y$ form a Markov chain, then
$$I(X; Y|Z) \leq I(X; Y).$$
This follows by the concavity of $I(X; Y)$ in $p(x)$ for a fixed $p(y|x)$.

The definition of mutual information can be extended to random vectors in a straightforward manner. In particular, we can establish the following useful identity.

Chain Rule for Mutual Information. Let $(X^n, Y) \sim F(x^n, y)$. Then

$$I(X^n; Y) = \sum_{i=1}^{n} I(X_i; Y|X^{i-1}).$$

The following inequality shows that processing cannot increase information.

Data Processing Inequality. If $X \to Y \to Z$ form a Markov chain, then

$$I(X; Z) \leq I(X; Y).$$

Consequently, for any function g, $I(X; g(Y)) \le I(X; Y)$, which implies the inequality in (2.2). To prove the data processing inequality, we use the chain rule to expand $I(X; Y, Z)$ in two ways as

$$\begin{aligned} I(X; Y, Z) &= I(X; Y) + I(X; Z|Y) = I(X; Y) \\ &= I(X; Z) + I(X; Y|Z) \ge I(X; Z). \end{aligned}$$

The chain rule can be also used to establish the following identity, which will be used in several converse proofs.

Csiszár Sum Identity. Let $(U, X^n, Y^n) \sim F(u, x^n, y^n)$. Then

$$\sum_{i=1}^{n} I(X_{i+1}^n; Y_i|Y^{i-1}, U) = \sum_{i=1}^{n} I(Y^{i-1}; X_i|X_{i+1}^n, U),$$

where $X_{n+1}^n, Y^0 = \emptyset$.

2.4 TYPICAL SEQUENCES

Let x^n be a sequence with elements drawn from a finite alphabet $\mathcal{X}$. Define the *empirical pmf* of x^n (also referred to as its *type*) as

$$\pi(x|x^n) = \frac{|\{i\colon x_i = x\}|}{n} \quad \text{for } x \in \mathcal{X}.$$

For example, if $x^n = (0, 1, 1, 0, 0, 1, 0)$, then

$$\pi(x|x^n) = \begin{cases} 4/7 & \text{for } x = 0, \\ 3/7 & \text{for } x = 1. \end{cases}$$

Let $X_1, X_2, \ldots$ be a sequence of independent and identically distributed (i.i.d.) random variables with $X_i \sim p_X(x_i)$. Then by the (weak) law of large numbers (LLN), for each $x \in \mathcal{X}$,

$$\pi(x|X^n) \to p(x) \quad \text{in probability.}$$

Thus, with high probability, the random empirical pmf $\pi(x|X^n)$ does not deviate much from the true pmf $p(x)$. For $X \sim p(x)$ and $\epsilon \in (0, 1)$, define the set of ϵ-typical n-sequences x^n (or the typical set in short) as

$$\mathcal{T}_\epsilon^{(n)}(X) = \left\{x^n\colon |\pi(x|x^n) - p(x)| \le \epsilon p(x) \text{ for all } x \in \mathcal{X}\right\}.$$

When it is clear from the context, we will use $\mathcal{T}_\epsilon^{(n)}$ instead of $\mathcal{T}_\epsilon^{(n)}(X)$. The following simple fact is a direct consequence of the definition of the typical set.

Typical Average Lemma. Let $x^n \in \mathcal{T}_\epsilon^{(n)}(X)$. Then for any nonnegative function $g(x)$ on $\mathcal{X}$,

$$(1-\epsilon)\,\mathsf{E}(g(X)) \le \frac{1}{n}\sum_{i=1}^{n} g(x_i) \le (1+\epsilon)\,\mathsf{E}(g(X)).$$

Typical sequences satisfy the following properties:

1. Let $p(x^n) = \prod_{i=1}^n p_X(x_i)$. Then for each $x^n \in \mathcal{T}_\epsilon^{(n)}(X)$,

$$2^{-n(H(X)+\delta(\epsilon))} \le p(x^n) \le 2^{-n(H(X)-\delta(\epsilon))},$$

where $\delta(\epsilon) = \epsilon H(X)$. This follows by the typical average lemma with $g(x) = -\log p(x)$.

2. The cardinality of the typical set is upper bounded as

$$\left|\mathcal{T}_\epsilon^{(n)}(X)\right| \le 2^{n(H(X)+\delta(\epsilon))}.$$

This can be shown by summing the lower bound in property 1 over the typical set.

3. If $X_1, X_2, \ldots$ are i.i.d. with $X_i \sim p_X(x_i)$, then by the LLN,

$$\lim_{n\to\infty} \mathsf{P}\{X^n \in \mathcal{T}_\epsilon^{(n)}(X)\} = 1.$$

4. The cardinality of the typical set is lower bounded as

$$\left|\mathcal{T}_\epsilon^{(n)}(X)\right| \ge (1-\epsilon)2^{n(H(X)-\delta(\epsilon))}$$

for n sufficiently large. This follows by property 3 and the upper bound in property 1.

The above properties are illustrated in Figure 2.1.

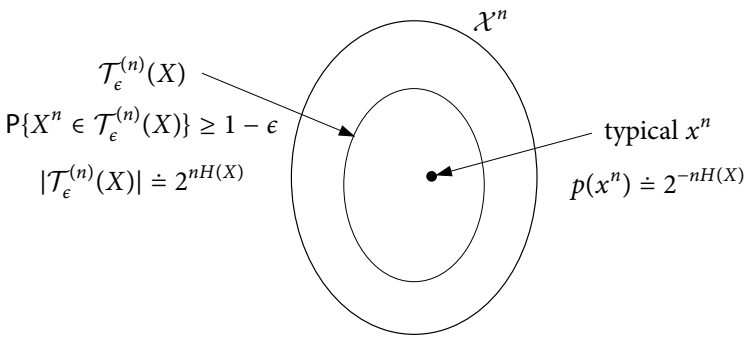


Figure 2.1. Properties of typical sequences. Here $X^n \sim \prod_{i=1}^n p_X(x_i)$.

2.5 JOINTLY TYPICAL SEQUENCES

The notion of typicality can be extended to multiple random variables. Let (x^n, y^n) be a pair of sequences with elements drawn from a pair of finite alphabets $(\mathcal{X}, \mathcal{Y})$. Define their joint empirical pmf (joint type) as

$$\pi(x, y|x^n, y^n) = \frac{|\{i\colon (x_i, y_i) = (x, y)\}|}{n} \quad \text{for } (x, y) \in \mathcal{X} \times \mathcal{Y}.$$

Let $(X, Y) \sim p(x, y)$. The set of jointly ϵ-typical n-sequences is defined as

$$\mathcal{T}_\epsilon^{(n)}(X, Y) = \{(x^n, y^n)\colon |\pi(x, y|x^n, y^n) - p(x, y)| \le \epsilon p(x, y) \text{ for all } (x, y) \in \mathcal{X} \times \mathcal{Y}\}.$$

Note that this is the same as the typical set for a single "large" random variable (X, Y), i.e., $\mathcal{T}_\epsilon^{(n)}(X, Y) = \mathcal{T}_\epsilon^{(n)}((X, Y))$. Also define the set of conditionally ϵ-typical n sequences as $\mathcal{T}_\epsilon^{(n)}(Y|x^n) = \{y^n\colon (x^n, y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y)\}$. The properties of typical sequences can be extended to jointly typical sequences as follows.

1. Let $(x^n, y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y)$ and $p(x^n, y^n) = \prod_{i=1}^n p_{X,Y}(x_i, y_i)$. Then
   (a) $x^n \in \mathcal{T}_\epsilon^{(n)}(X)$ and $y^n \in \mathcal{T}_\epsilon^{(n)}(Y)$,
   (b) $p(x^n) \doteq 2^{-nH(X)}$ and $p(y^n) \doteq 2^{-nH(Y)}$,
   (c) $p(x^n|y^n) \doteq 2^{-nH(X|Y)}$ and $p(y^n|x^n) \doteq 2^{-nH(Y|X)}$, and
   (d) $p(x^n, y^n) \doteq 2^{-nH(X,Y)}$.
2. $|\mathcal{T}_\epsilon^{(n)}(X, Y)| \doteq 2^{nH(X,Y)}$.
3. For every $x^n \in \mathcal{X}^n$,
$$\left|\mathcal{T}_\epsilon^{(n)}(Y|x^n)\right| \le 2^{n(H(Y|X)+\delta(\epsilon))},$$
   where $\delta(\epsilon) = \epsilon H(Y|X)$.
4. Let $X \sim p(x)$ and $Y = g(X)$. Let $x^n \in \mathcal{T}_\epsilon^{(n)}(X)$. Then $y^n \in \mathcal{T}_\epsilon^{(n)}(Y|x^n)$ iff $y_i = g(x_i)$ for $i \in [1 : n]$.

The following property deserves a special attention.

Conditional Typicality Lemma. Let $(X, Y) \sim p(x, y)$. Suppose that $x^n \in \mathcal{T}_{\epsilon'}^{(n)}(X)$ and $Y^n \sim p(y^n|x^n) = \prod_{i=1}^n p_{Y|X}(y_i|x_i)$. Then, for every $\epsilon > \epsilon'$,

$$\lim_{n\to\infty} \mathsf{P}\{(x^n, Y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y)\} = 1.$$

The proof of this lemma follows by the LLN. The details are given in Appendix 2A. Note that the condition $\epsilon > \epsilon'$ is crucial to applying the LLN because x^n could otherwise be on the boundary of $\mathcal{T}_\epsilon^{(n)}(X)$; see Problem 2.17.

The conditional typicality lemma implies the following additional property of jointly typical sequences.

5. If $x^n \in \mathcal{T}_{\epsilon'}^{(n)}(X)$ and $\epsilon' < \epsilon$, then for n sufficiently large,

$$\left|\mathcal{T}_{\epsilon}^{(n)}(Y|x^n)\right| \geq (1-\epsilon)2^{n(H(Y|X)-\delta(\epsilon))}.$$

The above properties of jointly typical sequences are illustrated in two different ways in Figure 2.2.

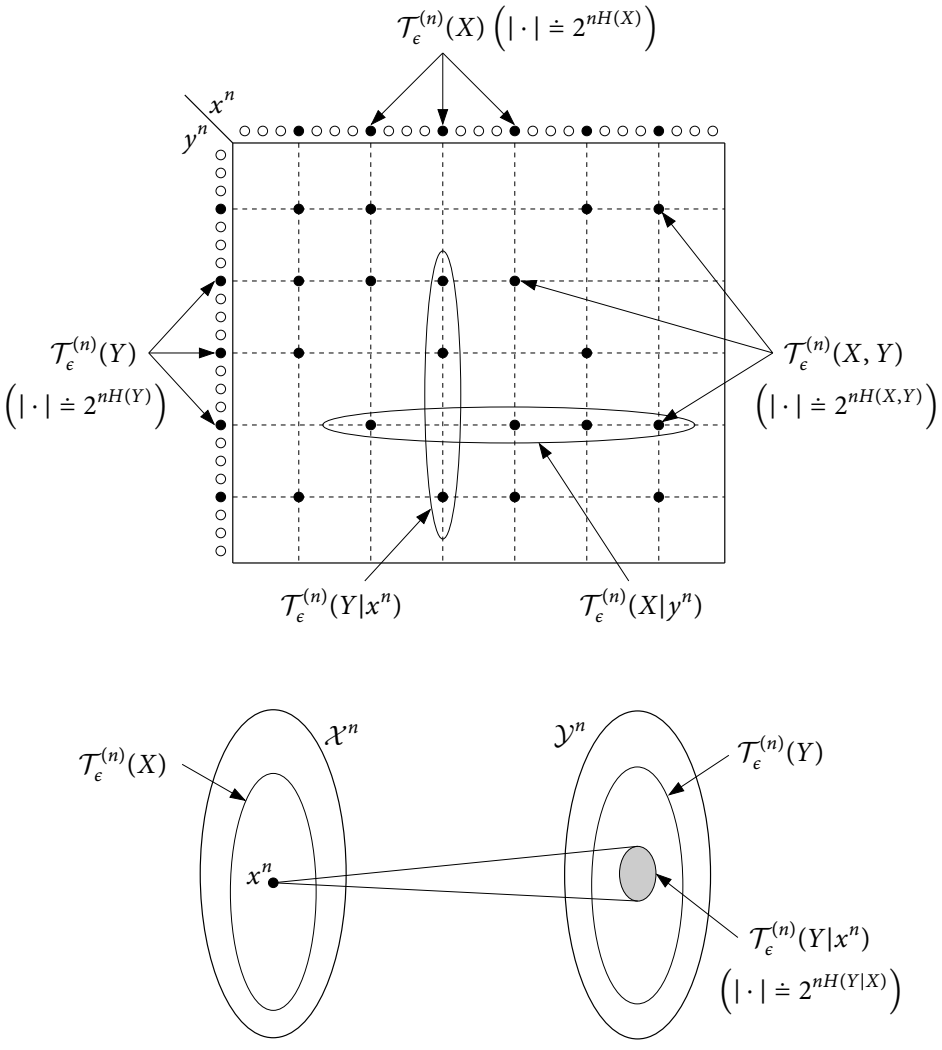


Figure 2.2. Properties of jointly typical sequences.

2.5.1 Joint Typicality for a Triple of Random Variables

Let $(X, Y, Z) \sim p(x, y, z)$. The set of jointly ϵ-typical (x^n, y^n, z^n) sequences is defined as

$$\mathcal{T}_\epsilon^{(n)}(X, Y, Z) = \{(x^n, y^n, z^n) \colon |\pi(x, y, z|x^n, y^n, z^n) - p(x, y, z)| \le \epsilon p(x, y, z) \text{ for all } (x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}\}.$$

Since this is equivalent to the typical set for a single "large" random variable (X, Y, Z) or a pair of random variables $((X, Y), Z)$, the properties of (jointly) typical sequences continue to hold. For example, suppose that $(x^n, y^n, z^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y, Z)$ and $p(x^n, y^n, z^n) = \prod_{i=1}^n p_{X,Y,Z}(x_i, y_i, z_i)$. Then

1. $x^n \in \mathcal{T}_\epsilon^{(n)}(X)$ and $(y^n, z^n) \in \mathcal{T}_\epsilon^{(n)}(Y, Z)$,
2. $p(x^n, y^n, z^n) \doteq 2^{-nH(X,Y,Z)}$,
3. $p(x^n, y^n|z^n) \doteq 2^{-nH(X,Y|Z)}$,
4. $|\mathcal{T}_\epsilon^{(n)}(X|y^n, z^n)| \le 2^{n(H(X|Y,Z)+\delta(\epsilon))}$, and
5. if $(y^n, z^n) \in \mathcal{T}_{\epsilon'}^{(n)}(Y, Z)$ and $\epsilon' < \epsilon$, then for n sufficiently large, $|\mathcal{T}_\epsilon^{(n)}(X|y^n, z^n)| \ge 2^{n(H(X|Y,Z)-\delta(\epsilon))}$.

The following two-part lemma will be used in the achievability proofs of many coding theorems.

Joint Typicality Lemma. Let $(X, Y, Z) \sim p(x, y, z)$ and $\epsilon' < \epsilon$. Then there exists $\delta(\epsilon) > 0$ that tends to zero as $\epsilon \to 0$ such that the following statements hold:

1. If $(\tilde{x}^n, \tilde{y}^n)$ is a pair of arbitrary sequences and $\tilde{Z}^n \sim \prod_{i=1}^n p_{Z|X}(\tilde{z}_i|\tilde{x}_i)$, then
$$\mathsf{P}\{(\tilde{x}^n, \tilde{y}^n, \tilde{Z}^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y, Z)\} \le 2^{-n(I(Y;Z|X)-\delta(\epsilon))}.$$
2. If $(x^n, y^n) \in \mathcal{T}_{\epsilon'}^{(n)}$ and $\tilde{Z}^n \sim \prod_{i=1}^n p_{Z|X}(\tilde{z}_i|x_i)$, then for n sufficiently large,
$$\mathsf{P}\{(x^n, y^n, \tilde{Z}^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y, Z)\} \ge 2^{-n(I(Y;Z|X)+\delta(\epsilon))}.$$

To prove the first statement, consider

$$\begin{aligned}
\mathsf{P}\{(\tilde{x}^n, \tilde{y}^n, \tilde{Z}^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y, Z)\} &= \sum_{\tilde{z}^n \in \mathcal{T}_\epsilon^{(n)}(Z|\tilde{x}^n, \tilde{y}^n)} p(\tilde{z}^n|\tilde{x}^n) \\
&\le \left|\mathcal{T}_\epsilon^{(n)}(Z|\tilde{x}^n, \tilde{y}^n)\right| \cdot 2^{-n(H(Z|X)-\epsilon H(Z|X))} \\
&\le 2^{n(H(Z|X,Y)+\epsilon H(Z|X,Y))} 2^{-n(H(Z|X)-\epsilon H(Z|X))} \\
&\le 2^{-n(I(Y;Z|X)-\delta(\epsilon))}.
\end{aligned}$$

Similarly, for every n sufficiently large,

$$\begin{aligned}\mathsf{P}\{(x^n, y^n, \tilde{Z}^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y, Z)\} &\geq \left|\mathcal{T}_\epsilon^{(n)}(Z|x^n, y^n)\right| \cdot 2^{-n(H(Z|X)+\epsilon H(Z|X))} \\ &\geq (1-\epsilon)2^{n(H(Z|X,Y)-\epsilon H(Z|X,Y))}2^{-n(H(Z|X)+\epsilon H(Z|X))} \\ &\geq 2^{-n(I(Y;Z|X)+\delta(\epsilon))},\end{aligned}$$

which proves the second statement.

Remark 2.2. As an application of the joint typicality lemma, it can be easily shown that if $(X^n, Y^n) \sim \prod_{i=1}^n p_{X,Y}(x_i, y_i)$ and $\tilde{Z}^n \,|\, \{X^n = x^n, Y^n = y^n\} \sim \prod_{i=1}^n p_{Z|X}(\tilde{z}_i|x_i)$, then

$$\mathsf{P}\{(X^n, Y^n, \tilde{Z}^n) \in \mathcal{T}_\epsilon^{(n)}\} \doteq 2^{-nI(Y;Z|X)}.$$

Other applications of the joint typicality lemma are given in Problem 2.14.

2.5.2 Multivariate Typical Sequences

Let $(X_1, X_2, \ldots, X_k) \sim p(x_1, x_2, \ldots, x_k)$ and $\mathcal{J}$ be a nonempty subset of $[1:k]$. Define the subtuple of random variables $X(\mathcal{J}) = (X_j\colon j \in \mathcal{J})$. For example, if $k = 3$ and $\mathcal{J} = \{1, 3\}$, then $X(\mathcal{J}) = (X_1, X_3)$. The set of ϵ-typical n-sequences $(x_1^n, x_2^n, \ldots, x_k^n)$ is defined as $\mathcal{T}_\epsilon^{(n)}(X_1, X_2, \ldots, X_k) = \mathcal{T}_\epsilon^{(n)}((X_1, X_2, \ldots, X_k))$, that is, as the typical set for a single random variable $(X_1, X_2, \ldots, X_k)$. We can similarly define $\mathcal{T}_\epsilon^{(n)}(X(\mathcal{J}))$ for every $\mathcal{J} \subseteq [1:k]$.

It can be easily checked that the properties of jointly typical sequences continue to hold by considering $X(\mathcal{J})$ as a single random variable. For example, if $(x_1^n, x_2^n, \ldots, x_k^n) \in \mathcal{T}_\epsilon^{(n)}(X_1, X_2, \ldots, X_k)$ and $p(x_1^n, x_2^n, \ldots, x_k^n) = \prod_{i=1}^n p_{X_1,X_2,\ldots,X_k}(x_{1i}, x_{2i}, \ldots, x_{ki})$, then for all $\mathcal{J}, \mathcal{J}' \subseteq [1:k]$,

1. $x^n(\mathcal{J}) \in \mathcal{T}_\epsilon^{(n)}(X(\mathcal{J}))$,
2. $p(x^n(\mathcal{J})|x^n(\mathcal{J}')) \doteq 2^{-nH(X(\mathcal{J})|X(\mathcal{J}'))}$,
3. $|\mathcal{T}_\epsilon^{(n)}(X(\mathcal{J})|x^n(\mathcal{J}'))| \leq 2^{n(H(X(\mathcal{J})|X(\mathcal{J}'))+\delta(\epsilon))}$, and
4. if $x^n(\mathcal{J}') \in \mathcal{T}_{\epsilon'}^{(n)}(X(\mathcal{J}'))$ and $\epsilon' < \epsilon$, then for n sufficiently large,

$$|\mathcal{T}_\epsilon^{(n)}(X(\mathcal{J})|x^n(\mathcal{J}'))| \geq 2^{n(H(X(\mathcal{J})|X(\mathcal{J}'))-\delta(\epsilon))}.$$

The conditional and joint typicality lemmas can be readily generalized to subsets $\mathcal{J}_1$, $\mathcal{J}_2$, and $\mathcal{J}_3$ and corresponding sequences $x^n(\mathcal{J}_1)$, $x^n(\mathcal{J}_2)$, and $x^n(\mathcal{J}_3)$ that satisfy similar conditions.

SUMMARY

- Entropy as a measure of information
- Mutual information as a measure of information transfer

- Key inequalities and identities:
  - Fano's inequality
  - Mrs. Gerber's lemma
  - Maximum differential entropy lemma
  - Entropy power inequality
  - Chain rules for entropy and mutual information
  - Data processing inequality
  - Csiszár sum identity
- Typical sequences:
  - Typical average lemma
  - Conditional typicality lemma
  - Joint typicality lemma

BIBLIOGRAPHIC NOTES

Shannon (1948) defined entropy and mutual information for discrete and continuous random variables, and provide justifications of these definitions in both axiomatic and operational senses. Many of the simple properties of these quantities, including the maximum entropy property of the Gaussian distribution, are also due to Shannon. Subsequently, Kolmogorov (1956) and Dobrushin (1959a) gave rigorous extensions of entropy and mutual information to abstract probability spaces.

Fano's inequality is due to Fano (1952). Mrs. Gerber's lemma is due to Wyner and Ziv (1973). Extensions of the MGL were given by Witsenhausen (1974), Witsenhausen and Wyner (1975), and Shamai and Wyner (1990).

The entropy power inequality has a longer history. It first appeared in Shannon (1948) without a proof. Full proofs were given subsequently by Stam (1959) and Blachman (1965) using de Bruijn's identity (Cover and Thomas 2006, Theorem 17.7.2). The EPI can be rewritten in the following equivalent inequality (Costa and Cover 1984). For a pair of independent random vectors $X^n \sim f(x^n)$ and $Z^n \sim f(z^n)$,

$$h(X^n + Z^n) \geq h(\tilde{X}^n + \tilde{Z}^n), \tag{2.9}$$

where $\tilde{X}^n$ and $\tilde{Z}^n$ are a pair of independent Gaussian random vectors with proportional covariance matrices, chosen so that $h(X^n) = h(\tilde{X}^n)$ and $h(Z^n) = h(\tilde{Z}^n)$. Now (2.9) can be proved by the strengthened version of Young's inequality (Beckner 1975, Brascamp and Lieb 1976); see, for example, Lieb (1978) and Gardner (2002). Recently, Verdú and Guo (2006) gave a simple proof by relating the minimum mean squared error (MMSE) and

mutual information in Gaussian channels; see Madiman and Barron (2007) for a similar proof from a different angle. Extensions of the EPI are given by Costa (1985), Zamir and Feder (1993), and Artstein, Ball, Barthe, and Naor (2004).

There are several notions of typicality in the literature. Our notion of typicality is that of *robust typicality* due to Orlitsky and Roche (2001). As is evident in the typical average lemma, it is often more convenient than the more widely known notion of *strong typicality* (Berger 1978, Csiszár and Körner 1981b) defined as

$$\mathcal{A}_\epsilon^{*(n)} = \left\{ x^n \colon |\pi(x|x^n) - p(x)| \le \frac{\epsilon}{|\mathcal{X}|} \text{ if } p(x) > 0,\ \pi(x|x^n) = 0 \text{ otherwise} \right\}.$$

Another widely used notion is *weak typicality* (Cover and Thomas 2006) defined as

$$\mathcal{A}_\epsilon^{(n)}(X) = \left\{ x^n \colon \left| -\frac{1}{n} \log p(x^n) - H(X) \right| \le \epsilon \right\}, \tag{2.10}$$

where $p(x^n) = \prod_{i=1}^n p_X(x_i)$. This is a weaker notion than the one we use, since $\mathcal{T}_\epsilon^{(n)} \subseteq \mathcal{A}_\delta^{(n)}$ for $\delta = \epsilon H(X)$, while in general for some $\epsilon > 0$ there is no $\delta' > 0$ such that $\mathcal{A}_{\delta'}^{(n)} \subseteq \mathcal{T}_\epsilon^{(n)}$. For example, every binary n-sequence is weakly typical with respect to the Bern(1/2) pmf, but not all of them are typical. Weak typicality is useful when dealing with discrete or continuous stationary ergodic processes because it is tightly coupled to the Shannon–McMillan–Breiman theorem (Shannon 1948, McMillan 1953, Breiman 1957, Barron 1985), commonly referred to as the *asymptotic equipartition property (AEP)*, which states that for a discrete stationary ergodic process $X = \{X_i\}$,

$$\lim_{n\to\infty} -\frac{1}{n} \log p(X^n) = \overline{H}(X).$$

However, we will encounter several coding schemes that require our notion of typicality. Note, for example, that the conditional typicality lemma fails to hold under weak typicality.

PROBLEMS

2.1. Prove Fano's inequality.

2.2. Prove the Csiszár sum identity.

2.3. Prove the properties of jointly typical sequences with $\delta(\epsilon)$ terms explicitly specified.

2.4. *Inequalities.* Label each of the following statements with $=$, $\le$, or $\ge$. Justify each answer.

(a) $H(X|Z)$ vs. $H(X|Y) + H(Y|Z)$.

(b) $h(X + Y)$ vs. $h(X)$, if X and Y are independent continuous random variables.

(c) $h(X + aY)$ vs. $h(X + Y)$, if $Y \sim \mathrm{N}(0, 1)$ is independent of X and $a \ge 1$.

(d) $I(X_1, X_2; Y_1, Y_2)$ vs. $I(X_1; Y_1) + I(X_2; Y_2)$, if $p(y_1, y_2|x_1, x_2) = p(y_1|x_1)p(y_2|x_2)$.

(e) $I(X_1, X_2; Y_1, Y_2)$ vs. $I(X_1; Y_1) + I(X_2; Y_2)$, if $p(x_1, x_2) = p(x_1)p(x_2)$.

(f) $I(aX + Y; bX)$ vs. $I(X + Y/a; X)$, if $a, b \neq 0$ and $Y \sim \mathrm{N}(0, 1)$ is independent of X.

2.5. *Mrs. Gerber's lemma.* Let $H^{-1}\colon [0, 1] \to [0, 1/2]$ be the inverse of the binary entropy function.

(a) Show that $H(H^{-1}(v) * p)$ is convex in v for every $p \in [0, 1]$.

(b) Use part (a) to prove the scalar MGL

$$H(Y|U) \geq H\big(H^{-1}(H(X|U)) * p\big).$$

(c) Use part (b) and induction to prove the vector MGL

$$\frac{H(Y^n|U)}{n} \geq H\left(H^{-1}\left(\frac{H(X^n|U)}{n}\right) * p\right).$$

2.6. *Maximum differential entropy.* Let $X \sim f(x)$ be a zero-mean random variable with finite variance and $X^* \sim f(x^*)$ be a zero-mean Gaussian random variable with the same variance as X.

(a) Show that

$$-\int f(x) \log f_{X^*}(x)\, dx = -\int f_{X^*}(x) \log f_{X^*}(x)\, dx = h(X^*).$$

(b) Using part (a) and the nonnegativity of relative entropy (see Remark 2.1), conclude that

$$h(X) = -D(f_X || f_{X^*}) - \int f(x) \log f_{X^*}(x)\, dx \leq h(X^*)$$

with equality iff X is Gaussian.

(c) Following similar steps, show that if $\mathbf{X} \sim f(\mathbf{x})$ is a zero-mean random vector and $\mathbf{X}^* \sim f(\mathbf{x}^*)$ is a zero-mean Gaussian random vector with the same covariance matrix, then

$$h(\mathbf{X}) \leq h(\mathbf{X}^*)$$

with equality iff $\mathbf{X}$ is Gaussian.

2.7. *Maximum conditional differential entropy.* Let $(\mathbf{X}, \mathbf{Y}) = (X^n, Y^k) \sim f(x^n, y^k)$ be a pair of random vectors with covariance matrices $K_{\mathbf{X}} = \mathsf{E}[(\mathbf{X} - \mathsf{E}(\mathbf{X}))(\mathbf{X} - \mathsf{E}(\mathbf{X}))^T]$ and $K_{\mathbf{Y}} = \mathsf{E}[(\mathbf{Y} - \mathsf{E}(\mathbf{Y}))(\mathbf{Y} - \mathsf{E}(\mathbf{Y}))^T]$, and crosscovariance matrix $K_{\mathbf{XY}} = \mathsf{E}[(\mathbf{X} - \mathsf{E}(\mathbf{X}))(\mathbf{Y} - \mathsf{E}(\mathbf{Y}))^T] = K_{\mathbf{YX}}^T$. Show that

$$h(\mathbf{X}|\mathbf{Y}) \leq \frac{1}{2} \log\big((2\pi e)^n |K_{\mathbf{X}} - K_{\mathbf{XY}} K_{\mathbf{Y}}^{-1} K_{\mathbf{YX}}|\big)$$

with equality if $(\mathbf{X}, \mathbf{Y})$ is jointly Gaussian.

2.8. *Hadamard's inequality.* Let $Y^n \sim \mathrm{N}(0, K)$. Use the fact that

$$h(Y^n) \le \frac{1}{2} \log\Big((2\pi e)^n \prod_{i=1}^{n} K_{ii} \Big)$$

to prove Hadamard's inequality

$$\det(K) \le \prod_{i=1}^{n} K_{ii}.$$

2.9. *Conditional entropy power inequality.* Let $X \sim f(x)$ and $Z \sim f(z)$ be independent random variables and $Y = X + Z$. Then by the EPI,

$$2^{2h(Y)} \ge 2^{2h(X)} + 2^{2h(Z)}$$

with equality iff both X and Z are Gaussian.

(a) Show that $\log(2^v + 2^w)$ is convex in (v, w).

(b) Let X^n and Z^n be conditionally independent given an arbitrary random variable U, with conditional densities $f(x^n|u)$ and $f(z^n|u)$, respectively. Use part (a), the scalar EPI, and induction to prove the conditional EPI

$$2^{2h(Y^n|U)/n} \ge 2^{2h(X^n|U)/n} + 2^{2h(Z^n|U)/n}.$$

2.10. *Entropy rate of a stationary source.* Let $X = \{X_i\}$ be a discrete stationary random process.

(a) Show that

$$\frac{H(X^n)}{n} \le \frac{H(X^{n-1})}{n-1} \quad \text{for } n = 2, 3, \ldots.$$

(b) Conclude that the entropy rate

$$\overline{H}(X) = \lim_{n\to\infty} \frac{H(X^n)}{n}$$

is well-defined.

(c) Show that for a continuous stationary process $Y = \{Y_i\}$,

$$\frac{h(Y^n)}{n} \le \frac{h(Y^{n-1})}{n-1} \quad \text{for } n = 2, 3, \ldots.$$

2.11. *Worst noise for estimation.* Let $X \sim \mathrm{N}(0, P)$ and Z be independent of X with zero mean and variance N. Show that the minimum mean squared error (MMSE) of estimating X given $X + Z$ is upper bounded as

$$\mathsf{E}\big[(X - \mathsf{E}(X|X+Z))^2\big] \le \frac{PN}{P+N}$$

with equality if Z is Gaussian. Thus, Gaussian noise is the worst noise if the input to the channel is Gaussian.

2.12. *Worst noise for information.* Let X and Z be independent, zero-mean random variables with variances P and N, respectively.

(a) Show that

$$h(X|X+Z) \le \frac{1}{2}\log\left(\frac{2\pi ePN}{P+N}\right)$$

with equality iff both X and Z are Gaussian. (Hint: Use the maximum differential entropy lemma or the EPI or Problem 2.11.)

(b) Let X^* and Z^* be independent zero-mean Gaussian random variables with variances P and N, respectively. Use part (a) to show that

$$I(X^*; X^*+Z^*) \le I(X^*; X^*+Z)$$

with equality iff Z is Gaussian. Thus, Gaussian noise is the worst noise when the input to an additive channel is Gaussian.

2.13. *Joint typicality.* Let $(X,Y) \sim p(x,y)$ and $\epsilon > \epsilon'$. Let $X^n \sim p(x^n)$ be an arbitrary random sequence and $Y^n|\{X^n = x^n\} \sim \prod_{i=1}^n p_{Y|X}(y_i|x_i)$. Using the conditional typicality lemma, show that

$$\lim_{n\to\infty} \mathsf{P}\{(X^n,Y^n) \in \mathcal{T}_\epsilon^{(n)} \,|\, X^n \in \mathcal{T}_{\epsilon'}^{(n)}\} = 1.$$

2.14. *Variations on the joint typicality lemma.* Let $(X,Y,Z) \sim p(x,y,z)$ and $0 < \epsilon' < \epsilon$. Prove the following statements.

(a) Let $(X^n,Y^n) \sim \prod_{i=1}^n p_{X,Y}(x_i,y_i)$ and $\tilde{Z}^n|\{X^n=x^n, Y^n=y^n\} \sim \prod_{i=1}^n p_{Z|X}(\tilde{z}_i|x_i)$, conditionally independent of Y^n given X^n. Then

$$\mathsf{P}\{(X^n,Y^n,\tilde{Z}^n) \in \mathcal{T}_\epsilon^{(n)}(X,Y,Z)\} \doteq 2^{-nI(Y;Z|X)}.$$

(b) Let $(x^n,y^n) \in \mathcal{T}_{\epsilon'}^{(n)}(X,Y)$ and $\tilde{Z}^n \sim \mathrm{Unif}(\mathcal{T}_\epsilon^{(n)}(Z|x^n))$. Then

$$\mathsf{P}\{(x^n,y^n,\tilde{Z}^n) \in \mathcal{T}_\epsilon^{(n)}(X,Y,Z)\} \doteq 2^{-nI(Y;Z|X)}.$$

(c) Let $x^n \in \mathcal{T}_{\epsilon'}^{(n)}(X)$, $\tilde{y}^n$ be an arbitrary sequence, and $\tilde{Z}^n \sim p(\tilde{z}^n|x^n)$, where

$$p(\tilde{z}^n|x^n) = \begin{cases} \dfrac{\prod_{i=1}^n p_{Z|X}(\tilde{z}_i|x_i)}{\sum_{z^n \in \mathcal{T}_\epsilon^{(n)}(Z|x^n)} \prod_{i=1}^n p_{Z|X}(z_i|x_i)} & \text{if } \tilde{z}^n \in \mathcal{T}_\epsilon^{(n)}(Z|x^n), \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\mathsf{P}\{(x^n,\tilde{y}^n,\tilde{Z}^n) \in \mathcal{T}_\epsilon^{(n)}(X,Y,Z)\} \le 2^{-n(I(Y;Z|X)-\delta(\epsilon))}.$$

(d) Let $(\tilde{X}^n,\tilde{Y}^n,\tilde{Z}^n) \sim \prod_{i=1}^n p_X(\tilde{x}_i)p_Y(\tilde{y}_i)p_{Z|X,Y}(\tilde{z}_i|\tilde{x}_i,\tilde{y}_i)$. Then

$$\mathsf{P}\{(\tilde{X}^n,\tilde{Y}^n,\tilde{Z}^n) \in \mathcal{T}_\epsilon^{(n)}(X,Y,Z)\} \doteq 2^{-nI(X;Y)}.$$

2.15. *Jointly typical triples.* Given $(X, Y, Z) \sim p(x, y, z)$, let

$$\mathcal{A}_n = \{(x^n, y^n, z^n)\colon\ (x^n, y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y),\\ (y^n, z^n) \in \mathcal{T}_\epsilon^{(n)}(Y, Z),\ (x^n, z^n) \in \mathcal{T}_\epsilon^{(n)}(X, Z)\}.$$

(a) Show that

$$|\mathcal{A}_n| \le 2^{n(H(X,Y)+H(Y,Z)+H(X,Z)+\delta(\epsilon))/2}.$$

(Hint: First show that $|\mathcal{A}_n| \le 2^{n(H(X,Y)+H(Z|Y)+\delta(\epsilon))}$.)

(b) Does the corresponding lower bound hold in general? (Hint: Consider $X = Y = Z$.)

Remark: It can be shown that $|\mathcal{A}_n| \doteq 2^{n(\max H(\tilde{X},\tilde{Y},\tilde{Z}))}$, where the maximum is over all joint pmfs $p(\tilde{x}, \tilde{y}, \tilde{z})$ such that $p(\tilde{x}, \tilde{y}) = p_{X,Y}(\tilde{x}, \tilde{y})$, $p(\tilde{y}, \tilde{z}) = p_{Y,Z}(\tilde{y}, \tilde{z})$, and $p(\tilde{x}, \tilde{z}) = p_{X,Z}(\tilde{x}, \tilde{z})$.

2.16. *Multivariate typicality.* Let $(U, X, Y, Z) \sim p(u, x, y, z)$. Prove the following statements.

(a) If $(\tilde{U}^n, \tilde{X}^n, \tilde{Y}^n, \tilde{Z}^n) \sim \prod_{i=1}^n p_U(\tilde{u}_i)p_X(\tilde{x}_i)p_Y(\tilde{y}_i)p_Z(\tilde{z}_i)$, then

$$\mathsf{P}\{(\tilde{U}^n, \tilde{X}^n, \tilde{Y}^n, \tilde{Z}^n) \in \mathcal{T}_\epsilon^{(n)}(U, X, Y, Z)\} \doteq 2^{-n(I(U;X)+I(U,X;Y)+I(U,X,Y;Z))}.$$

(b) If $(\tilde{U}^n, \tilde{X}^n, \tilde{Y}^n, \tilde{Z}^n) \sim \prod_{i=1}^n p_{U,X}(\tilde{u}_i, \tilde{x}_i)p_{Y|X}(\tilde{y}_i|\tilde{x}_i)p_Z(\tilde{z}_i)$, then

$$\mathsf{P}\{(\tilde{U}^n, \tilde{X}^n, \tilde{Y}^n, \tilde{Z}^n) \in \mathcal{T}_\epsilon^{(n)}(U, X, Y, Z)\} \doteq 2^{-n(I(U;Y|X)+I(U,X,Y;Z))}.$$

2.17. *Need for both ϵ and ϵ'.* Let (X, Y) be a pair of independent Bern(1/2) random variables. Let $k = \lfloor (n/2)(1 + \epsilon) \rfloor$ and x^n be a binary sequence with k ones followed by $(n - k)$ zeros.

(a) Check that $x^n \in \mathcal{T}_\epsilon^{(n)}(X)$.

(b) Let Y^n be an i.i.d. Bern(1/2) sequence, independent of x^n. Show that

$$\mathsf{P}\{(x^n, Y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y)\} \le \mathsf{P}\left\{\sum_{i=1}^k Y_i < (k + 1)/2\right\},$$

which converges to 1/2 as $n \to \infty$. Thus, the fact that $x^n \in \mathcal{T}_\epsilon^{(n)}(X)$ and $Y^n \sim \prod_{i=1}^n p_{Y|X}(y_i|x_i)$ does not necessarily imply that $\mathsf{P}\{(x^n, Y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y)\}$.

Remark: This problem illustrates that in general we need $\epsilon > \epsilon'$ in the conditional typicality lemma.

APPENDIX 2A PROOF OF THE CONDITIONAL TYPICALITY LEMMA

We wish to show that

$$\lim_{n\to\infty} \mathsf{P}\{|\pi(x, y|x^n, Y^n) - p(x, y)| > \epsilon p(x, y) \text{ for some } (x, y) \in \mathcal{X} \times \mathcal{Y}\} = 0.$$

For $x \in \mathcal{X}$ such that $p(x) \neq 0$, consider

$$\begin{aligned}
&\mathsf{P}\{|\pi(x, y|x^n, Y^n) - p(x, y)| > \epsilon p(x, y)\} \\
&\quad = \mathsf{P}\left\{\left|\frac{\pi(x, y|x^n, Y^n)}{p(x)} - p(y|x)\right| > \epsilon p(y|x)\right\} \\
&\quad = \mathsf{P}\left\{\left|\frac{\pi(x, y|x^n, Y^n)\pi(x|x^n)}{p(x)\pi(x|x^n)} - p(y|x)\right| > \epsilon p(y|x)\right\} \\
&\quad = \mathsf{P}\left\{\left|\frac{\pi(x, y|x^n, Y^n)}{\pi(x|x^n)p(y|x)} \cdot \frac{\pi(x|x^n)}{p(x)} - 1\right| > \epsilon\right\} \\
&\quad \le \mathsf{P}\left\{\frac{\pi(x, y|x^n, Y^n)}{\pi(x|x^n)p(y|x)} \cdot \frac{\pi(x|x^n)}{p(x)} > 1 + \epsilon\right\} + \mathsf{P}\left\{\frac{\pi(x, y|x^n, Y^n)}{\pi(x|x^n)p(y|x)} \cdot \frac{\pi(x|x^n)}{p(x)} < 1 - \epsilon\right\}.
\end{aligned}$$

Now, since $x^n \in \mathcal{T}_{\epsilon'}^{(n)}(X)$, $1 - \epsilon' \le \pi(x|x^n)/p(x) \le 1 + \epsilon'$,

$$\mathsf{P}\left\{\frac{\pi(x, y|x^n, Y^n)}{\pi(x|x^n)p(y|x)} \cdot \frac{\pi(x|x^n)}{p(x)} > 1 + \epsilon\right\} \le \mathsf{P}\left\{\frac{\pi(x, y|x^n, Y^n)}{\pi(x|x^n)} > \frac{1 + \epsilon}{1 + \epsilon'} p(y|x)\right\} \tag{2.11}$$

and

$$\mathsf{P}\left\{\frac{\pi(x, y|x^n, Y^n)}{\pi(x|x^n)p(y|x)} \cdot \frac{\pi(x|x^n)}{p(x)} < 1 - \epsilon\right\} \le \mathsf{P}\left\{\frac{\pi(x, y|x^n, Y^n)}{\pi(x|x^n)} < \frac{1 - \epsilon}{1 - \epsilon'} p(y|x)\right\}. \tag{2.12}$$

Since $\epsilon' < \epsilon$, we have $(1 + \epsilon)/(1 + \epsilon') > 1$ and $(1 - \epsilon)/(1 - \epsilon') < 1$. Furthermore, since Y^n is generated according to the correct conditional pmf, by the LLN, for every $y \in \mathcal{Y}$,

$$\frac{\pi(x, y|x^n, Y^n)}{\pi(x|x^n)} \to p(y|x) \quad \text{in probability.}$$

Hence, both upper bounds in (2.11) and (2.12) tend to zero as $n \to \infty$, which, by the union of events bound over all $(x, y) \in \mathcal{X} \times \mathcal{Y}$, completes the proof of the conditional typicality lemma.

CHAPTER 3

Point-to-Point Information Theory

We review Shannon's basic theorems for point-to-point communication. Over the course of the review, we introduce the techniques of random coding and joint typicality encoding and decoding, and develop the packing and covering lemmas. These techniques will be used in the achievability proofs for multiple sources and channels throughout the book. We rigorously show how achievability for a discrete memoryless channel or source can be extended to its Gaussian counterpart. We also show that under our definition of typicality, the lossless source coding theorem is a corollary of the lossy source coding theorem. This fact will prove useful in later chapters. Along the way, we point out some key differences between results for point-to-point communication and for the multiuser networks discussed in subsequent chapters.

3.1 CHANNEL CODING

Consider the point-to-point communication system model depicted in Figure 3.1, where a sender wishes to reliably communicate a message M at a rate R bits per transmission to a receiver over a noisy communication channel (or a noisy storage medium). Toward this end, the sender encodes the message into a codeword X^n and transmits it over the channel in n time instances (also referred to as transmissions or channel uses). Upon receiving the noisy sequence Y^n, the receiver decodes it to obtain the estimate $\hat{M}$ of the message. The channel coding problem is to find the channel capacity, which is the highest rate R such that the probability of decoding error can be made to decay asymptotically to zero with the code block length n.

We first consider the channel coding problem for a simple *discrete memoryless channel* (DMC) model $(\mathcal{X}, p(y|x), \mathcal{Y})$ (in short $p(y|x)$) that consists of a finite input set (or alphabet) $\mathcal{X}$, a finite output set $\mathcal{Y}$, and a collection of conditional pmfs $p(y|x)$ on $\mathcal{Y}$ for every $x \in \mathcal{X}$. Thus, if an input symbol $x \in \mathcal{X}$ is transmitted, the probability of receiving an output symbol $y \in \mathcal{Y}$ is $p(y|x)$. The channel is stationary and memoryless in the

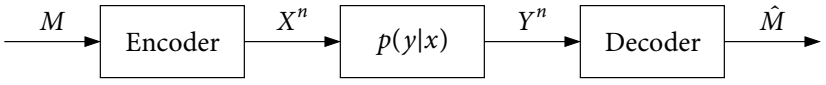


Figure 3.1. Point-to-point communication system.

sense that when it is used n times with message M drawn from an arbitrary set and input $X^n \in \mathcal{X}^n$, the output $Y_i \in \mathcal{Y}$ at time $i \in [1:n]$ given (M, X^i, Y^{i-1}) is distributed according to $p(y_i|x^i, y^{i-1}, m) = p_{Y|X}(y_i|x_i)$. Throughout the book, the phrase "discrete memoryless (DM)" will refer to "finite-alphabet and stationary memoryless".

A $(2^{nR}, n)$ code for the DMC $p(y|x)$ consists of

- a message set $[1:2^{nR}] = \{1, 2, \ldots, 2^{\lceil nR \rceil}\}$,
- an encoding function (encoder) $x^n\colon [1:2^{nR}] \to \mathcal{X}^n$ that assigns a *codeword* $x^n(m)$ to each message $m \in [1:2^{nR}]$, and
- a decoding function (decoder) $\hat{m}\colon \mathcal{Y}^n \to [1:2^{nR}] \cup \{\mathrm{e}\}$ that assigns an estimate $\hat{m} \in [1:2^{nR}]$ or an error message e to each received sequence y^n.

Note that under the above definition of a $(2^{nR}, n)$ code, the memoryless property implies that

$$p(y^n|x^n, m) = \prod_{i=1}^{n} p_{Y|X}(y_i|x_i). \tag{3.1}$$

The set $\mathcal{C} = \{x^n(1), x^n(2), \ldots, x^n(2^{\lceil nR \rceil})\}$ is referred to as the *codebook* associated with the $(2^{nR}, n)$ code. We assume that the message is uniformly distributed over the message set, i.e., $M \sim \mathrm{Unif}[1:2^{nR}]$.

The performance of a given code is measured by the probability that the estimate of the message is different from the actual message sent. More precisely, let $\lambda_m(\mathcal{C}) = \mathsf{P}\{\hat{M} \neq m \,|\, M = m\}$ be the conditional probability of error given that message m is sent. Then, the *average probability of error* for a $(2^{nR}, n)$ code is defined as

$$P_e^{(n)}(\mathcal{C}) = \mathsf{P}\{\hat{M} \neq M\} = \frac{1}{2^{\lceil nR \rceil}} \sum_{m=1}^{2^{\lceil nR \rceil}} \lambda_m(\mathcal{C}).$$

A rate R is said to be *achievable* if there exists a sequence of $(2^{nR}, n)$ codes such that $\lim_{n\to\infty} P_e^{(n)}(\mathcal{C}) = 0$. The *capacity* C of a DMC is the supremum over all achievable rates.

Remark 3.1. Although the message M depends on the block length n (through the message set), we will not show this dependency explicitly. Also, from this point on, we will not explicitly show the dependency of the probability of error $P_e^{(n)}$ on the codebook $\mathcal{C}$.

3.1.1 Channel Coding Theorem

Shannon established a simple characterization of channel capacity.

Theorem 3.1 (Channel Coding Theorem). The capacity of the discrete memoryless channel $p(y|x)$ is given by the information capacity formula

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

In the following, we evaluate the information capacity formula for several simple but important discrete memoryless channels.

Example 3.1 (Binary symmetric channel). Consider the *binary symmetric channel* with *crossover probability* p (in short BSC(p)) depicted in Figure 3.2. The channel input X and output Y are binary and each binary input symbol is flipped with probability p. Equivalently, we can specify the BSC as $Y = X \oplus Z$, where the noise $Z \sim \text{Bern}(p)$ is independent of the input X. The capacity is

$$\begin{aligned} C &= \max_{p(x)} I(X;Y) \\ &= \max_{p(x)} (H(Y) - H(Y|X)) \\ &= \max_{p(x)} (H(Y) - H(X \oplus Z|X)) \\ &= \max_{p(x)} (H(Y) - H(Z|X)) \\ &\overset{(a)}{=} \max_{p(x)} H(Y) - H(Z) \\ &= 1 - H(p), \end{aligned}$$

where (a) follows by the independence of X and Z. Note that the capacity is attained by $X \sim \text{Bern}(1/2)$, which, in turn, results in $Y \sim \text{Bern}(1/2)$.

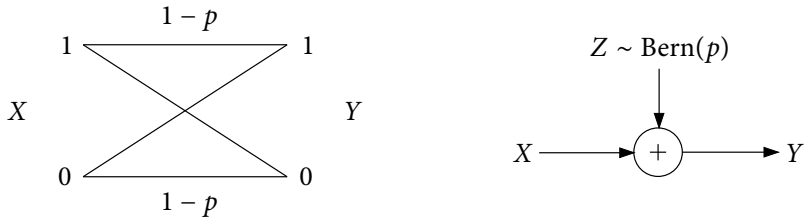


Figure 3.2. Equivalent representations of the binary symmetric channel BSC(p).

Example 3.2 (Binary erasure channel). Consider the *binary erasure channel* with *erasure probability* p (BEC(p)) depicted in Figure 3.3. The channel input X and output Y are binary and each binary input symbol is erased (mapped into an erasure symbol e) with probability p. Thus, the receiver knows which transmissions are erased, but the sender does not. The capacity is

$$\begin{aligned} C &= \max_{p(x)} (H(X) - H(X|Y)) \\ &\overset{(a)}{=} \max_{p(x)} (H(X) - pH(X)) \\ &= 1 - p, \end{aligned}$$

where (a) follows since $H(X|Y = y) = 0$ if $y = 0$ or 1, and $H(X|Y = \text{e}) = H(X)$. The capacity is again attained by $X \sim \text{Bern}(1/2)$.

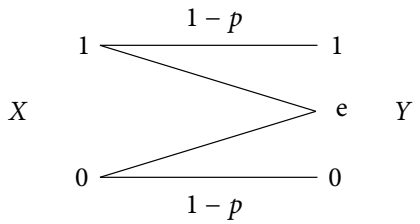


Figure 3.3. Binary erasure channel BEC(p).

Example 3.3 (Product DMC). Let $p(y_1|x_1)$ and $p(y_2|x_2)$ be two DMCs with capacities C_1 and C_2, respectively. The *product DMC* is a DMC $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1|x_1)p(y_2|x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ in which the symbols $x_1 \in \mathcal{X}_1$ and $x_2 \in \mathcal{X}_2$ are sent simultaneously in parallel and the received outputs Y_1 and Y_2 are distributed according to $p(y_1, y_2|x_1, x_2) = p(y_1|x_1)p(y_2|x_2)$. The capacity of the product DMC is

$$\begin{aligned} C &= \max_{p(x_1,x_2)} I(X_1, X_2; Y_1, Y_2) \\ &= \max_{p(x_1,x_2)} \big(I(X_1, X_2; Y_1) + I(X_1, X_2; Y_2|Y_1)\big) \\ &\overset{(a)}{=} \max_{p(x_1,x_2)} \big(I(X_1; Y_1) + I(X_2; Y_2)\big) \\ &= \max_{p(x_1)} I(X_1; Y_1) + \max_{p(x_2)} I(X_2; Y_2) \\ &= C_1 + C_2, \end{aligned}$$

where (a) follows since $Y_1 \to X_1 \to X_2 \to Y_2$ form a Markov chain, which implies that $I(X_1, X_2; Y_1) = I(X_1; Y_1)$ and $I(X_1, X_2; Y_2|Y_1) \le I(Y_1, X_1, X_2; Y_2) = I(X_2; Y_2)$ with equality iff X_1 and X_2 are independent.

More generally, let $p(y_j|x_j)$ be a DMC with capacity C_j for $j \in [1 : d]$. A product DMC consists of an input alphabet $\mathcal{X} = \bigtimes_{j=1}^{d} \mathcal{X}_j$, an output alphabet $\mathcal{Y} = \bigtimes_{j=1}^{d} \mathcal{Y}_j$, and a collection of conditional pmfs $p(y_1, \ldots, y_d|x_1, \ldots, x_d) = \prod_{j=1}^{d} p(y_j|x_j)$. The capacity of the product DMC is

$$C = \sum_{j=1}^{d} C_j.$$

To prove the channel coding theorem, we need to show that the *information* capacity in Theorem 3.1 is equal to the *operational* capacity defined in the channel coding setup. This involves the verification of two statements.

- **Achievability.** For every rate $R < C = \max_{p(x)} I(X; Y)$, there exists a sequence of $(2^{nR}, n)$ codes with average probability of error $P_e^{(n)}$ that tends to zero as $n \to \infty$. The proof of achievability uses random coding and joint typicality decoding.
- **Converse.** For every sequence of $(2^{nR}, n)$ codes with probability of error $P_e^{(n)}$ that tends to zero as $n \to \infty$, the rate must satisfy $R \le C = \max_{p(x)} I(X; Y)$. The proof of the converse uses Fano's inequality and basic properties of mutual information.

We first prove achievability in the following subsection. The proof of the converse is given in Section 3.1.4.

3.1.2 Proof of Achievability

For simplicity of presentation, we assume throughout the proof that nR is an integer.

Random codebook generation. We use random coding. Fix the pmf $p(x)$ that attains the information capacity C. Randomly and independently generate 2^{nR} sequences $x^n(m)$, $m \in [1 : 2^{nR}]$, each according to $p(x^n) = \prod_{i=1}^{n} p_X(x_i)$. The generated sequences constitute the codebook $\mathcal{C}$. Thus

$$p(\mathcal{C}) = \prod_{m=1}^{2^{nR}} \prod_{i=1}^{n} p_X(x_i(m)).$$

The chosen codebook $\mathcal{C}$ is revealed to both the encoder and the decoder before transmission commences.

Encoding. To send message $m \in [1 : 2^{nR}]$, transmit $x^n(m)$.

Decoding. We use *joint typicality decoding*. Let y^n be the received sequence. The receiver declares that $\hat{m} \in [1 : 2^{nR}]$ is sent if it is the unique message such that $(x^n(\hat{m}), y^n) \in \mathcal{T}_\epsilon^{(n)}$; otherwise—if there is none or more than one such message—it declares an error e.

Analysis of the probability of error. Assuming that message m is sent, the decoder makes an error if $(x^n(m), y^n) \notin \mathcal{T}_\epsilon^{(n)}$ or if there is another message $m' \neq m$ such that $(x^n(m'), y^n) \in \mathcal{T}_\epsilon^{(n)}$. Consider the probability of error averaged over M and codebooks

$$\begin{aligned}
\mathsf{P}(\mathcal{E}) &= \mathsf{E}_{\mathcal{C}}\left(P_e^{(n)}\right) \\
&= \mathsf{E}_{\mathcal{C}}\left(\frac{1}{2^{nR}} \sum_{m=1}^{2^{nR}} \lambda_m(\mathcal{C})\right) \\
&= \frac{1}{2^{nR}} \sum_{m=1}^{2^{nR}} \mathsf{E}_{\mathcal{C}}(\lambda_m(\mathcal{C})) \\
&\overset{(a)}{=} \mathsf{E}_{\mathcal{C}}(\lambda_1(\mathcal{C})) \\
&= \mathsf{P}(\mathcal{E} \mid M = 1),
\end{aligned}$$

where (a) follows by the symmetry of the random codebook generation. Thus, we assume without loss of generality that $M = 1$ is sent. For brevity, we do not explicitly condition on the event $\{M = 1\}$ in probability expressions whenever it is clear from the context.

The decoder makes an error iff one or both of the following events occur:

$$\begin{aligned}
\mathcal{E}_1 &= \{(X^n(1), Y^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \\
\mathcal{E}_2 &= \{(X^n(m), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m \neq 1\}.
\end{aligned}$$

Thus, by the union of events bound,

$$\mathsf{P}(\mathcal{E}) = \mathsf{P}(\mathcal{E}_1 \cup \mathcal{E}_2) \leq \mathsf{P}(\mathcal{E}_1) + \mathsf{P}(\mathcal{E}_2).$$

We now bound each term. By the law of large numbers (LLN), the first term $\mathsf{P}(\mathcal{E}_1)$ tends to zero as $n \to \infty$. For the second term, since for $m \neq 1$,

$$(X^n(m), X^n(1), Y^n) \sim \prod_{i=1}^{n} p_X(x_i(m)) p_{X,Y}(x_i(1), y_i),$$

we have $(X^n(m), Y^n) \sim \prod_{i=1}^{n} p_X(x_i(m)) p_Y(y_i)$. Thus, by the extension of the joint typicality lemma in Remark 2.2,

$$\mathsf{P}\{(X^n(m), Y^n) \in \mathcal{T}_\epsilon^{(n)}\} \leq 2^{-n(I(X;Y)-\delta(\epsilon))} = 2^{-n(C-\delta(\epsilon))}.$$

Again by the union of events bound,

$$\mathsf{P}(\mathcal{E}_2) \leq \sum_{m=2}^{2^{nR}} \mathsf{P}\{(X^n(m), Y^n) \in \mathcal{T}_\epsilon^{(n)}\} \leq \sum_{m=2}^{2^{nR}} 2^{-n(C-\delta(\epsilon))} \leq 2^{-n(C-R-\delta(\epsilon))},$$

which tends to zero as $n \to \infty$ if $R < C - \delta(\epsilon)$.

Note that since the probability of error averaged over codebooks, $\mathsf{P}(\mathcal{E})$, tends to zero as $n \to \infty$, there must exist a sequence of $(2^{nR}, n)$ codes such that $\lim_{n\to\infty} P_e^{(n)} = 0$, which proves that $R < C - \delta(\epsilon)$ is achievable. Finally, taking $\epsilon \to 0$ completes the proof.

Remark 3.2. To bound the average probability of error $\mathsf{P}(\mathcal{E})$, we divided the error event into two events, each of which comprises events with $(X^n(m), Y^n)$ having the same joint pmf. This observation will prove useful when we analyze more complex error events in later chapters.

Remark 3.3. By the Markov inequality, the probability of error for a random codebook, that is, a codebook consisting of random sequences $X^n(m)$, $m \in [1 : 2^{nR}]$, tends to zero as $n \to \infty$ in probability. Hence, most codebooks are good in terms of the error probability.

Remark 3.4. The capacity with the *maximal* probability of error $\lambda^* = \max_m \lambda_m$ is equal to that with the average probability of error $P_e^{(n)}$. This can be shown by discarding the worst half of the codewords (in terms of error probability) from each code in the sequence of $(2^{nR}, n)$ codes with $\lim_{n\to\infty} P_e^{(n)} = 0$. The maximal probability of error for each of the codes with the remaining codewords is at most $2P_e^{(n)}$, which again tends to zero as $n \to \infty$. As we will see, the capacity with maximal probability of error is not always equal to that with average probability of error for multiuser channels.

Remark 3.5. Depending on the structure of the channel, the rate $R = C$ may or may not be achievable. We will sometimes informally say that C is achievable to mean that every $R < C$ is achievable.

3.1.3 Achievability Using Linear Codes

Recall that in the achievability proof, we used only *pairwise* independence of codewords $X^n(m)$, $m \in [1 : 2^{nR}]$, rather than mutual independence among all of them. This observation has an interesting consequence—the capacity of a BSC can be achieved using *linear* codes.

Consider a BSC(p). Let $k = \lceil nR \rceil$ and $(u_1, u_2, \ldots, u_k) \in \{0,1\}^k$ be the binary expansion of the message $m \in [1 : 2^k - 1]$. Generate a random codebook such that each codeword $x^n(u^k)$ is a linear function of u^k (in binary field arithmetic). In particular, let

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1k} \\ g_{21} & g_{22} & \cdots & g_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{nk} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{bmatrix},$$

where $g_{ij} \in \{0,1\}$, $i \in [1 : n]$, $j \in [1 : k]$, are generated i.i.d. according to Bern(1/2).

Now we can easily check that $X_1(u^k), \ldots, X_n(u^k)$ are i.i.d. Bern(1/2) for each $u^k \neq 0$, and $X^n(u^k)$ and $X^n(\tilde{u}^k)$ are independent for each $u^k \neq \tilde{u}^k$. Therefore, using the same steps as in the proof of achievability for the channel coding theorem, it can be shown that the error probability of joint typicality decoding tends to zero as $n \to \infty$ if $R < 1 - H(p) - \delta(\epsilon)$. This shows that for a BSC there exists not only a good sequence of codes, but also a good sequence of *linear* codes.

It can be similarly shown that random linear codes achieve the capacity of the binary erasure channel, or more generally, channels for which the input alphabet is a finite field and the information capacity is attained by the uniform pmf.

3.1.4 Proof of the Converse

We need to show that for every sequence of $(2^{nR}, n)$ codes with $\lim_{n\to\infty} P_e^{(n)} = 0$, we must have $R \le C = \max_{p(x)} I(X;Y)$. Again for simplicity of presentation, we assume that nR is an integer. Every $(2^{nR}, n)$ code induces a joint pmf on (M, X^n, Y^n) of the form

$$p(m, x^n, y^n) = 2^{-nR} p(x^n|m) \prod_{i=1}^{n} p_{Y|X}(y_i|x_i).$$

By Fano's inequality,

$$H(M|\hat{M}) \le 1 + P_e^{(n)} nR = n\epsilon_n,$$

where ϵ_n tends to zero as $n \to \infty$ by the assumption that $\lim_{n\to\infty} P_e^{(n)} = 0$. Thus, by the data processing inequality,

$$H(M|Y^n) \le H(M|\hat{M}) \le n\epsilon_n. \tag{3.2}$$

Now consider

$$\begin{aligned} nR &= H(M) \\ &= I(M; Y^n) + H(M|Y^n) \\ &\overset{(a)}{\le} I(M; Y^n) + n\epsilon_n \\ &= \sum_{i=1}^{n} I(M; Y_i|Y^{i-1}) + n\epsilon_n \end{aligned}$$

$$\begin{aligned} &\le \sum_{i=1}^{n} I(M, Y^{i-1}; Y_i) + n\epsilon_n \\ &\overset{(b)}{=} \sum_{i=1}^{n} I(X_i, M, Y^{i-1}; Y_i) + n\epsilon_n \\ &\overset{(c)}{=} \sum_{i=1}^{n} I(X_i; Y_i) + n\epsilon_n \\ &\le nC + n\epsilon_n, \end{aligned} \tag{3.3}$$

where (a) follows from (3.2), (b) follows since X_i is a function of M, and (c) follows since the channel is memoryless, which implies that $(M, Y^{i-1}) \to X_i \to Y_i$ form a Markov chain. The last inequality follows by the definition of the information capacity. Since ϵ_n tends to zero as $n \to \infty$, $R \le C$, which completes the proof of the converse.

3.1.5 DMC with Feedback

Consider the DMC with *noiseless causal feedback* depicted in Figure 3.4. The encoder assigns a symbol $x_i(m, y^{i-1})$ to each message $m \in [1 : 2^{nR}]$ and past received output sequence $y^{i-1} \in \mathcal{Y}^{i-1}$ for $i \in [1 : n]$. Hence (3.1) does not hold in general and a $(2^{nR}, n)$ feedback code induces a joint pmf of the form

$$(M, X^n, Y^n) \sim p(m, x^n, y^n) = 2^{-nR} \prod_{i=1}^{n} p(x_i | m, y^{i-1}) p_{Y|X}(y_i | x_i).$$

Nonetheless, it can be easily shown that the chain of inequalities (3.3) continues to hold in the presence of such causal feedback. Hence, feedback *does not* increase the capacity of the DMC. In Chapter 17 we will discuss the role of feedback in communication in more detail.

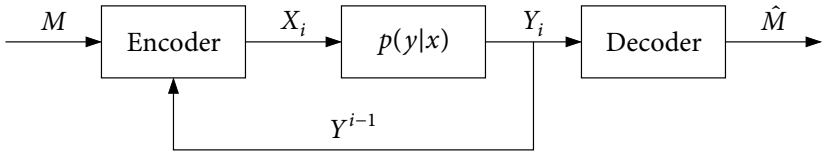


Figure 3.4. DMC with noiseless causal feedback.

3.2 PACKING LEMMA

The packing lemma generalizes the bound on the probability of the decoding error event $\mathcal{E}_2$ in the achievability proof of the channel coding theorem; see Section 3.1.2. The lemma will be used in the achievability proofs of many multiuser source and channel coding theorems.

Recall that in the bound on $\mathsf{P}(\mathcal{E}_2)$, we had a fixed input pmf $p(x)$ and a DMC $p(y|x)$. As illustrated in Figure 3.5, we considered a set of $(2^{nR} - 1)$ i.i.d. codewords $X^n(m)$,

$m \in [2 : 2^{nR}]$, each distributed according to $\prod_{i=1}^{n} p_X(x_i)$, and an output sequence $\tilde{Y}^n \sim \prod_{i=1}^{n} p_Y(\tilde{y}_i)$ generated by the codeword $X^n(1) \sim \prod_{i=1}^{n} p_X(x_i)$, which is independent of the set of codewords. We showed that the probability that $(X^n(m), \tilde{Y}^n) \in \mathcal{T}_\epsilon^{(n)}$ for some $m \in [2 : 2^{nR}]$ tends to zero as $n \to \infty$ if $R < I(X; Y) - \delta(\epsilon)$.

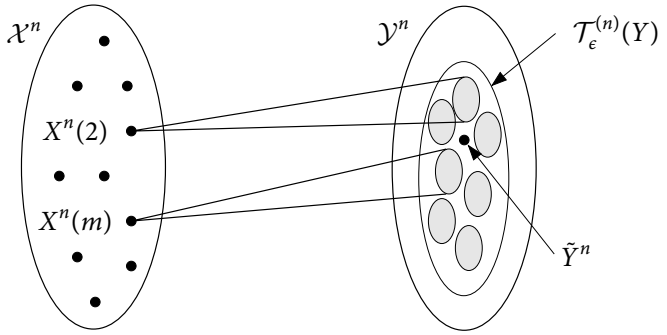


Figure 3.5. Illustration of the setup for the bound on $\mathsf{P}(\mathcal{E}_2)$.

The following lemma extends this bound in three ways:

1. The codewords that are independent of $\tilde{Y}^n$ need not be mutually independent.
2. The sequence $\tilde{Y}^n$ can have an arbitrary pmf (not necessarily $\prod_{i=1}^{n} p_Y(\tilde{y}_i)$).
3. The sequence $\tilde{Y}^n$ and the set of codewords are conditionally independent of a sequence U^n that has a general joint pmf with $\tilde{Y}^n$.

Lemma 3.1 (Packing lemma). Let $(U, X, Y) \sim p(u, x, y)$. Let $(\tilde{U}^n, \tilde{Y}^n) \sim p(\tilde{u}^n, \tilde{y}^n)$ be a pair of arbitrarily distributed random sequences, not necessarily distributed according to $\prod_{i=1}^{n} p_{U,Y}(\tilde{u}_i, \tilde{y}_i)$. Let $X^n(m)$, $m \in \mathcal{A}$, where $|\mathcal{A}| \le 2^{nR}$, be random sequences, each distributed according to $\prod_{i=1}^{n} p_{X|U}(x_i|\tilde{u}_i)$. Further assume that $X^n(m)$, $m \in \mathcal{A}$, is pairwise conditionally independent of $\tilde{Y}^n$ given $\tilde{U}^n$, but is arbitrarily dependent on other $X^n(m)$ sequences. Then, there exists $\delta(\epsilon)$ that tends to zero as $\epsilon \to 0$ such that

$$\lim_{n\to\infty} \mathsf{P}\{(\tilde{U}^n, X^n(m), \tilde{Y}^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m \in \mathcal{A}\} = 0,$$

if $R < I(X; Y|U) - \delta(\epsilon)$.

Note that the packing lemma can be readily applied to the linear coding case where the $X^n(m)$ sequences are only pairwise independent. We will later encounter cases for which $U \neq \emptyset$ and $(\tilde{U}^n, \tilde{Y}^n)$ is not generated i.i.d.

Proof. Define the events

$$\tilde{\mathcal{E}}_m = \{(\tilde{U}^n, X^n(m), \tilde{Y}^n) \in \mathcal{T}_\epsilon^{(n)}\} \quad \text{for } m \in \mathcal{A}.$$

By the union of events bound, the probability of the event of interest can be bounded as

$$\mathsf{P}\Big(\bigcup_{m\in\mathcal{A}} \tilde{\mathcal{E}}_m\Big) \le \sum_{m\in\mathcal{A}} \mathsf{P}(\tilde{\mathcal{E}}_m).$$

Now consider

$$\begin{aligned}
\mathsf{P}(\tilde{\mathcal{E}}_m) &= \mathsf{P}\{(\tilde{U}^n, X^n(m), \tilde{Y}^n) \in \mathcal{T}_\epsilon^{(n)}(U, X, Y)\} \\
&= \sum_{(\tilde{u}^n,\tilde{y}^n)\in\mathcal{T}_\epsilon^{(n)}} p(\tilde{u}^n, \tilde{y}^n)\, \mathsf{P}\{(\tilde{u}^n, X^n(m), \tilde{y}^n) \in \mathcal{T}_\epsilon^{(n)}(U, X, Y) \,|\, \tilde{U}^n = \tilde{u}^n, \tilde{Y}^n = \tilde{y}^n\} \\
&\overset{(a)}{=} \sum_{(\tilde{u}^n,\tilde{y}^n)\in\mathcal{T}_\epsilon^{(n)}} p(\tilde{u}^n, \tilde{y}^n)\, \mathsf{P}\{(\tilde{u}^n, X^n(m), \tilde{y}^n) \in \mathcal{T}_\epsilon^{(n)}(U, X, Y) \,|\, \tilde{U}^n = \tilde{u}^n\} \\
&\overset{(b)}{\le} \sum_{(\tilde{u}^n,\tilde{y}^n)\in\mathcal{T}_\epsilon^{(n)}} p(\tilde{u}^n, \tilde{y}^n) 2^{-n(I(X;Y|U)-\delta(\epsilon))} \\
&\le 2^{-n(I(X;Y|U)-\delta(\epsilon))},
\end{aligned}$$

where (a) follows by the conditional independence of $X^n(m)$ and $\tilde{Y}^n$ given $\tilde{U}^n$, and (b) follows by the joint typicality lemma in Section 2.5 since $(\tilde{u}^n, \tilde{y}^n) \in \mathcal{T}_\epsilon^{(n)}$ and $X^n(m) \,|\, \{\tilde{U}^n = \tilde{u}^n, \tilde{Y}^n = \tilde{y}^n\} \sim \prod_{i=1}^n p_{X|U}(x_i|\tilde{u}_i)$. Hence

$$\sum_{m\in\mathcal{A}} \mathsf{P}(\tilde{\mathcal{E}}_m) \le |\mathcal{A}| 2^{-n(I(X;Y|U)-\delta(\epsilon))} \le 2^{-n(I(X;Y|U)-R-\delta(\epsilon))},$$

which tends to zero as $n \to \infty$ if $R < I(X; Y|U) - \delta(\epsilon)$. This completes the proof of the packing lemma.

3.3 CHANNEL CODING WITH INPUT COST

Consider a DMC $p(y|x)$. Suppose that there is a nonnegative cost function $b(x)$ associated with each input symbol $x \in \mathcal{X}$. Assume without loss of generality that there exists a zero-cost symbol $x_0 \in \mathcal{X}$, i.e., $b(x_0) = 0$. We further assume an average input cost constraint

$$\sum_{i=1}^n b(x_i(m)) \le nB \quad \text{for every } m \in [1 : 2^{nR}],$$

(in short, average cost constraint B on X). Now, defining the channel capacity of the DMC with cost constraint B, or the *capacity–cost function*, $C(B)$ in a similar manner to capacity without cost constraint, we can establish the following extension of the channel coding theorem.

Theorem 3.2. The capacity of the DMC $p(y|x)$ with average cost constraint B on X is

$$C(B) = \max_{p(x):\mathsf{E}(b(X))\le B} I(X; Y).$$

Note that $C(B)$ is nondecreasing, concave, and continuous in B.

Proof of achievability. The proof involves a minor change to the proof of achievability for the case with no cost constraint in Section 3.1.2 to ensure that every codeword satisfies the cost constraint.

Fix the pmf $p(x)$ that attains $C(B/(1+\epsilon))$. Randomly and independently generate 2^{nR} sequences $x^n(m)$, $m \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p_X(x_i)$. To send message m, the encoder transmits $x^n(m)$ if $x^n(m) \in \mathcal{T}_\epsilon^{(n)}$, and consequently, by the typical average lemma in Section 2.4, the sequence satisfies the cost constraint $\sum_{i=1}^n b(x_i(m)) \le nB$. Otherwise, it transmits $(x_0, \ldots, x_0)$. The analysis of the average probability of error for joint typicality decoding follows similar lines to the case without cost constraint. Assume $M = 1$. For the probability of the first error event,

$$\begin{aligned}
\mathsf{P}(\mathcal{E}_1) &= \mathsf{P}\{(X^n(1), Y^n) \notin \mathcal{T}_\epsilon^{(n)}\} \\
&= \mathsf{P}\{X^n(1) \in \mathcal{T}_\epsilon^{(n)}, (X^n(1), Y^n) \notin \mathcal{T}_\epsilon^{(n)}\} + \mathsf{P}\{X^n(1) \notin \mathcal{T}_\epsilon^{(n)}, (X^n(1), Y^n) \notin \mathcal{T}_\epsilon^{(n)}\} \\
&\le \sum_{x^n \in \mathcal{T}_\epsilon^{(n)}} \prod_{i=1}^n p_X(x_i) \sum_{y^n \notin \mathcal{T}_\epsilon^{(n)}(Y|x^n)} \prod_{i=1}^n p_{Y|X}(y_i|x_i) + \mathsf{P}\{X^n(1) \notin \mathcal{T}_\epsilon^{(n)}\} \\
&\le \sum_{(x^n, y^n) \notin \mathcal{T}_\epsilon^{(n)}} \prod_{i=1}^n p_X(x_i) p_{Y|X}(y_i|x_i) + \mathsf{P}\{X^n(1) \notin \mathcal{T}_\epsilon^{(n)}\}.
\end{aligned}$$

Thus, by the LLN for each term, $\mathsf{P}(\mathcal{E}_1)$ tends to zero as $n \to \infty$. The probability of the second error event, $\mathsf{P}(\mathcal{E}_2)$, is upper bounded in exactly the same manner as when there is no cost constraint. Hence, every rate $R < I(X;Y) = C(B/(1+\epsilon))$ is achievable. Finally, by the continuity of $C(B)$ in B, $C(B/(1+\epsilon))$ converges to $C(B)$ as $\epsilon \to 0$, which implies the achievability of every rate $R < C(B)$.

Proof of the converse. Consider a sequence of $(2^{nR}, n)$ codes with $\lim_{n\to\infty} P_e^{(n)} = 0$ such that for every n, the cost constraint $\sum_{i=1}^n b(x_i(m)) \le nB$ is satisfied for every $m \in [1 : 2^{nR}]$ and thus $\sum_{i=1}^n \mathsf{E}[b(X_i)] = \sum_{i=1}^n \mathsf{E}_M[b(x_i(M))] \le nB$. As before, by Fano's inequality and the data processing inequality,

$$\begin{aligned}
nR &\le \sum_{i=1}^n I(X_i; Y_i) + n\epsilon_n \\
&\overset{(a)}{\le} \sum_{i=1}^n C(\mathsf{E}[b(X_i)]) + n\epsilon_n \\
&\overset{(b)}{\le} nC\Big(\frac{1}{n}\sum_{i=1}^n \mathsf{E}[b(X_i)]\Big) + n\epsilon_n \\
&\overset{(c)}{\le} nC(B) + n\epsilon_n,
\end{aligned} \tag{3.4}$$

where (a) follows by the definition of $C(B)$, (b) follows by the concavity of $C(B)$, and (c) follows by the monotonicity of $C(B)$. This completes the proof of Theorem 3.2.

3.4 GAUSSIAN CHANNEL

Consider the discrete-time additive white Gaussian noise channel model depicted in Figure 3.6. The channel output corresponding to the input X is

$$Y = gX + Z, \tag{3.5}$$

where g is the *channel gain*, or *path loss*, and $Z \sim \mathrm{N}(0, N_0/2)$ is the noise. Thus, in transmission time $i \in [1 : n]$, the channel output is

$$Y_i = gX_i + Z_i,$$

where $\{Z_i\}$ is a white Gaussian noise process with average power $N_0/2$ (in short, $\{Z_i\}$ is a WGN($N_0/2$) process), independent of the channel input $X^n = x^n(M)$. We assume an *average transmission power constraint*

$$\sum_{i=1}^{n} x_i^2(m) \le nP \quad \text{for every } m \in [1 : 2^{nR}]$$

(in short, average power constraint P on X). The Gaussian channel is quite popular because it provides a simple model for several real-world communication channels, such as wireless and digital subscriber line (DSL) channels. We will later study more sophisticated models for these channels.

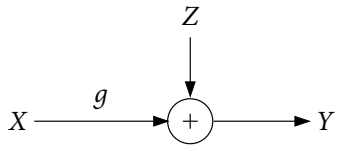


Figure 3.6. Additive white Gaussian noise channel.

We assume without loss of generality that $N_0/2 = 1$ (since one can define an equivalent Gaussian channel by dividing both sides of (3.5) by $\sqrt{N_0/2}$) and label the received power (which is now equal to the received *signal-to-noise ratio* (SNR)) g^2P as S. Note that the Gaussian channel is an example of the channel with cost discussed in the previous section, but with continuous (instead of finite) alphabets. Nonetheless, its capacity under power constraint P can be defined in the exact same manner as for the DMC with cost constraint.

Remark 3.6. If causal feedback from the receiver to the sender is present, then X_i depends only on the message M and the past received symbols Y^{i-1}. In this case X_i is *not* in general independent of the noise process. However, the message M and the noise process $\{Z_i\}$ are always assumed to be independent.

Remark 3.7. Since we discuss mainly additive white Gaussian noise channels, for brevity we will consistently use "Gaussian" in place of "additive white Gaussian noise."

3.4.1 Capacity of the Gaussian Channel

The capacity of the Gaussian channel is a simple function of the received SNR S.

Theorem 3.3. The capacity of the Gaussian channel is

$$C = \sup_{F(x):\mathsf{E}(X^2)\le P} I(X;Y) = \mathsf{C}(S),$$

where $\mathsf{C}(x) = (1/2)\log(1+x)$, $x \ge 0$, is the Gaussian capacity function.

For low SNR (small S), C grows linearly with S, while for high SNR, it grows logarithmically.

Proof of the converse. First note that the proof of the converse for the DMC with input cost constraint in Section 3.3 applies to arbitrary (not necessarily discrete) memoryless channels. Therefore, continuing the chain of inequalities in (3.4) with $b(x) = x^2$, we obtain

$$C \le \sup_{F(x):\mathsf{E}(X^2)\le P} I(X;Y).$$

Now for any $X \sim F(x)$ with $\mathsf{E}(X^2) \le P$,

$$\begin{aligned} I(X;Y) &= h(Y) - h(Y|X) \\ &= h(Y) - h(Z|X) \\ &= h(Y) - h(Z) \\ &\overset{(a)}{\le} \frac{1}{2}\log(2\pi e(S+1)) - \frac{1}{2}\log(2\pi e) \\ &= \mathsf{C}(S), \end{aligned}$$

where (a) follows by the maximum differential entropy lemma in Section 2.2 with $\mathsf{E}(Y^2) \le g^2P + 1 = S + 1$. Since this inequality becomes equality if $X \sim \mathrm{N}(0,P)$, we have shown that

$$C \le \sup_{F(x):\mathsf{E}(X^2)\le P} I(X;Y) = \mathsf{C}(S).$$

This completes the proof of the converse.

Proof of achievability. We extend the achievability proof for the DMC with cost constraint to show that $C \ge \mathsf{C}(S)$. Let $X \sim \mathrm{N}(0,P)$. Then, $I(X;Y) = \mathsf{C}(S)$. For every $j = 1, 2, \ldots$, let $[X]_j \in \{-j\Delta, -(j-1)\Delta, \ldots, -\Delta, 0, \Delta, \ldots, (j-1)\Delta, j\Delta\}$, $\Delta = 1/\sqrt{j}$, be a quantized version of X, obtained by mapping X to the closest quantization point $[X]_j = \hat{x}_j(X)$ such that $|[X]_j| \le |X|$. Clearly, $\mathsf{E}([X]_j^2) \le \mathsf{E}(X^2) = P$. Let $Y_j = g[X]_j + Z$ be the output corresponding to the input $[X]_j$ and let $[Y_j]_k = \hat{y}_k(Y_j)$ be a quantized version of Y_j defined in the same manner. Now, using the achievability proof for the DMC with cost constraint, we can show that for each j, k, any rate $R < I([X]_j; [Y_j]_k)$ is achievable for the channel with input $[X_j]$ and output $[Y_j]_k$ under power constraint P.

We now show that $I([X]_j; [Y_j]_k)$ can be made as close to $I(X; Y)$ as desired by taking j, k sufficiently large. First, by the data processing inequality,

$$I([X]_j; [Y_j]_k) \le I([X]_j; Y_j) = h(Y_j) - h(Z).$$

Since $\mathrm{Var}(Y_j) \le S + 1$, $h(Y_j) \le h(Y)$ for all j. Thus, $I([X]_j; [Y_j]_k) \le I(X; Y)$. For the other direction, we have the following.

Lemma 3.2. $\liminf_{j\to\infty} \lim_{k\to\infty} I([X]_j; [Y_j]_k) \ge I(X; Y)$.

The proof of this lemma is given in Appendix 3A. Combining both bounds, we have

$$\lim_{j\to\infty} \lim_{k\to\infty} I([X]_j; [Y_j]_k) = I(X; Y),$$

which completes the proof of Theorem 3.3.

Remark 3.8. This discretization procedure shows how to extend the coding theorem for a DMC to a Gaussian or any other well-behaved continuous-alphabet channel. Similar procedures can be used to extend coding theorems for finite-alphabet multiuser channels to their Gaussian counterparts. Hence, in subsequent chapters we will not provide formal proofs of such extensions.

3.4.2 Minimum Energy Per Bit

In the discussion of the Gaussian channel, we assumed average power constraint P on each transmitted codeword and found the highest reliable transmission rate under this constraint. A "dual" formulation of this problem is to assume a given transmission rate R and determine the *minimum energy per bit* needed to achieve it. This formulation can be viewed as more natural since it leads to a fundamental limit on the energy needed to reliably communicate one bit of information over a Gaussian channel.

Consider a $(2^{nR}, n)$ code for the Gaussian channel. Define the average power for the code as

$$P = \frac{1}{2^{nR}} \sum_{m=1}^{2^{nR}} \frac{1}{n} \sum_{i=1}^{n} x_i^2(m),$$

and the average energy per bit for the code as $E = P/R$ (that is, the energy per transmission divided by bits per transmission).

Following similar steps to the converse proof for the Gaussian channel in the previous section, we can show that for every sequence of $(2^{nR}, n)$ codes with average power P and $\lim_{n\to\infty} P_e^{(n)} = 0$, we must have

$$R \le \frac{1}{2} \log(1 + g^2 P).$$

Substituting $P = ER$, we obtain the lower bound on the energy per bit $E \ge (2^{2R} - 1)/(g^2 R)$.

We also know that if the average power of the code is P, then any rate $R < \mathsf{C}(g^2P)$ is achievable. Therefore, reliable communication at rate R with energy per bit $E > (2^{2R} - 1)/R$ is possible. Hence, the *energy-per-bit–rate function*, that is, the minimum energy-per-bit needed for reliable communication at rate R, is

$$E_b(R) = \frac{1}{g^2 R}(2^{2R} - 1).$$

This is a monotonically increasing and strictly convex function of R (see Figure 3.7). As R tends to zero, $E_b(R)$ converges to $E_b^* = (1/g^2)2 \ln 2$, which is the minimum energy per bit needed for reliable communication over a Gaussian channel with noise power $N_0/2 = 1$ and gain g.

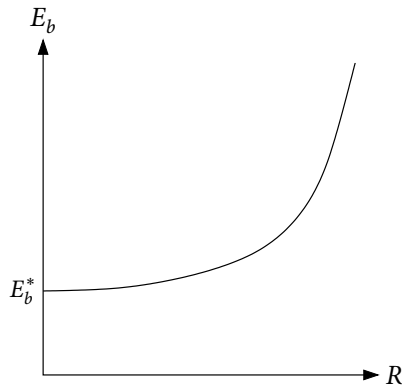


Figure 3.7. Minimum energy per bit versus transmission rate.

3.4.3 Gaussian Product Channel

The *Gaussian product channel* depicted in Figure 3.8 consists of a set of parallel Gaussian channels

$$Y_j = g_j X_j + Z_j \quad \text{for } j \in [1 : d],$$

where g_j is the gain of the j-th channel component and $Z_1, Z_2, \ldots, Z_d$ are independent zero-mean Gaussian noise components with the same average power $N_0/2 = 1$. We assume an average transmission power constraint

$$\frac{1}{n} \sum_{i=1}^{n} \sum_{j=1}^{d} x_{ji}^2(m) \le P \quad \text{for } m \in [1 : 2^{nR}].$$

The Gaussian product channel is a model for continuous-time (waveform) additive Gaussian noise channels; the parallel channels represent different frequency bands, time slots, or more generally, orthogonal signal dimensions.

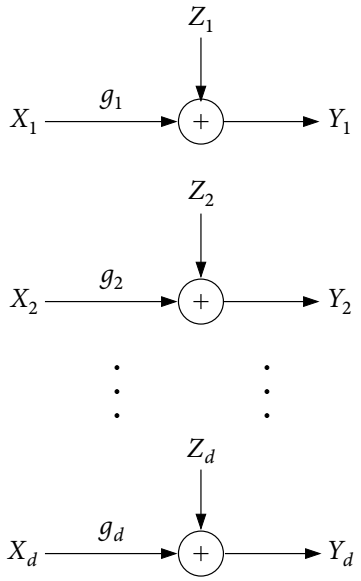


Figure 3.8. Gaussian product channel: d parallel Gaussian channels.

The capacity of the Gaussian product channel is

$$C = \max_{\substack{P_1, P_2, \ldots, P_d \\ \sum_{j=1}^{d} P_j \le P}} \sum_{j=1}^{d} \mathsf{C}(g_j^2 P_j). \tag{3.6}$$

The proof of the converse follows by noting that the capacity is upper bounded as

$$C \le \sup_{F(x^d):\sum_{j=1}^{d} \mathsf{E}(X_j^2) \le P} I(X^d; Y^d) = \sup_{F(x^d):\sum_{j=1}^{d} \mathsf{E}(X_j^2) \le P} \sum_{j=1}^{d} I(X_j; Y_j)$$

and that the supremum is attained by mutually independent $X_j \sim \mathrm{N}(0, P_j)$, $j \in [1 : d]$. For the achievability proof, note that this bound can be achieved by the discretization procedure for each component Gaussian channel. The constrained optimization problem in (3.6) is convex and can be solved by forming the Lagrangian; see Appendix E. The solution yields

$$P_j^* = \left[\lambda - \frac{1}{g_j^2}\right]^+ = \max\left\{\lambda - \frac{1}{g_j^2}, 0\right\},$$

where the Lagrange multiplier λ is chosen to satisfy the condition

$$\sum_{j=1}^{d} \left[\lambda - \frac{1}{g_j^2}\right]^+ = P.$$

This optimal power allocation has the *water-filling* interpretation illustrated in Figure 3.9.

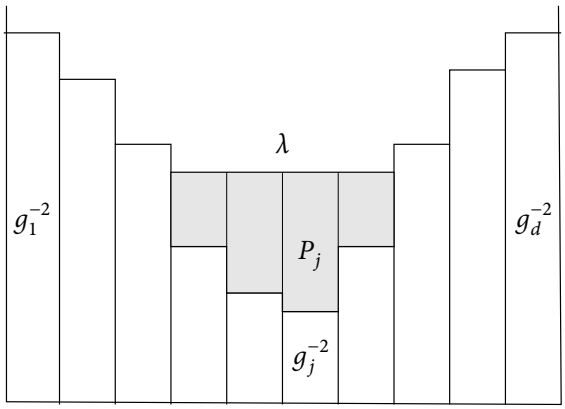


Figure 3.9. Water-filling interpretation of optimal power allocation.

Although this solution maximizes the mutual information and thus is optimal only in the asymptotic sense, it has been proven effective in practical subcarrier bit-loading algorithms for DSL and orthogonal frequency division multiplexing (OFDM) systems.

3.5 LOSSLESS SOURCE CODING

In the previous sections, we considered reliable communication of a maximally compressed information source represented by a uniformly distributed message over a noisy channel. In this section we consider the "dual" problem of communicating (or storing) an uncompressed source over a noiseless link (or in a memory) as depicted in Figure 3.10. The source sequence X^n is encoded (described or compressed) into an index M at rate R bits per source symbol, and the receiver decodes (decompresses) the index to find the estimate (reconstruction) $\hat{X}^n$ of the source sequence. The lossless source coding problem is to find the lowest compression rate in bits per source symbol such that the probability of decoding error decays asymptotically to zero with the code block length n.

We consider the lossless source coding problem for a *discrete memoryless source* (DMS) model $(\mathcal{X}, p(x))$, informally referred to as X, that consists of a finite alphabet $\mathcal{X}$ and a pmf $p(x)$ over $\mathcal{X}$. The DMS $(\mathcal{X}, p(x))$ generates an i.i.d. random process $\{X_i\}$ with $X_i \sim p_X(x_i)$. For example, the Bern(p) source X for $p \in [0, 1]$ has a binary alphabet and the Bern(p) pmf. It generates a Bern(p) random process $\{X_i\}$.

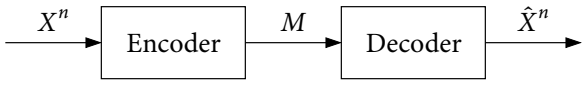


Figure 3.10. Point-to-point compression system.

A $(2^{nR}, n)$ *lossless source code* of rate R bits per source symbol consists of

- an encoding function (encoder) $m\colon \mathcal{X}^n \to [1 : 2^{nR}) = \{1, 2, \ldots, 2^{\lfloor nR \rfloor}\}$ that assigns an index $m(x^n)$ (a codeword of length $\lfloor nR \rfloor$ bits) to each source n-sequence x^n, and
- a decoding function (decoder) $\hat{x}^n\colon [1 : 2^{nR}) \to \mathcal{X}^n \cup \{\mathrm{e}\}$ that assigns an estimate $\hat{x}^n(m) \in \mathcal{X}^n$ or an error message e to each index $m \in [1 : 2^{nR})$.

The probability of error for a $(2^{nR}, n)$ lossless source code is defined as $P_e^{(n)} = \mathsf{P}\{\hat{X}^n \neq X^n\}$. A rate R is said to be *achievable* if there exists a sequence of $(2^{nR}, n)$ codes such that $\lim_{n\to\infty} P_e^{(n)} = 0$ (hence the coding is required to be only *asymptotically* error-free). The *optimal rate* R^* for lossless source coding is the infimum of all achievable rates.

3.5.1 Lossless Source Coding Theorem

The optimal compression rate is characterized by the entropy of the source.

Theorem 3.4 (Lossless Source Coding Theorem). The optimal rate for lossless source coding of a discrete memoryless source X is

$$R^* = H(X).$$

For example, the optimal lossless compression rate for a Bern(p) source X is $R^* = H(X) = H(p)$. To prove this theorem, we again need to verify the following two statements:

- **Achievability.** For every $R > R^* = H(X)$ there exists a sequence of $(2^{nR}, n)$ codes with $\lim_{n\to\infty} P_e^{(n)} = 0$. We prove achievability using properties of typical sequences. Two alternative proofs will be given in Sections 3.6.4 and 10.3.1.
- **Converse.** For every sequence of $(2^{nR}, n)$ codes with $\lim_{n\to\infty} P_e^{(n)} = 0$, the source coding rate $R \geq R^* = H(X)$. The proof uses Fano's inequality and basic properties of entropy and mutual information.

We now prove each statement.

3.5.2 Proof of Achievability

For simplicity of presentation, assume nR is an integer. For $\epsilon > 0$, let $R = H(X) + \delta(\epsilon)$ with $\delta(\epsilon) = \epsilon H(X)$. Hence, $|\mathcal{T}_\epsilon^{(n)}| \leq 2^{n(H(X)+\delta(\epsilon))} = 2^{nR}$.

Encoding. Assign a distinct index $m(x^n)$ to each $x^n \in \mathcal{T}_\epsilon^{(n)}$. Assign $m = 1$ to all $x^n \notin \mathcal{T}_\epsilon^{(n)}$.

Decoding. Upon receiving the index m, the decoder declares $\hat{x}^n = x^n(m)$ for the unique $x^n(m) \in \mathcal{T}_\epsilon^{(n)}$.

Analysis of the probability of error. All typical sequences are recovered error-free. Thus, the probability of error is $P_e^{(n)} = \mathsf{P}\{X^n \notin \mathcal{T}_\epsilon^{(n)}\}$, which tends to zero as $n \to \infty$. This completes the proof of achievability.

3.5.3 Proof of the Converse

Given a sequence of $(2^{nR}, n)$ codes with $\lim_{n\to\infty} P_e^{(n)} = 0$, let M be the random variable corresponding to the index generated by the encoder. By Fano's inequality,

$$H(X^n|M) \le H(X^n|\hat{X}^n) \le 1 + nP_e^{(n)} \log|\mathcal{X}| = n\epsilon_n,$$

where ϵ_n tends to zero as $n \to \infty$ by the assumption that $\lim_{n\to\infty} P_e^{(n)} = 0$. Now consider

$$\begin{aligned} nR &\ge H(M) \\ &= I(X^n; M) \\ &= nH(X) - H(X^n|M) \\ &\ge nH(X) - n\epsilon_n. \end{aligned}$$

By taking $n \to \infty$, we conclude that $R \ge H(X)$. This completes the converse proof of the lossless source coding theorem.

3.6 LOSSY SOURCE CODING

Recall the compression system shown in Figure 3.10. Suppose that the source alphabet is continuous, for example, the source is a sensor that outputs an analog signal, then lossless reconstruction of the source sequence would require an infinite transmission rate! This motivates the lossy compression setup we study in this section, where the reconstruction is only required to be *close* to the source sequence according to some *fidelity criterion* (or distortion measure). In the scalar case, where each symbol is separately compressed, this lossy compression setup reduces to scalar quantization (analog-to-digital conversion), which often employs a mean squared error fidelity criterion. As in channel coding, however, it turns out that performing the lossy compression in blocks (vector quantization) can achieve better performance.

Unlike the lossless source coding setup where there is an optimal compression rate, the lossy source coding setup involves a tradeoff between the rate and the desired distortion. The problem is to find the limit on such tradeoff, which we refer to as the rate–distortion function. Note that this function is the source coding equivalent of the capacity–cost function in channel coding.

Although the motivation for lossy compression comes from sources with continuous alphabets, we first consider the problem for a DMS $(\mathcal{X}, p(x))$ as defined in the previous section. We assume the following per-letter distortion criterion. Let $\hat{\mathcal{X}}$ be a *reconstruction* alphabet and define a *distortion measure* as a mapping

$$d\colon \mathcal{X} \times \hat{\mathcal{X}} \to [0, \infty).$$

This mapping measures the cost of representing the symbol x by the symbol $\hat{x}$. The *average distortion* between x^n and $\hat{x}^n$ is defined as

$$d(x^n, \hat{x}^n) = \frac{1}{n}\sum_{i=1}^{n} d(x_i, \hat{x}_i).$$

For example, when $\mathcal{X} = \hat{\mathcal{X}}$, the *Hamming distortion measure* (loss) is the indicator for an error, i.e.,

$$d(x, \hat{x}) = \begin{cases} 1 & \text{if } x \neq \hat{x}, \\ 0 & \text{if } x = \hat{x}. \end{cases}$$

Thus, $d(\hat{x}^n, x^n)$ is the fraction of symbols in error (bit error rate for the binary alphabet).

Formally, a $(2^{nR}, n)$ *lossy source code* consists of

- an encoder that assigns an index $m(x^n) \in [1 : 2^{nR})$ to each sequence $x^n \in \mathcal{X}^n$, and
- a decoder that assigns an estimate $\hat{x}^n(m) \in \hat{\mathcal{X}}^n$ to each index $m \in [1 : 2^{nR})$.

The set $\mathcal{C} = \{\hat{x}^n(1), \ldots, \hat{x}^n(2^{\lfloor nR \rfloor})\}$ constitutes the *codebook*.

The expected distortion associated with a $(2^{nR}, n)$ lossy source code is defined as

$$\mathsf{E}(d(X^n, \hat{X}^n)) = \sum_{x^n} p(x^n) d\big(x^n, \hat{x}^n(m(x^n))\big).$$

A rate–distortion pair (R, D) is said to be *achievable* if there exists a sequence of $(2^{nR}, n)$ codes with

$$\limsup_{n \to \infty} \mathsf{E}(d(X^n, \hat{X}^n)) \leq D. \tag{3.7}$$

The *rate–distortion function* $R(D)$ is the infimum of rates R such that (R, D) is achievable.

3.6.1 Lossy Source Coding Theorem

Shannon showed that mutual information is again the canonical quantity that characterizes the rate–distortion function.

Theorem 3.5 (Lossy Source Coding Theorem). The rate–distortion function for a DMS X and a distortion measure $d(x, \hat{x})$ is

$$R(D) = \min_{p(\hat{x}|x): \mathsf{E}(d(X,\hat{X})) \leq D} I(X; \hat{X})$$

for $D \geq D_{\min} = \min_{\hat{x}(x)} \mathsf{E}[d(X, \hat{x}(X))]$.

Similar to the capacity–cost function in Section 3.3, the rate–distortion function $R(D)$ is nonincreasing, convex, and continuous in $D \geq D_{\min}$ (see Figure 3.11). Unless noted otherwise, we will assume throughout the book that $D_{\min} = 0$, that is, for every symbol $x \in \mathcal{X}$ there exists a reconstruction symbol $\hat{x} \in \hat{\mathcal{X}}$ such that $d(x, \hat{x}) = 0$.

Example 3.4 (Bernoulli source with Hamming distortion). The rate–distortion function for a Bern(p) source X, $p \in [0, 1/2]$, and Hamming distortion measure is

$$R(D) = \begin{cases} H(p) - H(D) & \text{for } 0 \leq D < p, \\ 0 & \text{for } D \geq p. \end{cases}$$

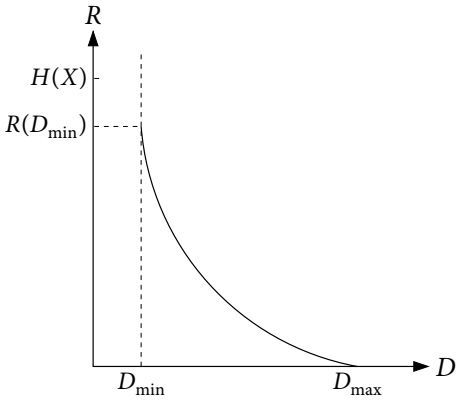


Figure 3.11. Graph of a typical rate–distortion function. Note that $R(D) = 0$ for $D \geq D_{\max} = \min_{\hat{x}} \mathsf{E}(d(X, \hat{x}))$ and $R(D_{\min}) \leq H(X)$.

To show this, recall that

$$R(D) = \min_{p(\hat{x}|x):\mathsf{E}(d(X,\hat{X}))\leq D} I(X; \hat{X}).$$

If $D \geq p$, $R(D) = 0$ by simply taking $\hat{X} = 0$. If $D < p$, we find a lower bound on $R(D)$ and then show that there exists a test channel $p(\hat{x}|x)$ that attains it. For any joint pmf that satisfies the distortion constraint $\mathsf{E}(d(X, \hat{X})) = \mathsf{P}\{X \neq \hat{X}\} \leq D$, we have

$$\begin{aligned} I(X; \hat{X}) &= H(X) - H(X|\hat{X}) \\ &= H(p) - H(X \oplus \hat{X}|\hat{X}) \\ &\geq H(p) - H(X \oplus \hat{X}) \\ &\overset{(a)}{\geq} H(p) - H(D), \end{aligned}$$

where (a) follows since $\mathsf{P}\{X \neq \hat{X}\} \leq D$. Thus

$$R(D) \geq H(p) - H(D).$$

It can be easily shown that this bound is attained by the *backward* BSC (with $\hat{X}$ and Z independent) shown in Figure 3.12, and the associated expected distortion is D.

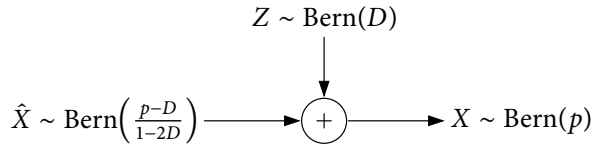


Figure 3.12. The backward BSC (test channel) that attains the rate–distortion function $R(D)$.

3.6.2 Proof of the Converse

The proof of the lossy source coding theorem again requires establishing achievability and the converse. We first prove the converse.

We need to show that for any sequence of $(2^{nR}, n)$ codes with

$$\limsup_{n\to\infty} \mathsf{E}(d(X^n, \hat{X}^n)) \le D, \tag{3.8}$$

we must have $R \ge R(D)$. Consider

$$\begin{aligned}
nR &\ge H(M) \\
&\ge I(M; X^n) \\
&\ge I(\hat{X}^n; X^n) \\
&= \sum_{i=1}^{n} I(X_i; \hat{X}^n | X^{i-1}) \\
&\overset{(a)}{=} \sum_{i=1}^{n} I(X_i; \hat{X}^n, X^{i-1}) \\
&\ge \sum_{i=1}^{n} I(X_i; \hat{X}_i) \\
&\overset{(b)}{\ge} \sum_{i=1}^{n} R\big(\mathsf{E}[d(X_i, \hat{X}_i)]\big) \\
&\overset{(c)}{\ge} nR\big(\mathsf{E}[d(X^n, \hat{X}^n)]\big),
\end{aligned}$$

where (a) follows by the memoryless property of the source, (b) follows by the definition of $R(D) = \min I(X; \hat{X})$, and (c) follows by the convexity of $R(D)$. Since $R(D)$ is continuous and nonincreasing in D, it follows from the bound on distortion in (3.8) that

$$R \ge \limsup_{n\to\infty} R\big(\mathsf{E}[d(X^n, \hat{X}^n)]\big) \ge R\Big(\limsup_{n\to\infty} \mathsf{E}[d(X^n, \hat{X}^n)]\Big) \ge R(D).$$

This completes the proof of the converse.

3.6.3 Proof of Achievability

The proof uses random coding and joint typicality encoding. Assume that nR is an integer.

Random codebook generation. Fix the conditional pmf $p(\hat{x}|x)$ that attains $R(D/(1+\epsilon))$, where D is the desired distortion, and let $p(\hat{x}) = \sum_x p(x)p(\hat{x}|x)$. Randomly and independently generate 2^{nR} sequences $\hat{x}^n(m)$, $m \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^{n} p_{\hat{X}}(\hat{x}_i)$. These sequences constitute the codebook $\mathcal{C}$, which is revealed to the encoder and the decoder.

Encoding. We use *joint typicality encoding*. Given a sequence x^n, find an index m such that $(x^n, \hat{x}^n(m)) \in \mathcal{T}_\epsilon^{(n)}$. If there is more than one such index, choose the smallest one among them. If there is no such index, set $m = 1$.

Decoding. Upon receiving the index m, the decoder sets the reconstruction sequence $\hat{x}^n = \hat{x}^n(m)$.

Analysis of expected distortion. Let $\epsilon' < \epsilon$ and M be the index chosen by the encoder. We bound the distortion averaged over the random choice of the codebook $\mathcal{C}$. Define the "encoding error" event

$$\mathcal{E} = \{(X^n, \hat{X}^n(M)) \notin \mathcal{T}_\epsilon^{(n)}\},$$

and consider the events

$$\mathcal{E}_1 = \{X^n \notin \mathcal{T}_{\epsilon'}^{(n)}\},$$
$$\mathcal{E}_2 = \{X^n \in \mathcal{T}_{\epsilon'}^{(n)}, (X^n, \hat{X}^n(m)) \notin \mathcal{T}_\epsilon^{(n)} \text{ for all } m \in [1 : 2^{nR}]\}.$$

Then by the union of events bound,

$$\mathsf{P}(\mathcal{E}) \le \mathsf{P}(\mathcal{E}_1) + \mathsf{P}(\mathcal{E}_2).$$

We bound each term. By the LLN, the first term $\mathsf{P}(\mathcal{E}_1)$ tends to zero as $n \to \infty$. Consider the second term

$$\begin{aligned}
\mathsf{P}(\mathcal{E}_2) &= \sum_{x^n \in \mathcal{T}_{\epsilon'}^{(n)}} p(x^n)\, \mathsf{P}\{(x^n, \hat{X}^n(m)) \notin \mathcal{T}_\epsilon^{(n)} \text{ for all } m \mid X^n = x^n\} \\
&= \sum_{x^n \in \mathcal{T}_{\epsilon'}^{(n)}} p(x^n) \prod_{m=1}^{2^{nR}} \mathsf{P}\{(x^n, \hat{X}^n(m)) \notin \mathcal{T}_\epsilon^{(n)}\} \\
&= \sum_{x^n \in \mathcal{T}_{\epsilon'}^{(n)}} p(x^n) \big(\mathsf{P}\{(x^n, \hat{X}^n(1)) \notin \mathcal{T}_\epsilon^{(n)}\}\big)^{2^{nR}}.
\end{aligned}$$

Since $x^n \in \mathcal{T}_{\epsilon'}^{(n)}$ and $\hat{X}^n(1) \sim \prod_{i=1}^n p_{\hat{X}}(\hat{x}_i)$, it follows by the second part of the joint typicality lemma in Section 2.5 that for n sufficiently large

$$\mathsf{P}\{(x^n, \hat{X}^n(1)) \in \mathcal{T}_\epsilon^{(n)}\} \ge 2^{-n(I(X;\hat{X})+\delta(\epsilon))},$$

where $\delta(\epsilon)$ tends to zero as $\epsilon \to 0$. Since $(1-x)^k \le e^{-kx}$ for $x \in [0,1]$ and $k \ge 0$, we have

$$\begin{aligned}
\sum_{x^n \in \mathcal{T}_{\epsilon'}^{(n)}} p(x^n) \big(\mathsf{P}\{(x^n, \hat{X}^n(1)) \notin \mathcal{T}_\epsilon^{(n)}\}\big)^{2^{nR}} &\le \big(1 - 2^{-n(I(X;\hat{X})+\delta(\epsilon))}\big)^{2^{nR}} \\
&\le \exp\big(-2^{nR} \cdot 2^{-n(I(X;\hat{X})+\delta(\epsilon))}\big) \\
&= \exp\big(-2^{n(R-I(X;\hat{X})-\delta(\epsilon))}\big),
\end{aligned}$$

which tends to zero as $n \to \infty$ if $R > I(X;\hat{X}) + \delta(\epsilon)$.

Now, by the law of total expectation and the typical average lemma,

$$\begin{aligned}
\mathsf{E}_{\mathcal{C},X^n}\big[d(X^n, \hat{X}^n(M))\big] &= \mathsf{P}(\mathcal{E})\, \mathsf{E}_{\mathcal{C},X^n}\big[d(X^n, \hat{X}^n(M)) \big| \mathcal{E}\big] + \mathsf{P}(\mathcal{E}^c)\, \mathsf{E}_{\mathcal{C},X^n}\big[d(X^n, \hat{X}^n(M)) \big| \mathcal{E}^c\big] \\
&\le \mathsf{P}(\mathcal{E})\, d_{\max} + \mathsf{P}(\mathcal{E}^c)(1+\epsilon)\, \mathsf{E}(d(X, \hat{X})),
\end{aligned}$$

where $d_{\max} = \max_{(x,\hat{x})\in\mathcal{X}\times\hat{\mathcal{X}}} d(x,\hat{x})$. Hence, by the assumption on the conditional pmf $p(\hat{x}|x)$ that $\mathsf{E}(d(X,\hat{X})) \le D/(1+\epsilon)$,

$$\limsup_{n\to\infty} \mathsf{E}_{\mathcal{C},X^n}\big[d(X^n,\hat{X}^n(M))\big] \le D$$

if $R > I(X;\hat{X}) + \delta(\epsilon) = R(D/(1+\epsilon)) + \delta(\epsilon)$. Since the expected distortion (averaged over codebooks) is asymptotically $\le D$, there must exist a sequence of codes with expected distortion asymptotically $\le D$, which proves the achievability of the rate–distortion pair $(R(D/(1+\epsilon)) + \delta(\epsilon), D)$. Finally, by the continuity of $R(D)$ in D, it follows that the achievable rate $R(D/(1+\epsilon)) + \delta(\epsilon)$ converges to $R(D)$ as $\epsilon \to 0$, which completes the proof of achievability.

Remark 3.9. The above proof can be extended to unbounded distortion measures, provided that there exists a symbol $\hat{x}_0$ such that $d(x,\hat{x}_0) < \infty$ for every x. In this case, encoding is modified so that $\hat{x}^n = (\hat{x}_0,\ldots,\hat{x}_0)$ whenever joint typicality encoding fails. For example, for an erasure distortion measure with $\mathcal{X} = \{0,1\}$ and $\hat{\mathcal{X}} = \{0,1,\mathrm{e}\}$, where $d(0,0) = d(1,1) = 0$, $d(0,\mathrm{e}) = d(1,\mathrm{e}) = 1$, and $d(0,1) = d(1,0) = \infty$, we have $\hat{x}_0 = \mathrm{e}$. When $X \sim \mathrm{Bern}(1/2)$, it can be easily shown that $R(D) = 1 - D$.

3.6.4 Lossless Source Coding Revisited

We show that the lossless source coding theorem can be viewed as a *corollary* of the lossy source coding theorem. This leads to an alternative *random coding* achievability proof of the lossless source coding theorem. Consider the lossy source coding problem for a DMS X, reconstruction alphabet $\hat{\mathcal{X}} = \mathcal{X}$, and Hamming distortion measure. Setting $D = 0$, we obtain

$$R(0) = \min_{p(\hat{x}|x):\mathsf{E}(d(X,\hat{X}))=0} I(X;\hat{X}) = I(X;X) = H(X),$$

which is equal to the optimal lossless source coding rate R^* as we have already seen in the lossless source coding theorem.

Here we prove that operationally $R^* = R(0)$ without resorting to the fact that $R^* = H(X)$. To prove the converse ($R^* \ge R(0)$), note that the converse for the lossy source coding theorem under the above conditions implies that for any sequence of $(2^{nR}, n)$ codes if the average symbol error probability

$$\frac{1}{n}\sum_{i=1}^{n} \mathsf{P}\{\hat{X}_i \ne X_i\}$$

tends to zero as $n \to \infty$, then $R \ge R(0)$. Since the average symbol error probability is smaller than or equal to the block error probability $\mathsf{P}\{\hat{X}^n \ne X^n\}$, this also establishes the converse for the lossless case.

To prove achievability ($R^* \le R(0)$), we can still use random coding and joint typicality encoding! We fix a test channel

$$p(\hat{x}|x) = \begin{cases} 1 & \text{if } x = \hat{x}, \\ 0 & \text{otherwise,} \end{cases}$$

and define $\mathcal{T}_\epsilon^{(n)}(X, \hat{X})$ in the usual way. Then, $(x^n, \hat{x}^n) \in \mathcal{T}_\epsilon^{(n)}$ implies that $x^n = \hat{x}^n$. Following the achievability proof of the lossy source coding theorem, we generate a random code $\hat{x}^n(m)$, $m \in [1 : 2^{nR}]$, and use the same encoding and decoding procedures. Then, the probability of decoding error averaged over codebooks is upper bounded as

$$\mathsf{P}(\mathcal{E}) \le \mathsf{P}\{(X^n, \hat{X}^n) \notin \mathcal{T}_\epsilon^{(n)}\},$$

which tends to zero as $n \to \infty$ if $R > I(X; \hat{X}) + \delta(\epsilon) = R(0) + \delta(\epsilon)$. Thus there exists a sequence of $(2^{nR}, n)$ lossless source codes with $\lim_{n\to\infty} P_e^{(n)} = 0$.

Remark 3.10. We already know how to construct a sequence of asymptotically optimal lossless source codes by uniquely labeling each typical sequence. The above proof, however, shows that random coding can be used to establish *all* point-to-point communication coding theorems. Such unification shows the power of random coding and is aesthetically pleasing. More importantly, the technique of specializing a lossy source coding theorem to the lossless case will prove crucial later in Chapters 11 and 21.

3.7 COVERING LEMMA

The covering lemma generalizes the bound on the probability of the encoding error event $\mathcal{E}$ in the achievability proof of the lossy source coding theorem. The lemma will be used in the achievability proofs of several multiuser source and channel coding theorems.

Recall that in the bound on $\mathsf{P}(\mathcal{E})$, we had a fixed conditional pmf $p(\hat{x}|x)$ and a source $X \sim p(x)$. As illustrated in Figure 3.13, we considered a set of 2^{nR} i.i.d. reconstruction sequences $\hat{X}^n(m)$, $m \in [1 : 2^{nR}]$, each distributed according to $\prod_{i=1}^n p_{\hat{X}}(\hat{x}_i)$ and an independently generated source sequence $X^n \sim \prod_{i=1}^n p_X(x_i)$. We showed that the probability that $(X^n, \hat{X}^n(m)) \in \mathcal{T}_\epsilon^{(n)}$ for some $m \in [1 : 2^{nR}]$ tends to one as $n \to \infty$ if $R > I(X; \hat{X}) + \delta(\epsilon)$.

The following lemma extends this bound by assuming that X^n and the set of codewords are conditionally independent given a sequence U^n with the condition that U^n and X^n are jointly typical with high probability. As such, the covering lemma is a dual to the packing lemma in which we do not wish any of the untransmitted (independent) codewords to be jointly typical with the received sequence given U^n.

Lemma 3.3 (Covering Lemma). Let $(U, X, \hat{X}) \sim p(u, x, \hat{x})$ and $\epsilon' < \epsilon$. Let $(U^n, X^n) \sim p(u^n, x^n)$ be a pair of random sequences with $\lim_{n\to\infty} \mathsf{P}\{(U^n, X^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U, X)\} = 1$, and let $\hat{X}^n(m)$, $m \in \mathcal{A}$, where $|\mathcal{A}| \ge 2^{nR}$, be random sequences, conditionally independent of each other and of X^n given U^n, each distributed according to $\prod_{i=1}^n p_{\hat{X}|U}(\hat{x}_i|u_i)$. Then, there exists $\delta(\epsilon)$ that tends to zero as $\epsilon \to 0$ such that

$$\lim_{n\to\infty} \mathsf{P}\{(U^n, X^n, \hat{X}^n(m)) \notin \mathcal{T}_\epsilon^{(n)} \text{ for all } m \in \mathcal{A}\} = 0,$$

if $R > I(X; \hat{X}|U) + \delta(\epsilon)$.

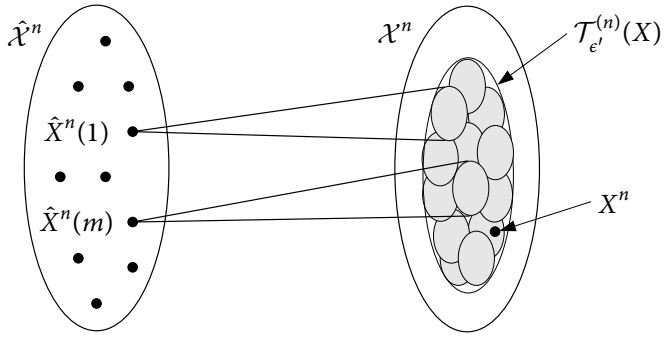


Figure 3.13. Illustration of the setup for the bound on $\mathsf{P}(\mathcal{E})$.

Proof. Define the event

$$\mathcal{E}_0 = \{(U^n, X^n) \notin \mathcal{T}_{\epsilon'}^{(n)}\}.$$

Then, the probability of the event of interest can be upper bounded as

$$\mathsf{P}(\mathcal{E}) \le \mathsf{P}(\mathcal{E}_0) + \mathsf{P}(\mathcal{E} \cap \mathcal{E}_0^c).$$

By the condition of the lemma, $\mathsf{P}(\mathcal{E}_0)$ tends to zero as $n \to \infty$. For the second term, recall from the joint typicality lemma that if $(u^n, x^n) \in \mathcal{T}_{\epsilon'}^{(n)}$, then for n sufficiently large,

$$\begin{aligned}\mathsf{P}\{(u^n, x^n, \hat{X}^n(m)) \in \mathcal{T}_{\epsilon}^{(n)} \,|\, U^n = u^n, X^n = x^n\} &= \mathsf{P}\{(u^n, x^n, \hat{X}^n(m)) \in \mathcal{T}_{\epsilon}^{(n)} \,|\, U^n = u^n\} \\ &\ge 2^{-n(I(X;\hat{X}|U)+\delta(\epsilon))}\end{aligned}$$

for each $m \in \mathcal{A}$ for some $\delta(\epsilon)$ that tends to zero as $\epsilon \to 0$. Hence, for n sufficiently large,

$$\begin{aligned}\mathsf{P}(\mathcal{E} \cap \mathcal{E}_0^c) &= \sum_{(u^n,x^n)\in\mathcal{T}_{\epsilon'}^{(n)}} p(u^n, x^n)\, \mathsf{P}\{(u^n, x^n, \hat{X}^n(m)) \notin \mathcal{T}_{\epsilon}^{(n)} \text{ for all } m \,|\, U^n = u^n, X^n = x^n\} \\ &= \sum_{(u^n,x^n)\in\mathcal{T}_{\epsilon'}^{(n)}} p(u^n, x^n) \prod_{m\in\mathcal{A}} \mathsf{P}\{(u^n, x^n, \hat{X}^n(m)) \notin \mathcal{T}_{\epsilon}^{(n)} \,|\, U^n = u^n\} \\ &\le \big(1 - 2^{-n(I(X;\hat{X}|U)+\delta(\epsilon))}\big)^{|\mathcal{A}|} \\ &\le \exp\big(-|\mathcal{A}| \cdot 2^{-n(I(X;\hat{X}|U)+\delta(\epsilon))}\big) \\ &\le \exp\big(-2^{n(R-I(X;\hat{X}|U)-\delta(\epsilon))}\big),\end{aligned}$$

which tends to zero as $n \to \infty$, provided $R > I(X; \hat{X}|U) + \delta(\epsilon)$. This completes the proof.

Remark 3.11. The covering lemma continues to hold even when independence among all the sequences $\hat{X}^n(m)$, $m \in \mathcal{A}$, is replaced with pairwise independence; see the mutual covering lemma in Section 8.3.

3.8 QUADRATIC GAUSSIAN SOURCE CODING

We motivated the need for lossy source coding by considering compression of continuous-alphabet sources. In this section, we study lossy source coding of a Gaussian source, which is an important example of a continuous-alphabet source and is often used to model real-world analog signals such as video and speech.

Let X be a WGN(P) source, that is, a source that generates a WGN(P) random process $\{X_i\}$. We consider a lossy source coding problem for the source X with *quadratic (squared error) distortion measure* $d(x, \hat{x}) = (x - \hat{x})^2$ on $\mathbb{R}^2$. The rate–distortion function for this quadratic Gaussian source coding problem can be defined in the exact same manner as for the DMS case. Furthermore, Theorem 3.5 with the minimum over arbitrary test channels applies and the rate–distortion function can be expressed simply in terms of the power-to-distortion ratio.

Theorem 3.6. The rate–distortion function for a WGN(P) source with squared error distortion measure is

$$R(D) = \inf_{F(\hat{x}|x):\mathsf{E}((X-\hat{X})^2)\le D} I(X;\hat{X}) = \mathsf{R}\left(\frac{P}{D}\right),$$

where $\mathsf{R}(x) = (1/2)[\log x]^+$ is the quadratic Gaussian rate function.

Proof of the converse. It is easy to see that the converse proof for the lossy source coding theorem extends to continuous sources with well-defined density such as Gaussian, and we have

$$R(D) \ge \inf_{F(\hat{x}|x):\mathsf{E}((X-\hat{X})^2)\le D} I(X;\hat{X}). \tag{3.9}$$

For $D \ge P$, we set $\hat{X} = \mathsf{E}(X) = 0$; thus $R(D) = 0$. For $0 \le D < P$, we first find a lower bound on the infimum in (3.9) and then show that there exists a test channel that attains it. Consider

$$\begin{aligned}
I(X;\hat{X}) &= h(X) - h(X|\hat{X}) \\
&= \frac{1}{2}\log(2\pi eP) - h(X-\hat{X}|\hat{X}) \\
&\ge \frac{1}{2}\log(2\pi eP) - h(X-\hat{X}) \\
&\ge \frac{1}{2}\log(2\pi eP) - \frac{1}{2}\log(2\pi e\,\mathsf{E}[(X-\hat{X})^2]) \\
&\overset{(a)}{\ge} \frac{1}{2}\log(2\pi eP) - \frac{1}{2}\log(2\pi eD) \\
&= \frac{1}{2}\log\frac{P}{D},
\end{aligned}$$

where (a) follows since $\mathsf{E}((X-\hat{X})^2) \le D$. It is easy to show that this bound is attained by the backward Gaussian test channel shown in Figure 3.14 and that the associated expected distortion is D.

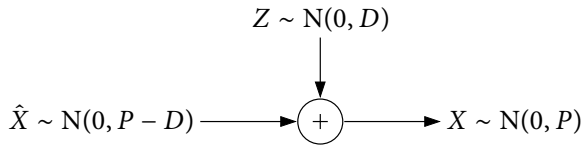


Figure 3.14. The backward Gaussian test channel that attains the minimum in (3.9).

Proof of achievability. We extend the achievability proof for the DMS to the case of a Gaussian source with quadratic distortion measure by using the following discretization procedure. Let D be the desired distortion and let $(X, \hat{X})$ be a pair of jointly Gaussian random variables attaining $I(X;\hat{X}) = R((1-2\epsilon)D)$ with distortion $\mathsf{E}((X-\hat{X})^2) = (1-2\epsilon)D$. Let $[X]$ and $[\hat{X}]$ be finitely quantized versions of X and $\hat{X}$, respectively, such that

$$\begin{aligned} \mathsf{E}\big(([X]-[\hat{X}])^2\big) &\le (1-\epsilon)^2 D, \\ \mathsf{E}\big((X-[X])^2\big) &\le \epsilon^2 D. \end{aligned} \tag{3.10}$$

Then by the data processing inequality,

$$I([X];[\hat{X}]) \le I(X;\hat{X}) = R((1-2\epsilon)D).$$

Now, by the achievability proof for the DMS $[X]$ and reconstruction $[\hat{X}]$, there exists a sequence of $(2^{nR}, n)$ rate–distortion codes with asymptotic distortion

$$\limsup_{n\to\infty} \frac{1}{n}\,\mathsf{E}\big(d([X]^n, [\hat{X}]^n)\big) \le (1-\epsilon)^2 D, \tag{3.11}$$

if $R > R((1-2\epsilon)D) \ge I([X];[\hat{X}])$. We use this sequence of codes for the original source X by mapping each x^n to the codeword $[\hat{x}]^n$ that is assigned to $[x]^n$. Then

$$\begin{aligned} \limsup_{n\to\infty} \mathsf{E}\big(d(X^n, [\hat{X}]^n)\big) &= \limsup_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \mathsf{E}\big((X_i - [\hat{X}]_i)^2\big) \\ &= \limsup_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \mathsf{E}\big(((X_i-[X_i]) + ([X_i]-[\hat{X}]_i))^2\big) \\ &\overset{(a)}{\le} \limsup_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \Big(\mathsf{E}\big((X_i-[X_i])^2\big) + \mathsf{E}\big(([X_i]-[\hat{X}]_i)^2\big)\Big) \\ &\qquad + \limsup_{n\to\infty} \frac{2}{n}\sum_{i=1}^{n} \sqrt{\mathsf{E}\big((X_i-[X_i])^2\big)\,\mathsf{E}\big(([X_i]-[\hat{X}]_i)^2\big)} \\ &\overset{(b)}{\le} \epsilon^2 D + (1-\epsilon)^2 D + 2\epsilon(1-\epsilon)D \\ &= D, \end{aligned}$$

where (a) follows by Cauchy's inequality and (b) follows by (3.10) and (3.11), and Jensen's inequality. Thus, $R > R((1-2\epsilon)D)$ is achievable for distortion D. Using the continuity of $R(D)$ completes the proof of achievability.

3.9 JOINT SOURCE–CHANNEL CODING

In previous sections we studied limits on communication of compressed sources over noisy channels and uncompressed sources over noiseless channels. In this section, we study the more general joint source–channel coding setup depicted in Figure 3.15. The sender wishes to communicate k symbols of an uncompressed source U over a DMC $p(y|x)$ in n transmissions so that the receiver can reconstruct the source symbols with a prescribed distortion D. A straightforward scheme would be to perform separate source and channel encoding and decoding. Is this separation scheme optimal? Can we do better by allowing more general joint source–channel encoding and decoding?

Figure 3.15. Joint source–channel coding setup.

It turns out that separate source and channel coding is asymptotically optimal for sending a DMS over a DMC, and hence the fundamental limit depends only on the rate–distortion function of the source and the capacity of the channel.

Formally, let U be a DMS and $d(u, \hat{u})$ be a distortion measure with rate–distortion function $R(D)$ and $p(y|x)$ be a DMC with capacity C. A $(|\mathcal{U}|^k, n)$ joint source–channel code of rate $r = k/n$ consists of

- an encoder that assigns a codeword $x^n(u^k) \in \mathcal{X}^n$ to each sequence $u^k \in \mathcal{U}^k$ and
- a decoder that assigns an estimate $\hat{u}^k(y^n) \in \hat{\mathcal{U}}^k$ to each sequence $y^n \in \mathcal{Y}^n$.

A rate–distortion pair (r, D) is said to be achievable if there exists a sequence of $(|\mathcal{U}|^k, n)$ joint source–channel codes of rate r such that

$$\limsup_{k\to\infty} \mathsf{E}\big[d(U^k, \hat{U}^k(Y^n))\big] \le D.$$

Shannon established the following fundamental limit on joint source–channel coding.

Theorem 3.7 (Source–Channel Separation Theorem). Given a DMS U and a distortion measure $d(u, \hat{u})$ with rate–distortion function $R(D)$ and a DMC $p(y|x)$ with capacity C, the following statements hold:

- If $rR(D) < C$, then (r, D) is achievable.
- If (r, D) is achievable, then $rR(D) \le C$.

Proof of achievability. We use separate lossy source coding and channel coding.

- Source coding: For any $\epsilon > 0$, there exists a sequence of lossy source codes with rate $R(D/(1+\epsilon)) + \delta(\epsilon)$ that achieve expected distortion less than or equal to D. We treat the index for each code in the sequence as a message to be sent over the channel.
- Channel coding: The sequence of source indices can be reliably communicated over the channel if $r(R(D/(1+\epsilon)) + \delta(\epsilon)) \le C - \delta'(\epsilon)$.

The source decoder finds the reconstruction sequence corresponding to the received index. If the channel decoder makes an error, the distortion is upper bounded by $d_{\max}$. Because the probability of error tends to zero as $n \to \infty$, the overall expected distortion is less than or equal to D.

Proof of the converse. We wish to show that if a sequence of codes achieves the rate–distortion pair (r, D), then $rR(D) \le C$. By the converse proof of the lossy source coding theorem, we know that

$$R(D) \le \frac{1}{k} I(U^k; \hat{U}^k).$$

Now, by the data processing inequality,

$$\frac{1}{k} I(U^k; \hat{U}^k) \le \frac{1}{k} I(U^k; Y^n).$$

Following similar steps to the converse proof for the DMC, we have

$$\frac{1}{k} I(U^k; Y^n) \le \frac{1}{k} \sum_{i=1}^{n} I(X_i; Y_i) \le \frac{1}{r} C.$$

Combining the above inequalities completes the proof of the converse.

Remark 3.12. Since the converse of the channel coding theorem holds when causal feedback is present (see Section 3.1.5), the separation theorem continues to hold with feedback.

Remark 3.13. As in Remark 3.5, there are cases where $rR(D) = C$ and the rate–distortion pair (r, D) is achievable via joint source–channel coding; see Example 3.5. However, if $rR(D) > C$, the rate–distortion pair (r, D) is not achievable. Hence, we informally say that source–channel separation holds in general for sending a DMS over a DMC.

Remark 3.14. As a special case of joint source–channel coding, consider the problem of sending U over a DMC losslessly, i.e., $\lim_{k\to\infty} \mathsf{P}\{\hat{U}^k \neq U^k\} = 0$. The separation theorem holds with the requirement that $rH(U) \le C$.

Remark 3.15. The separation theorem can be extended to sending an arbitrary stationary ergodic source over a DMC.

Remark 3.16. As we will see in Chapter 14, source–channel separation does not hold in general for communicating multiple sources over multiuser channels, that is, even in the asymptotic regime, it may be beneficial to leverage the structure of the source and channel jointly rather than separately.

3.9.1 Uncoded Transmission

Sometimes optimal joint source–channel coding is simpler than separate source and channel coding. This is illustrated in the following.

Example 3.5. Consider communicating a Bern(1/2) source over a BSC(p) at rate $r = 1$ with Hamming distortion less than or equal to D. The separation theorem shows that $1 - H(D) < 1 - H(p)$, or equivalently, $D > p$, can be achieved using separate source and channel coding. More simply, we can transmit the binary sequence over the channel *without any coding* and achieve average distortion $D = p$!

Similar *uncoded transmission* is optimal also for communicating a Gaussian source over a Gaussian channel with quadratic distortion (with proper scaling to satisfy the power constraint); see Problem 3.20.

Remark 3.17. In general, we have the following condition for the optimality of uncoded transmission. A DMS U can be communicated over a DMC $p(y|x)$ uncoded if $X \sim p_U(x)$ attains the capacity $C = \max_{p(x)} I(X;Y)$ of the channel and the test channel $p_{Y|X}(\hat{u}|u)$ attains the rate–distortion function $R(D) = \min_{p(\hat{u}|u):\mathsf{E}(d(U,\hat{U}))\le D} I(U;\hat{U})$ of the source. In this case, $C = R(D)$.

SUMMARY

- Point-to-point communication system architecture
- Discrete memoryless channel (DMC), e.g., BSC and BEC
- Coding theorem: achievability and the converse
- Channel capacity is the limit on channel coding
- Random codebook generation
- Joint typicality decoding
- Packing lemma
- Feedback does not increase the capacity of a DMC
- Capacity with input cost
- Gaussian channel:
  - Capacity with average power constraint is achieved via Gaussian codes
  - Extending the achievability proof from discrete to Gaussian
  - Minimum energy per bit
  - Water filling
- Discrete memoryless source (DMS)

- Entropy is the limit on lossless source coding
- Joint typicality encoding
- Covering lemma
- Rate–distortion function is the limit on lossy source coding
- Rate–distortion function for Gaussian source with quadratic distortion
- Lossless source coding theorem is a corollary of lossy source coding theorem
- Source–channel separation
- Uncoded transmission can be optimal

BIBLIOGRAPHIC NOTES

The channel coding theorem was first proved in Shannon (1948). There are alternative proofs of achievability for this theorem that yield stronger results, including Feinstein's (1954) maximal coding theorem and Gallager's (1965) random coding exponent technique, which yield stronger results. For example, it can be shown (Gallager 1968) that the probability of error decays exponentially fast in the block length and the random coding exponent technique gives a very good bound on the optimal error exponent (reliability function) for the DMC. These proofs, however, do not extend easily to many multiuser channel and source coding problems. In comparison, the current proof (Forney 1972, Cover 1975b), which is based on Shannon's original arguments, is much simpler and can be readily extended to more complex settings. Hence we will adopt random codebook generation and joint typicality decoding throughout.

The achievability proof of the channel coding theorem for the BSC using a random linear code is due to Elias (1955). Even though random linear codes allow for computationally efficient encoding (by simply multiplying the message by a *generator matrix* G), decoding still requires an exponential search, which limits its practical value. This problem can be mitigated by considering a linear code ensemble with special structures, such as Gallager's (1963) low density parity check (LDPC) codes, which have efficient decoding algorithms and achieve rates close to capacity (Richardson and Urbanke 2008). A more recently developed class of capacity-achieving linear codes is polar codes (Arıkan 2009), which involve an elegant information theoretic low-complexity decoding algorithm and can be applied also to lossy compression settings (Korada and Urbanke 2010). Linear codes for the BSC or BEC are examples of structured codes. Other examples include lattice codes for the Gaussian channel, which have been shown to achieve the capacity by Erez and Zamir (2004); see Zamir (2009) for a survey of recent developments.

The converse of the channel coding theorem states that if $R > C$, then $P_e^{(n)}$ is bounded away from zero as $n \to \infty$. This is commonly referred to as the *weak converse*. In comparison, the *strong converse* (Wolfowitz 1957) states that if $R > C$, then $\lim_{n\to\infty} P_e^{(n)} = 1$. A similar statement holds for the lossless source coding theorem. However, except for a few

cases to be discussed later, it appears to be difficult to prove the strong converse for most multiuser settings. As such, we only present weak converse proofs in our main exposition.

The capacity formula for the Gaussian channel under average power constraint in Theorem 3.3 is due to Shannon (1948). The achievability proof using the discretization procedure follows McEliece (1977). Alternative proofs of achievability for the Gaussian channel can be found in Gallager (1968) and Cover and Thomas (2006). The discrete-time Gaussian channel is the model for a continuous-time (waveform) bandlimited Gaussian channel with bandwidth $W = 1/2$, noise power spectral density (psd) $N_0/2$, average transmission power P (area under psd of signal), and channel gain g. If the channel has bandwidth W, then it is equivalent to $2W$ parallel discrete-time Gaussian channels (per second) and the capacity (see, for example, Wyner (1966) and Slepian (1976)) is

$$C = W \log\left(1 + \frac{g^2 P}{W N_0}\right) \quad \text{bits/second.}$$

For a wideband channel, the capacity C converges to $(S/2)\ln 2$ as $W \to \infty$, where $S = 2g^2P/N_0$. Thus the capacity grows linearly with S and can be achieved via simple binary code as shown by Golay (1949). The minimum energy per bit for the Gaussian channel also first appeared in this paper. The minimum energy per bit can be also viewed as a special case of the reciprocal of the capacity per unit cost studied by Csiszár and Körner (1981b, p. 120) and Verdú (1990). The capacity of the spectral Gaussian channel, which is the continuous counterpart of the Gaussian product channel, and its water-filling solution are due to Shannon (1949a).

The lossless source coding theorem was first proved in Shannon (1948). In many applications, one cannot afford to have any errors introduced by compression. Error-free compression ($\mathsf{P}\{X^n \neq \hat{X}^n\} = 0$) for fixed-length codes, however, requires that $R \geq \log|\mathcal{X}|$. Using *variable-length* codes, Shannon (1948) also showed that error-free compression is possible if the average rate of the code is larger than the entropy $H(X)$. Hence, the limit on the average achievable rate is the same for both lossless and error-free compression. This is not true in general for distributed coding of correlated sources; see Bibliographic Notes in Chapter 10.

The lossy source coding theorem was first proved in Shannon (1959), following an earlier result for the quadratic Gaussian case in Shannon (1948). The current achievability proof of the quadratic Gaussian lossy source coding theorem follows McEliece (1977). There are several other ways to prove achievability for continuous sources and unbounded distortion measures (Berger 1968, Dunham 1978, Bucklew 1987, Cover and Thomas 2006). As an alternative to the expected distortion criterion in (3.7), several authors have considered the stronger criterion

$$\lim_{n\to\infty} \mathsf{P}\{d(X^n, \hat{x}^n(m(X^n))) \leq D\} = 0$$

in the definition of achievability of a rate–distortion pair (R, D). The lossy source coding theorem and its achievability proof in Section 3.6 continue to hold for this alternative distortion criterion. In the other direction, a strong converse—if $R < R(D)$, then

$\mathsf{P}\{d(X^n, \hat{X}^n) \le D\}$ tends to zero as $n \to \infty$—can be established (Csiszár and Körner 1981b, Theorem 2.3) that implies the converse for the expected distortion criterion.

The lossless source coding theorem can be extended to discrete stationary ergodic (not necessarily i.i.d.) sources (Shannon 1948). Similarly, the lossy source coding theorem can be extended to stationary ergodic sources (Gallager 1968) with the following characterization of the rate–distortion function

$$R(D) = \lim_{k\to\infty} \min_{p(\hat{x}^k|x^k):\mathsf{E}(d(X^k,\hat{X}^k))\le D} \frac{1}{k} I(X^k; \hat{X}^k).$$

However, the notion of ergodicity for channels is more subtle and involved. Roughly speaking, the capacity is well-defined for discrete channels such that for every time $i \ge 1$ and shift $j \ge 1$, the conditional pmf $p(y_i^{j+i}|x_i^{j+i})$ is time invariant (that is, independent of i) and can be estimated using appropriate time averages. For example, if $Y_i = g(X_i, Z_i)$ for some stationary ergodic process $\{Z_i\}$, then it can be shown (Kim 2008b) that the capacity is

$$C = \lim_{k\to\infty} \sup_{p(x^k)} \frac{1}{k} I(X^k; Y^k).$$

The coding theorem for more general classes of channels with memory can be found in Gray (1990) and Verdú and Han (1994). As for point-to-point communication, the essence of the multiuser source and channel coding problems is captured by the memoryless case. Moreover, the multiuser problems with memory often have only uncomputable "multiletter" expressions as above. We therefore restrict our attention to discrete memoryless and white Gaussian noise sources and channels.

The source–channel separation theorem was first proved in Shannon (1959). The general condition for optimality of uncoded transmission in Remark 3.17 is given by Gastpar, Rimoldi, and Vetterli (2003).

PROBLEMS

3.1. *Memoryless property.* Show that under the given definition of a $(2^{nR}, n)$ code, the memoryless property $p(y_i|x^i, y^{i-1}, m) = p_{Y|X}(y_i|x_i)$, $i \in [1 : n]$, reduces to

$$p(y^n|x^n, m) = \prod_{i=1}^{n} p_{Y|X}(y_i|x_i).$$

3.2. *Z channel.* The Z channel has binary input and output alphabets, and conditional pmf $p(0|0) = 1$, $p(1|1) = p(0|1) = 1/2$. Find the capacity C.

3.3. *Capacity of the sum channel.* Find the capacity C of the union of two DMCs $(\mathcal{X}_1, p(y_1|x_1), \mathcal{Y}_1)$ and $(\mathcal{X}_2, p(y_2|x_2), \mathcal{Y}_2)$, where, in each transmission, one can send a symbol over channel 1 or channel 2 but not both. Assume that the output alphabets are distinct, i.e., $\mathcal{Y}_1 \cap \mathcal{Y}_2 = \emptyset$.

3.4. *Applications of the packing lemma.* Identify the random variables U, X, and Y in the packing lemma for the following scenarios, and write down the packing lemma condition on the rate R for each case.

(a) Let $(X_1, X_2, X_3) \sim p(x_1)p(x_2)p(x_3|x_1, x_2)$. Let $X_1^n(m)$, $m \in [1 : 2^{nR}]$, be each distributed according to $\prod_{i=1}^n p_{X_1}(x_{1i})$, and $(\tilde{X}_2^n, \tilde{X}_3^n) \sim \prod_{i=1}^n p_{X_2,X_3}(\tilde{x}_{2i}, \tilde{x}_{3i})$ be independent of $X_1^n(m)$ for $m \in [1 : 2^{nR}]$.

(b) Let $(X_1, X_2, X_3) \sim p(x_1, x_2)p(x_3|x_2)$ and $R = R_0 + R_1$. Let $X_1^n(m_0)$, $m_0 \in [1 : 2^{nR_0}]$, be distributed according to $\prod_{i=1}^n p_{X_1}(x_{1i})$. For each m_0, let $X_2^n(m_0, m_1)$, $m_1 \in [1 : 2^{nR_1}]$, be distributed according to $\prod_{i=1}^n p_{X_2|X_1}(x_{2i}|x_{1i}(m_0))$. Let $\tilde{X}_3^n \sim \prod_{i=1}^n p_{X_3}(\tilde{x}_{3i})$ be independent of $(X_1^n(m_0), X_2^n(m_0, m_1))$ for $m_0 \in [1 : 2^{nR_0}]$, $m_1 \in [1 : 2^{nR_1}]$.

3.5. *Maximum likelihood decoding.* The achievability proof of the channel coding theorem in Section 3.1.1 uses joint typicality decoding. This technique greatly simplifies the proof, especially for multiuser channels. However, given a codebook, the joint typicality decoding is not optimal in terms of minimizing the probability of decoding error (it is in fact surprising that such a suboptimal decoding rule can still achieve capacity).

Since the messages are equally likely, maximum likelihood decoding (MLD)

$$\hat{m} = \arg\max_m p(y^n|m) = \arg\max_m \prod_{i=1}^n p_{Y|X}(y_i|x_i(m))$$

is the optimal decoding rule (when there is a tie, choose an arbitrary index that maximizes the likelihood). Achievability proofs using MLD are more complex but provide tighter bounds on the optimal error exponent (reliability function); see, for example, Gallager (1968).

In this problem we use MLD to establish achievability of the capacity for a BSC(p), $p < 1/2$. Define the Hamming distance $d(x^n, y^n)$ between two binary sequences x^n and y^n as the number of positions where they differ, i.e., $d(x^n, y^n) = |\{i : x_i \neq y_i\}|$.

(a) Show that the MLD rule reduces to the minimum Hamming distance decoding rule—declare $\hat{m}$ is sent if $d(x^n(\hat{m}), y^n) < d(x^n(m), y^n)$ for all $m \neq \hat{m}$.

(b) Now fix $X \sim \text{Bern}(1/2)$. Using random coding and minimum distance decoding, show that for every $\epsilon > 0$, the probability of error averaged over codebooks is upper bounded as

$$\begin{aligned} P_e^{(n)} &= \mathsf{P}\{\hat{M} \neq 1 \,|\, M = 1\} \\ &\leq \mathsf{P}\big\{d(X^n(1), Y^n) > n(p + \epsilon) \,\big|\, M = 1\big\} \\ &\quad + (2^{nR} - 1)\,\mathsf{P}\big\{d(X^n(2), Y^n) \leq n(p + \epsilon) \,\big|\, M = 1\big\}. \end{aligned}$$

(c) Show that the first term tends to zero as $n \to \infty$. It can be shown using the

Chernoff–Hoeffding bound (Hoeffding 1963) that

$$\mathsf{P}\{d(X^n(2), Y^n) \le n(p+\epsilon) \,\big|\, M = 1\} \le 2^{-n(1-H(p+\epsilon))}.$$

Using these results, show that any $R < C = 1 - H(p)$ is achievable.

3.6. *Randomized code.* Suppose that in the definition of the $(2^{nR}, n)$ code for the DMC $p(y|x)$, we allow the encoder and the decoder to use random mappings. Specifically, let W be an arbitrary random variable independent of the message M and the channel, i.e., $p(y_i|x^i, y^{i-1}, m, w) = p_{Y|X}(y_i|x_i)$ for $i \in [1:n]$. The encoder generates a codeword $x^n(m, W)$, $m \in [1:2^{nR}]$, and the decoder generates an estimate $\hat{m}(y^n, W)$. Show that this randomization does not increase the capacity of the DMC.

3.7. *Nonuniform message.* Recall that a $(2^{nR}, n)$ code for the DMC $p(y|x)$ consists of an encoder $x^n = \phi_n(m)$ and a decoder $\hat{m} = \psi_n(y^n)$. Suppose that there exists a sequence of $(2^{nR}, n)$ codes such that $P_e^{(n)} = \mathsf{P}\{M \ne \hat{M}\}$ tends to zero as $n \to \infty$, where M is uniformly distributed over $[1:2^{nR}]$. (In other words, the rate R is achievable.) Now suppose that we wish to communicate a message M' that is arbitrarily (not uniformly) distributed over $[1:2^{nR}]$.

(a) Show that there exists a sequence of $(2^{nR}, n)$ codes with encoder–decoder pairs (ϕ_n', ψ_n') such that

$$\lim_{n\to\infty} \mathsf{P}\{M' \ne \hat{M}'\} = 0.$$

(Hint: Consider a random ensemble of codes $\Phi_n' = \phi_n \circ \sigma$ and $\Psi_n' = \sigma^{-1} \circ \psi_n$, where σ is a random permutation. Show the probability of error, averaged over M' and σ, is equal to $P_e^{(n)}$ and conclude that there exists a good permutation σ for each M'.)

(b) Does this result imply that the capacity for the maximal probability of error is equal to that for the average probability of error?

3.8. *Independently generated codebooks.* Let $(X, Y) \sim p(x, y)$, and $p(x)$ and $p(y)$ be their marginals. Consider two randomly and independently generated codebooks $\mathcal{C}_1 = \{X^n(1), \ldots, X^n(2^{nR_1})\}$ and $\mathcal{C}_2 = \{Y^n(1), \ldots, Y^n(2^{nR_2})\}$. The codewords of $\mathcal{C}_1$ are generated independently each according to $\prod_{i=1}^n p_X(x_i)$, and the codewords for $\mathcal{C}_2$ are generated independently according to $\prod_{i=1}^n p_Y(y_i)$. Define the set

$$\mathcal{C} = \{(x^n, y^n) \in \mathcal{C}_1 \times \mathcal{C}_2 \colon (x^n, y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y)\}.$$

Show that

$$\mathsf{E}\,|\mathcal{C}| \doteq 2^{n(R_1+R_2-I(X;Y))}.$$

3.9. *Capacity with input cost.* Consider the DMC $p(y|x)$ with cost constraint B.

(a) Using the operational definition of the capacity–cost function $C(B)$, show that it is nondecreasing and concave for $B \ge 0$.

(b) Show that the information capacity–cost function $C(B)$ is nondecreasing, concave, and continuous for $B \geq 0$.

3.10. *BSC with input cost.* Find the capacity–cost function $C(B)$ for a BSC(p) with input cost function $b(1) = 1$ and $b(0) = 0$.

3.11. *Channels with input–output cost.* Let $b(x, y)$ be a nonnegative input–output cost function on $\mathcal{X} \times \mathcal{Y}$. Consider a DMC $p(y|x)$ in which every codeword $x^n(m)$, $m \in [1 : 2^{nR}]$, must satisfy the average cost constraint

$$\mathsf{E}(b(x^n(m), Y^n)) = \frac{1}{n} \sum_{i=1}^{n} \mathsf{E}(b(x_i(m), Y_i)) \leq B,$$

where the expectation is with respect to the channel pmf $\prod_{i=1}^{n} p_{Y|X}(y_i|x_i(m))$. Show that the capacity of the DMC with cost constraint B is

$$C(B) = \max_{p(x):\mathsf{E}(b(X,Y))\leq B} I(X; Y).$$

(Hint: Consider the input-only cost function $b'(x) = \mathsf{E}(b(x, Y))$, where the expectation is taken with respect to $p(y|x)$.)

3.12. *Output scaling.* Show that the capacity of the Gaussian channel $Y = gX + Z$ remains the same if we scale the output by a nonzero constant a.

3.13. *Water-filling.* Consider the 2-component Gaussian product channel $Y_j = g_j X_j + Z_j$, $j = 1, 2$, with $g_1 < g_2$ and average power constraint P.

(a) Above what power P should we begin to use both channels?

(b) What is the energy-per-bit–rate function $E_b(R)$ needed for reliable communication at rate R over the channel? Show that $E_b(R)$ is strictly monotonically increasing and convex in R. What is the minimum energy per bit for the 2-component Gaussian product channel, i.e., $\lim_{R\to 0} E_b(R)$?

3.14. *List codes.* A $(2^{nR}, 2^{nL}, n)$ list code for a DMC $p(y|x)$ with capacity C consists of an encoder that assigns a codeword $x^n(m)$ to each message $m \in [1 : 2^{nR}]$ and a decoder that upon receiving y^n tries to finds the list of messages $\mathcal{L}(y^n) \subseteq [1 : 2^{nR}]$ of size $|\mathcal{L}| \leq 2^{nL}$ that contains the transmitted message. An error occurs if the list does not contain the transmitted message M, i.e., $P_e^{(n)} = \mathsf{P}\{M \notin \mathcal{L}(Y^n)\}$. A rate–list exponent pair (R, L) is said to be achievable if there exists a sequence of $(2^{nR}, 2^{nL}, n)$ list codes with $P_e^{(n)} \to 0$ as $n \to \infty$.

(a) Using random coding and joint typicality decoding, show that any (R, L) is achievable, provided $R < C + L$.

(b) Show that for every sequence of $(2^{nR}, 2^{nL}, n)$ list codes with $P_e^{(n)} \to 0$ as $n \to \infty$, we must have $R \leq C + L$. (Hint: You will need to develop a modified Fano's inequality.)

3.15. *Strong converse for source coding.* Given a sequence of $(2^{nR}, n)$ lossless source codes with $R < H(X)$, show that $P_e^{(n)} \to 1$ as $n \to \infty$. (Hint: A $(2^{nR}, n)$ code can represent only 2^{nR} points in $\mathcal{X}^n$. Using typicality, show that if $R < H(X)$, the probability of these 2^{nR} points converges to zero, no matter how we choose them.)

3.16. *Infinite alphabet.* Consider the lossless source coding problem for a discrete, but infinite-alphabet source X with finite entropy $H(X) < \infty$. Show that $R^* = H(X)$. (Hint: For the proof of achievability, consider a truncated DMS $[X]$ such that $\mathsf{P}\{X^n \neq [X]^n\}$ tends to zero as $n \to \infty$.)

3.17. *Rate–distortion function.* Consider the lossy source coding for a DMS X with distortion measure $d(x, \hat{x})$.

(a) Using the operational definition, show that the rate–distortion function $R(D)$ is nonincreasing and convex for $D \geq 0$.

(b) Show that the information rate–distortion function $R(D)$ is nonincreasing, convex, and continuous for $D \geq 0$.

3.18. *Bounds on the quadratic rate–distortion function.* Let X be an arbitrary memoryless (stationary) source with variance P, and let $d(x, \hat{x}) = (x - \hat{x})^2$ be the quadratic distortion measure.

(a) Show that the rate–distortion function is bounded as

$$h(X) - \frac{1}{2}\log(2\pi e D) \leq R(D) \leq \frac{1}{2}\log\left(\frac{P}{D}\right)$$

with equality iff X is a WGN(P) source. (Hint: For the upper bound, consider $\hat{X} = (P - D)X/P + Z$, where $Z \sim \mathrm{N}(0, D(P - D)/P)$ is independent of X.)

Remark: The lower bound is referred to as the *Shannon lower bound*.

(b) Is the Gaussian source harder or easier to describe than other sources with the same variance?

3.19. *Lossy source coding from a noisy observation.* Let $X \sim p(x)$ be a DMS and Y be another DMS obtained by passing X through a DMC $p(y|x)$. Let $d(x, \hat{x})$ be a distortion measure and consider a lossy source coding problem in which Y (instead of X) is encoded and sent to the decoder who wishes to reconstruct X with a prescribed distortion D.

Unlike the regular lossy source coding setup, the encoder maps each y^n sequence to an index $m \in [1 : 2^{nR})$. Otherwise, the definitions of $(2^{nR}, n)$ codes, achievability, and rate–distortion function are the same as before.

Let $D_{\min} = \min_{\hat{x}(y)} \mathsf{E}[d(X, \hat{x}(Y))]$. Show that the rate–distortion function for this setting is

$$R(D) = \min_{p(\hat{x}|y):\mathsf{E}(d(X,\hat{X}))\leq D} I(Y; \hat{X}) \quad \text{for } D \geq D_{\min}.$$

(Hint: Define a new distortion measure $d'(y, \hat{x}) = \mathsf{E}(d(X, \hat{x}) \,|\, Y = y)$, and show

that

$$\mathsf{E}\big[d\big(X^n, \hat{x}^n(m(Y^n))\big)\big] = \mathsf{E}\big[d'\big(Y^n, \hat{x}^n(m(Y^n))\big)\big].\ )$$

3.20. *To code or not to code.* Consider a WGN(P) source U and a Gaussian channel with output $Y = gX + Z$, where $Z \sim \mathrm{N}(0, 1)$. We wish to communicate the source over the channel at rate $r = 1$ symbol/transmission with the smallest possible squared error distortion. Assume an *expected* average power constraint

$$\frac{1}{n}\sum_{i=1}^{n} \mathsf{E}(x_i^2(U^n)) \le nP.$$

(a) Find the minimum distortion achieved by separate source and channel coding.

(b) Find the distortion achieved when the sender transmits $X_i = U_i$, $i \in [1 : n]$, i.e., performs no coding, and the receiver uses the (linear) MMSE estimate $\hat{U}_i$ of U_i given Y_i. Compare this to the distortion in part (a) and comment on the results.

3.21. *Two reconstructions.* Let X be a DMS, and $d_1(x, \hat{x}_1)$, $\hat{x}_1 \in \hat{\mathcal{X}}_1$, and $d_2(x, \hat{x}_2)$, $\hat{x}_2 \in \hat{\mathcal{X}}_2$, be two distortion measures. We wish to reconstruct X under both distortion measures from the same description as depicted in Figure 3.16.

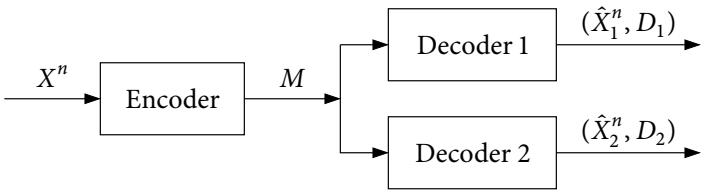


Figure 3.16. Lossy source coding with two reconstructions.

Define a $(2^{nR}, n)$ code, achievability of the rate–distortion triple (R, D_1, D_2), and the rate–distortion function $R(D_1, D_2)$ in the standard way. Show that

$$R(D_1, D_2) = \min_{p(\hat{x}_1, \hat{x}_2|x):\, \mathsf{E}(d_j(x, \hat{x}_j)) \le D_j,\ j=1,2} I(X; \hat{X}_1, \hat{X}_2).$$

3.22. *Lossy source coding with reconstruction cost.* Let X be a DMS and $d(x, \hat{x})$ be a distortion measure. Further let $b(\hat{x}) \ge 0$ be a cost function on $\hat{\mathcal{X}}$. Suppose that there is an average cost constraint on each reconstruction sequence $\hat{x}^n(m)$,

$$b(\hat{x}^n(m)) \le \sum_{i=1}^{n} b(\hat{x}_i(m)) \le nB \quad \text{for every } m \in [1 : 2^{nR}),$$

in addition to the distortion constraint $\mathsf{E}(d(X^n, \hat{X}^n)) \le D$. Define a $(2^{nR}, n)$ code,

achievability of the triple (R, D, B), and rate–distortion–cost function $R(D, B)$ in the standard way. Show that

$$R(D, B) = \min_{p(\hat{x}|x):\mathsf{E}(d(X,\hat{X}))\le D,\, \mathsf{E}(b(\hat{X}))\le B} I(X; \hat{X}).$$

Note that this problem is not a special case of the above two-reconstruction problem.

APPENDIX 3A PROOF OF LEMMA 3.2

We first note that $I([X]_j; [Y_j]_k) \to I([X]_j; Y_j) = h(Y_j) - h(Z)$ as $k \to \infty$. This follows since $([Y_j]_k - Y_j)$ tends to zero as $k \to \infty$; recall Section 2.3. Hence it suffices to show that

$$\liminf_{j\to\infty} h(Y_j) \ge h(Y).$$

First note that the pdf of Y_j converges pointwise to that of $Y \sim \mathrm{N}(0, S + 1)$. To prove this, consider

$$f_{Y_j}(y) = \int f_Z(y - x)\, dF_{[X]_j}(x) = \mathsf{E}\big(f_Z(y - [X]_j)\big).$$

Since the Gaussian pdf $f_Z(z)$ is continuous and bounded, $f_{Y_j}(y)$ converges to $f_Y(y)$ for every y by the weak convergence of $[X]_j$ to X. Furthermore, we have

$$f_{Y_j}(y) = \mathsf{E}\big(f_Z(y - [X]_j)\big) \le \max_z f_Z(z) = \frac{1}{\sqrt{2\pi}}.$$

Hence, for each $a > 0$, by the dominated convergence theorem (Appendix B),

$$\begin{aligned} h(Y_j) &= \int_{-\infty}^{\infty} -f_{Y_j}(y) \log f_{Y_j}(y)\, dy \\ &\ge \int_{-a}^{a} -f_{Y_j}(y) \log f_{Y_j}(y)\, dy + \mathsf{P}\{|Y_j| \ge a\} \cdot \min_y(-\log f_{Y_j}(y)), \end{aligned}$$

which converges to

$$\int_{-a}^{a} -f(y) \log f(y)\, dy + \mathsf{P}\{|Y| \ge a\} \cdot \min_y(-\log f(y))$$

as $j \to \infty$. Taking $a \to \infty$, we obtain the desired result.

CHAPTER 6

Interference Channels

We introduce the interference channel as a model for single-hop multiple one-to-one communications, such as pairs of base stations–handsets communicating over a frequency band that suffers from intercell interference, pairs of DSL modems communicating over a bundle of telephone lines that suffers from crosstalk, or pairs of people talking to each other in a cocktail party. The capacity region of the interference channel is not known in general. In this chapter, we focus on coding schemes for the two sender–receiver pair interference channel that are optimal or close to optimal in some special cases.

We first study simple coding schemes that use point-to-point channel codes, namely time division, treating interference as noise, and simultaneous decoding. We show that simultaneous decoding is optimal under strong interference, that is, when the interfering signal at each receiver is stronger than the signal from its respective sender. These inner bounds are compared for the Gaussian interference channel. We extend the strong interference result to the Gaussian case and show that treating interference as noise is sum-rate optimal when the interference is sufficiently weak. The converse proof of the latter result uses the new idea of a genie that provides side information to each receiver about its intended codeword.

We then present the Han–Kobayashi coding scheme, which generalizes the aforementioned simple schemes by also using rate splitting (see Section 4.4) and superposition coding (see Section 5.3). We show that the Han–Kobayashi scheme is optimal for the class of injective deterministic interference channels. The converse proof of this result is extended to establish an outer bound on the capacity region of the class of injective semideterministic interference channels, which includes the Gaussian interference channel. The outer bound for the Gaussian case, and hence the capacity region, is shown to be within half a bit per dimension of the Han–Kobayashi inner bound. This gap vanishes in the limit of high signal and interference to noise ratios for the normalized symmetric capacity (degrees of freedom). We discuss an interesting correspondence to q-ary expansion deterministic (QED) interference channels in this limit.

Finally, we introduce the new idea of interference alignment through a QED interference channel with many sender–receiver pairs. Interference alignment for wireless fading channels will be illustrated in Section 23.7.

6.1 DISCRETE MEMORYLESS INTERFERENCE CHANNEL

Consider the two sender–receiver pair communication system depicted in Figure 6.1, where each sender wishes to communicate a message to its respective receiver over a shared *interference channel*. Each message M_j, $j = 1, 2$, is separately encoded into a codeword X_j^n and transmitted over the channel. Upon receiving the sequence Y_j^n, receiver $j = 1, 2$ finds an estimate $\hat{M}_j$ of message M_j. Because communication takes place over a shared channel, the signal at each receiver can suffer not only from the noise in the channel, but also from interference by the other transmitted codeword. This leads to a tradeoff between the rates at which both messages can be reliably communicated. We seek to determine the limits on this tradeoff.

We first consider a two sender–receiver (2-user) pair *discrete memoryless interference channel* (DM-IC) model $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1, y_2|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ that consists of four finite sets $\mathcal{X}_1$, $\mathcal{X}_2$, $\mathcal{Y}_1$, $\mathcal{Y}_2$, and a collection of conditional pmfs $p(y_1, y_2|x_1, x_2)$ on $\mathcal{Y}_1 \times \mathcal{Y}_2$. A $(2^{nR_1}, 2^{nR_2}, n)$ code for the interference channel consists of

- two message sets $[1 : 2^{nR_1}]$ and $[1 : 2^{nR_2}]$,
- two encoders, where encoder 1 assigns a codeword $x_1^n(m_1)$ to each message $m_1 \in [1 : 2^{nR_1}]$ and encoder 2 assigns a codeword $x_2^n(m_2)$ to each message $m_2 \in [1 : 2^{nR_2}]$, and
- two decoders, where decoder 1 assigns an estimate $\hat{m}_1$ or an error message e to each received sequence y_1^n and decoder 2 assigns an estimate $\hat{m}_2$ or an error message e to each received sequence y_2^n.

We assume that the message 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 DM-IC if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that $\lim_{n\to\infty} P_e^{(n)} = 0$. The capacity region $\mathscr{C}$ of the DM-IC is the closure of the set of achievable rate pairs (R_1, R_2) and the sum-capacity C_{sum} of the DM-IC is defined as $C_{\text{sum}} = \max\{R_1 + R_2 : (R_1, R_2) \in \mathscr{C}\}$.

As for the broadcast channel, the capacity region of the DM-IC depends on the channel conditional pmf $p(y_1, y_2|x_1, x_2)$ only through the conditional marginals $p(y_1|x_1, x_2)$ and $p(y_2|x_1, x_2)$. The capacity region of the DM-IC is not known in general.

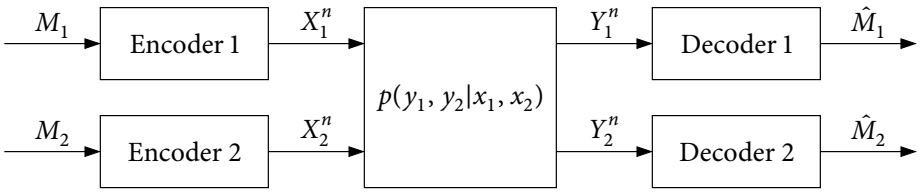


Figure 6.1. Two sender–receiver pair communication system.

6.2 SIMPLE CODING SCHEMES

We first consider several simple coding schemes for the interference channel.

Time division. The maximum achievable individual rates for the two sender–receiver pairs are

$$C_1 = \max_{p(x_1), x_2} I(X_1; Y_1|X_2 = x_2),$$
$$C_2 = \max_{p(x_2), x_1} I(X_2; Y_2|X_1 = x_1).$$

These capacities define the time-division inner bound consisting of all rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< \alpha C_1, \\ R_2 &< \bar{\alpha} C_2 \end{aligned} \tag{6.1}$$

for some $\alpha \in [0, 1]$. This bound is tight in some special cases.

Example 6.1 (Modulo-2 sum IC). Consider a DM-IC where the channel inputs X_1, X_2 and outputs Y_1, Y_2 are binary, and $Y_1 = Y_2 = X_1 \oplus X_2$. The time-division inner bound reduces to the set of rate pairs (R_1, R_2) such that $R_1 + R_2 < 1$. In the other direction, by allowing cooperation between the receivers, we obtain the upper bound on the sum-rate

$$R_1 + R_2 \le C_{12} = \max_{p(x_1)p(x_2)} I(X_1, X_2; Y_1, Y_2).$$

Since in our example, $Y_1 = Y_2$, this bound reduces to the set of rate pairs (R_1, R_2) such that $R_1 + R_2 \le 1$. Hence the time-division inner bound is tight.

The time-division inner bound is not tight in general, however.

Example 6.2 (No interference). Consider an interference channel with orthogonal components $p(y_1, y_2|x_1, x_2) = p(y_1|x_1)p(y_2|x_2)$. In this case, the channel can be viewed simply as two separate DMCs and the capacity region is the set of rate pairs (R_1, R_2) such that $R_1 \le C_1$ and $R_2 \le C_2$. This is clearly larger than the time-division inner bound.

Treating interference as noise. Another inner bound on the capacity region of the interference channel can be achieved using point-to-point codes, time sharing, and treating interference as noise. This yields the *interference-as-noise* inner bound consisting of all rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< I(X_1; Y_1|Q), \\ R_2 &< I(X_2; Y_2|Q) \end{aligned} \tag{6.2}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)$.

Simultaneous decoding. At the opposite extreme of treating interference as noise, we can have each receiver recover both messages. Following the achievability proof for the

DM-MAC using simultaneous decoding and coded time sharing in Section 4.5.3 (also see Problem 4.4), we can easily show that this scheme yields the *simultaneous-decoding* inner bound on the capacity region of the DM-IC consisting of all rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< \min\{I(X_1; Y_1|X_2, Q),\ I(X_1; Y_2|X_2, Q)\}, \\ R_2 &< \min\{I(X_2; Y_1|X_1, Q),\ I(X_2; Y_2|X_1, Q)\}, \\ R_1 + R_2 &< \min\{I(X_1, X_2; Y_1|Q),\ I(X_1, X_2; Y_2|Q)\} \end{aligned} \tag{6.3}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)$.

Remark 6.1. Let $\mathscr{R}(X_1, X_2)$ be the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< \min\{I(X_1; Y_1|X_2), I(X_1; Y_2|X_2)\}, \\ R_2 &< \min\{I(X_2; Y_2|X_1), I(X_2; Y_1|X_1)\}, \\ R_1 + R_2 &< \min\{I(X_1, X_2; Y_1),\ I(X_1, X_2; Y_2)\} \end{aligned}$$

for some pmf $p(x_1)p(x_2)$. Unlike the DM-MAC, the inner bound in 6.3 can be strictly larger than the convex closure of $\mathscr{R}(X_1, X_2)$ over all $p(x_1)p(x_2)$. Hence, coded time sharing can achieve higher rates than (uncoded) time sharing, and is needed to achieve the inner bound in (6.3).

The simultaneous-decoding inner bound is sometimes tight.

Example 6.3. Consider a DM-IC with output alphabets $\mathcal{Y}_1 = \mathcal{Y}_2$ and $p_{Y_1|X_1,X_2}(y|x_1, x_2) = p_{Y_2|X_1,X_2}(y|x_1, x_2)$. The simultaneous-decoding inner bound reduces to the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< I(X_1; Y_1|X_2, Q), \\ R_2 &< I(X_2; Y_2|X_1, Q), \\ R_1 + R_2 &< I(X_1, X_2; Y_1|Q) \end{aligned}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)$. Now, using standard converse proof techniques, we can establish the outer bound on the capacity region of the general DM-IC consisting of all rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\le I(X_1; Y_1|X_2, Q), \\ R_2 &\le I(X_2; Y_2|X_1, Q), \\ R_1 + R_2 &\le I(X_1, X_2; Y_1, Y_2|Q) \end{aligned}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)$. This bound can be further improved by using the fact that the capacity region depends only on the marginals of $p(y_1, y_2|x_1, x_2)$. If a rate pair (R_1, R_2) is achievable, then it must satisfy the inequalities

$$\begin{aligned} R_1 &\le I(X_1; Y_1|X_2, Q), \\ R_2 &\le I(X_2; Y_2|X_1, Q), \\ R_1 + R_2 &\le \min_{\tilde{p}(y_1,y_2|x_1,x_2)} I(X_1, X_2; Y_1, Y_2|Q) \end{aligned} \tag{6.4}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)$, where the minimum in the third inequality is over all

conditional pmfs $\tilde{p}(y_1, y_2|x_1, x_2)$ with the same marginals $p(y_1|x_1, x_2)$ and $p(y_2|x_1, x_2)$ as the given channel conditional pmf $p(y_1, y_2|x_1, x_2)$.

Now, since the marginals of the channel in our example are identical, the minimum in the third inequality of the outer bound in (6.4) is attained for $Y_1 = Y_2$, and the bound reduces to the set of all rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\le I(X_1; Y_1|X_2, Q), \\ R_2 &\le I(X_2; Y_2|X_1, Q), \\ R_1 + R_2 &\le I(X_1, X_2; Y_1|Q) \end{aligned}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)$. Hence, simultaneous decoding is optimal for the DM-IC in this example.

Simultaneous nonunique decoding. We can improve upon the simultaneous-decoding inner bound via nonunique decoding, that is, by not requiring each receiver to recover the message intended for the other receiver. This yields the *simultaneous-nonunique-decoding* inner bound consisting of all rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< I(X_1; Y_1|X_2, Q), \\ R_2 &< I(X_2; Y_2|X_1, Q), \\ R_1 + R_2 &< \min\{I(X_1, X_2; Y_1|Q),\ I(X_1, X_2; Y_2|Q)\} \end{aligned} \tag{6.5}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)$.

The achievability proof of this inner bound uses techniques we have already encountered in Sections 4.5 and 5.3. Fix a pmf $p(q)p(x_1|q)p(x_2|q)$. Randomly generate a sequence $q^n \sim \prod_{i=1}^n p_Q(q_i)$. Randomly and conditionally independently generate 2^{nR_1} sequences $x_1^n(m_1)$, $m_1 \in [1 : 2^{nR_1}]$, each according to $\prod_{i=1}^n p_{X_1|Q}(x_{1i}|q_i)$, and 2^{nR_2} sequences $x_2^n(m_2)$, $m_2 \in [1 : 2^{nR_2}]$, each according to $\prod_{i=1}^n p_{X_2|Q}(x_{2i}|q_i)$. To send (m_1, m_2), encoder $j = 1, 2$ transmits $x_j^n(m_j)$.

Decoder 1 finds the unique message $\hat{m}_1$ such that $(q^n, x_1^n(\hat{m}_1), x_2^n(m_2), y_1^n) \in \mathcal{T}_\epsilon^{(n)}$ for some m_2. By the LLN and the packing lemma, the probability of error for decoder 1 tends to zero as $n \to \infty$ if $R_1 < I(X_1; Y_1, X_2|Q) - \delta(\epsilon) = I(X_1; Y_1|X_2, Q) - \delta(\epsilon)$ and $R_1 + R_2 < I(X_1, X_2; Y_1|Q) - \delta(\epsilon)$. Similarly, decoder 2 finds the unique message $\hat{m}_2$ such that $(q^n, x_1^n(m_1), x_2^n(\hat{m}_2), y_2^n) \in \mathcal{T}_\epsilon^{(n)}$ for some m_1. Again by the LLN and the packing lemma, the probability of error for decoder 2 tends to zero as $n \to \infty$ if $R_2 < I(X_2; Y_2|X_1, Q) - \delta(\epsilon)$ and $R_1 + R_2 < I(X_1, X_2; Y_2|Q) - \delta(\epsilon)$. This completes the achievability proof of the simultaneous-nonunique-decoding inner bound.

6.3 STRONG INTERFERENCE

Suppose that each receiver in an interference channel is physically closer to the interfering transmitter than to its own transmitter and hence the received signal from the interfering transmitter is stronger than that from its transmitter. Under such strong interference

condition, each receiver can essentially recover the message of the interfering transmitter without imposing an additional constraint on its rate. We define two notions of strong interference for the DM-IC and show that simultaneous decoding is optimal under both notions.

Very strong interference. A DM-IC is said to have *very strong interference* if

$$\begin{aligned} I(X_1; Y_1|X_2) &\le I(X_1; Y_2), \\ I(X_2; Y_2|X_1) &\le I(X_2; Y_1) \end{aligned} \tag{6.6}$$

for all $p(x_1)p(x_2)$. The capacity region of the DM-IC with very strong interference is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\le I(X_1; Y_1|X_2, Q), \\ R_2 &\le I(X_2; Y_2|X_1, Q) \end{aligned}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)$. The converse proof is quite straightforward, since this region constitutes an outer bound on the capacity region of the general DM-IC. The proof of achievability follows by noting that under the very strong interference condition, the sum-rate inequality in the simultaneous (unique or nonunique) decoding inner bound is inactive. Note that the capacity region can be achieved also via successive cancellation decoding and time sharing. Each decoder successively recovers the other message and then its own message. Because of the very strong interference condition, only the requirements on the achievable rates for the second decoding step matter.

Strong interference. A DM-IC is said to have *strong interference* if

$$\begin{aligned} I(X_1; Y_1|X_2) &\le I(X_1; Y_2|X_2), \\ I(X_2; Y_2|X_1) &\le I(X_2; Y_1|X_1) \end{aligned} \tag{6.7}$$

for all $p(x_1)p(x_2)$. Note that this is an extension of the more capable condition for the DM-BC. In particular, Y_2 is more capable than Y_1 given X_2, and Y_1 is more capable than Y_2 given X_1. Clearly, if the channel has very strong interference, then it also has strong interference. The converse is not necessarily true as illustrated by the following.

Example 6.4. Consider the DM-IC with binary inputs X_1, X_2 and ternary outputs $Y_1 = Y_2 = X_1 + X_2$. Then

$$\begin{aligned} I(X_1; Y_1|X_2) &= I(X_1; Y_2|X_2) = H(X_1), \\ I(X_2; Y_2|X_1) &= I(X_2; Y_1|X_1) = H(X_2). \end{aligned}$$

Therefore, this DM-IC has strong interference. However,

$$\begin{aligned} I(X_1; Y_1|X_2) &= H(X_1) \ge H(X_1) - H(X_1|Y_2) = I(X_1; Y_2), \\ I(X_2; Y_2|X_1) &= H(X_2) \ge H(X_2) - H(X_2|Y_1) = I(X_2; Y_1) \end{aligned}$$

with strict inequality for some pmf $p(x_1)p(x_2)$. Therefore, this channel does not satisfy the very strong interference condition.

We now show that the simultaneous-nonunique-decoding inner bound is tight under the strong interference condition.

Theorem 6.1. The capacity region of the DM-IC $p(y_1, y_2|x_1, x_2)$ with strong interference is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\le I(X_1; Y_1|X_2, Q), \\ R_2 &\le I(X_2; Y_2|X_1, Q), \\ R_1 + R_2 &\le \min\{I(X_1, X_2; Y_1|Q),\ I(X_1, X_2; Y_2|Q)\} \end{aligned}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)$ with $|\mathcal{Q}| \le 4$.

Proof of the converse. The first two inequalities can be easily established. By symmetry it suffices to show that $R_1 + R_2 \le I(X_1, X_2; Y_2|Q)$. Consider

$$\begin{aligned} n(R_1 + R_2) &= H(M_1) + H(M_2) \\ &\overset{(a)}{\le} I(M_1; Y_1^n) + I(M_2; Y_2^n) + n\epsilon_n \\ &\overset{(b)}{=} I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) + n\epsilon_n \\ &\le I(X_1^n; Y_1^n|X_2^n) + I(X_2^n; Y_2^n) + n\epsilon_n \\ &\overset{(c)}{\le} I(X_1^n; Y_2^n|X_2^n) + I(X_2^n; Y_2^n) + n\epsilon_n \\ &= I(X_1^n, X_2^n; Y_2^n) + n\epsilon_n \\ &\le \sum_{i=1}^{n} I(X_{1i}, X_{2i}; Y_{2i}) + n\epsilon_n \\ &= nI(X_1, X_2; Y_2|Q) + n\epsilon_n, \end{aligned}$$

where (a) follows by Fano's inequality and (b) follows since $M_j \to X_j^n \to Y_j^n$ for $j = 1, 2$ (by the independence of M_1 and M_2). Step (c) is established using the following.

Lemma 6.1. For a DM-IC $p(y_1, y_2|x_1, x_2)$ with strong interference, $I(X_1^n; Y_1^n|X_2^n) \le I(X_1^n; Y_2^n|X_2^n)$ for all $(X_1^n, X_2^n) \sim p(x_1^n)p(x_2^n)$ and all $n \ge 1$.

This lemma can be proved by noting that the strong interference condition implies that $I(X_1; Y_1|X_2, U) \le I(X_1; Y_2|X_2, U)$ for all $p(u)p(x_1|u)p(x_2|u)$ and using induction on n.

The other bound $R_1 + R_2 \le I(X_1, X_2; Y_1|Q)$ follows similarly, which completes the proof of the theorem.

6.4 GAUSSIAN INTERFERENCE CHANNEL

Consider the 2-user-pair Gaussian interference channel depicted in Figure 6.2, which is

a simple model for a wireless interference channel or a DSL cable bundle. The channel outputs corresponding to the inputs X_1 and X_2 are

$$Y_1 = g_{11}X_1 + g_{12}X_2 + Z_1,$$
$$Y_2 = g_{21}X_1 + g_{22}X_2 + Z_2,$$

where g_{jk}, $j, k = 1, 2$, is the channel gain from sender k to receiver j, and $Z_1 \sim \mathrm{N}(0, N_0/2)$ and $Z_2 \sim \mathrm{N}(0, N_0/2)$ are noise components. Assume average power constraint P on each of X_1 and X_2. We assume without loss of generality that $N_0/2 = 1$ and define the received SNRs as $S_1 = g_{11}^2 P$ and $S_2 = g_{22}^2 P$ and the received *interference-to-noise ratios* (INRs) as $I_1 = g_{12}^2 P$ and $I_2 = g_{21}^2 P$.

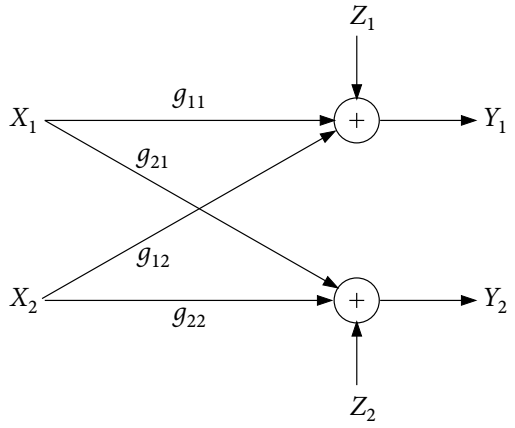


Figure 6.2. Gaussian interference channel.

The capacity region of the Gaussian IC is not known in general.

6.4.1 Inner Bounds

We specialize the inner bounds in Section 6.2 to the Gaussian case.

Time division with power control. Using time division and power control, we obtain the time-division inner bound on the capacity region of the Gaussian IC that consists of all rate pairs (R_1, R_2) such that

$$R_1 < \alpha\, \mathsf{C}(S_1/\alpha),$$
$$R_2 < \bar{\alpha}\, \mathsf{C}(S_2/\bar{\alpha})$$

for some $\alpha \in [0, 1]$.

Treating interference as noise. Consider the inner bound in (6.2) subject to the power constraints. By setting $X_1 \sim \mathrm{N}(0, P)$, $X_2 \sim \mathrm{N}(0, P)$, and $Q = \emptyset$, we obtain the inner bound on the capacity region of the Gaussian IC consisting of all rate pairs (R_1, R_2) such that

$$R_1 < \mathsf{C}\big(S_1/(1 + I_1)\big),$$
$$R_2 < \mathsf{C}\big(S_2/(1 + I_2)\big).$$

Note, however, that Gaussian input signals are not necessarily optimal when evaluating the mutual information characterization in (6.2) under the power constraints. Also note that the above inner bound can be further improved via time sharing and power control.

Simultaneous nonunique decoding. The inner bound in (6.5) subject to the power constraints is optimized by setting $X_1 \sim \mathrm{N}(0, P)$, $X_2 \sim \mathrm{N}(0, P)$, and $Q = \emptyset$. This gives the inner bound on the capacity region of the Gaussian IC that consists of all rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< \mathsf{C}(S_1), \\ R_2 &< \mathsf{C}(S_2), \\ R_1 + R_2 &< \min\{\mathsf{C}(S_1 + I_1),\ \mathsf{C}(S_2 + I_2)\}. \end{aligned}$$

Although this bound is again achieved using optimal point-to-point Gaussian codes, it cannot be achieved in general via successive cancellation decoding.

The above inner bounds are compared in Figure 6.3 for symmetric Gaussian ICs with SNRs $S_1 = S_2 = S = 1$ and increasing INRs $I_1 = I_2 = I$. When interference is weak (Figure 6.3a), treating interference as noise can outperform time division and simultaneous nonunique decoding, and is in fact sum-rate optimal as we show in Section 6.4.3. As interference becomes stronger (Figure 6.3b), simultaneous nonunique decoding and time division begin to outperform treating interference as noise. As interference becomes even stronger, simultaneous nonunique decoding outperforms the other two coding schemes (Figures 6.3c,d), ultimately achieving the interference-free rate region consisting of all rate pairs (R_1, R_2) such that $R_1 < C_1$ and $R_2 < C_2$ (Figure 6.3d).

6.4.2 Capacity Region of the Gaussian IC with Strong Interference

A Gaussian IC is said to have *strong interference* if $|g_{21}| \geq |g_{11}|$ and $|g_{12}| \geq |g_{22}|$, or equivalently, $I_2 \geq S_1$ and $I_1 \geq S_2$.

Theorem 6.2. The capacity region of the Gaussian IC with strong interference is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq \mathsf{C}(S_1), \\ R_2 &\leq \mathsf{C}(S_2), \\ R_1 + R_2 &\leq \min\{\mathsf{C}(S_1 + I_1),\ \mathsf{C}(S_2 + I_2)\}. \end{aligned}$$

The proof of achievability follows by using simultaneous nonunique decoding. The proof of the converse follows by noting that the above condition is equivalent to the strong interference condition for the DM-IC in (6.7) and showing that $X_1 \sim \mathrm{N}(0, P)$ and $X_2 \sim \mathrm{N}(0, P)$ optimize the mutual information terms.

The nontrivial step is to show that the condition $I_2 \geq S_1$ and $I_1 \geq S_2$ is equivalent to the condition $I(X_1; Y_1|X_2) \leq I(X_1; Y_2|X_2)$ and $I(X_2; Y_2|X_1) \leq I(X_2; Y_1|X_1)$ for every

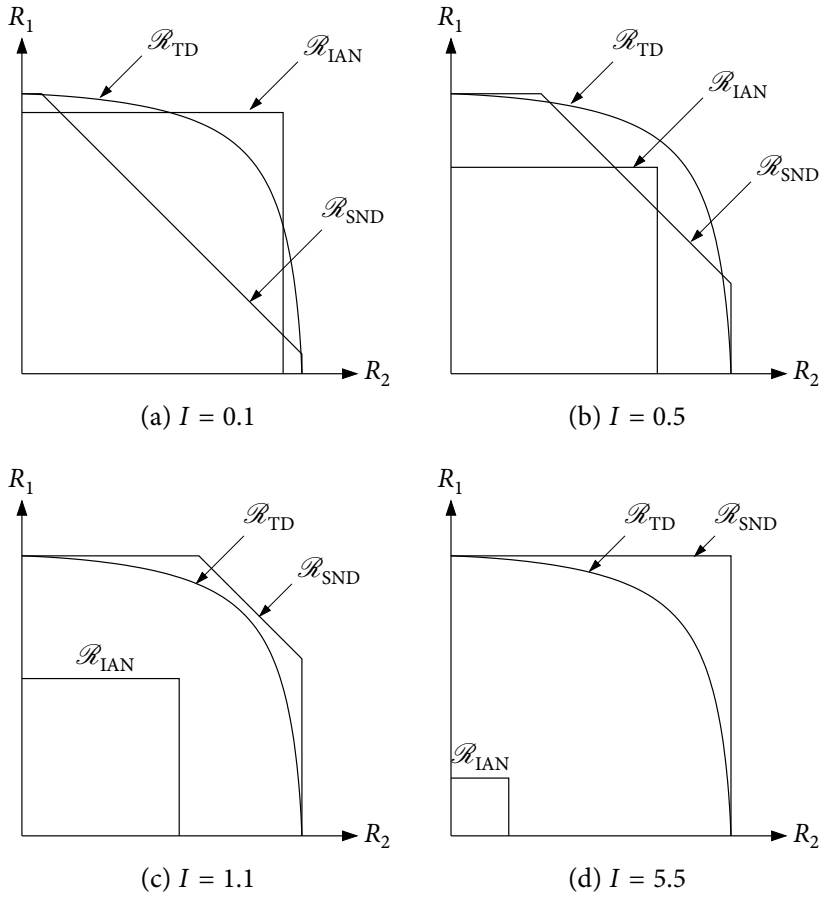


Figure 6.3. Comparison of time division (region $\mathscr{R}_{\text{TD}}$), treating interference as noise (region $\mathscr{R}_{\text{IAN}}$), and simultaneous nonunique decoding (region $\mathscr{R}_{\text{SND}}$) for $S = 1$ and different values of I. Treating interference as noise achieves the sum-capacity for case (a), while $\mathscr{R}_{\text{SND}}$ is the capacity region for cases (c) and (d).

$F(x_1)F(x_2)$. If $I_2 \geq S_1$ and $I_1 \geq S_2$, then it can be easily shown that the Gaussian BC from X_1 to $(Y_2 - g_{22}X_2, Y_1 - g_{12}X_2)$ given X_2 is degraded and the Gaussian BC from X_2 to $(Y_1 - g_{11}X_1, Y_2 - g_{21}X_1)$ given X_1 is degraded, and hence each is more capable. This proves one direction of the equivalence. To prove the other direction, assume that $h(g_{11}X_1 + Z_1) \leq h(g_{21}X_1 + Z_2)$ and $h(g_{22}X_2 + Z_2) \leq h(g_{12}X_2 + Z_1)$. Substituting $X_1 \sim \text{N}(0, P)$ and $X_2 \sim \text{N}(0, P)$ shows that $I_2 \geq S_1$ and $I_1 \geq S_2$, respectively.

Remark 6.2. A Gaussian IC is said to have *very strong interference* if $S_2 \leq I_1/(1 + S_1)$ and $S_1 \leq I_2/(1 + S_2)$. It can be shown that this condition is the same as the very strong interference condition for the DM-IC in (6.6) when restricted to Gaussian inputs. Under this condition, the capacity region is the set of rate pairs (R_1, R_2) such that $R_1 \leq \mathsf{C}(S_1)$ and $R_2 \leq \mathsf{C}(S_2)$ and hence interference does not impair communication.

6.4.3 Sum-Capacity of the Gaussian IC with Weak Interference

A Gaussian IC is said to have *weak interference* if for some $\rho_1, \rho_2 \in [0, 1]$,

$$\begin{aligned} \sqrt{I_1/S_2}\,(1 + I_2) &\le \rho_2\sqrt{1-\rho_1^2}, \\ \sqrt{I_2/S_1}\,(1 + I_1) &\le \rho_1\sqrt{1-\rho_2^2}. \end{aligned} \tag{6.8}$$

Under this weak interference condition, treating interference as noise is optimal for the sum-rate.

Theorem 6.3. The sum-capacity of the Gaussian IC with weak interference is

$$C_{\text{sum}} = \mathsf{C}\left(\frac{S_1}{1+I_1}\right) + \mathsf{C}\left(\frac{S_2}{1+I_2}\right).$$

The interesting part of the proof is the converse. It involves the use of a *genie* to establish an upper bound on the sum-capacity. For simplicity of presentation, we consider the symmetric case with $I_1 = I_2 = I$ and $S_1 = S_2 = S$. In this case, the weak interference condition in (6.8) reduces to

$$\sqrt{I/S}\,(1 + I) \le \frac{1}{2} \tag{6.9}$$

and the sum-capacity is $C_{\text{sum}} = 2\,\mathsf{C}(S/(1 + I))$.

Proof of the converse. Consider the *genie-aided* Gaussian IC depicted in Figure 6.4 with side information

$$\begin{aligned} T_1 &= \sqrt{I/P}\,(X_1 + \eta W_1), \\ T_2 &= \sqrt{I/P}\,(X_2 + \eta W_2), \end{aligned}$$

where $W_1 \sim \mathrm{N}(0, 1)$ and $W_2 \sim \mathrm{N}(0, 1)$ are independent noise components with $\mathsf{E}(Z_1 W_1) = \mathsf{E}(Z_2 W_2) = \rho$ and $\eta \ge 0$. Suppose that a genie reveals T_1 to decoder 1 and T_2 to decoder 2. Clearly, the sum-capacity of this channel $\tilde{C}_{\text{sum}} \ge C_{\text{sum}}$.

We first show that if $\eta^2 I \le (1 - \rho^2)P$ (useful genie), then the sum-capacity of the genie-aided channel is achieved by using Gaussian inputs and treating interference as noise. We then show that if in addition, $\eta\rho\sqrt{S/P} = 1 + I$ (smart genie), then the sum-capacity of the genie-aided channel is the same as that of the original channel. Since $\tilde{C}_{\text{sum}} \ge C_{\text{sum}}$, this also shows that C_{sum} is achieved by using Gaussian inputs and treating interference as noise. Using the second condition to eliminate η from the first condition gives $\sqrt{I/S}(1 + I) \le \rho\sqrt{1-\rho^2}$. Taking $\rho = \sqrt{1/2}$, which maximizes the range of I, gives the weak interference condition in the theorem. The proof steps involve properties of differential entropy, including the maximum differential entropy lemma; the fact that Gaussian is the worst noise with a given average power in an additive noise channel with Gaussian input (see Problem 2.12); and properties of jointly Gaussian random variables (see Appendix B).

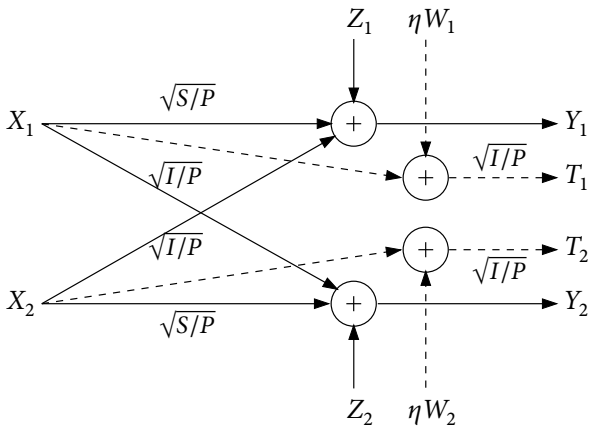


Figure 6.4. Genie-aided Gaussian interference channel.

Let X_1^* and X_2^* be independent $\mathrm{N}(0, P)$ random variables, and Y_1^*, Y_2^* and T_1^*, T_2^* be the corresponding channel outputs and side information. Then we can establish the following condition under which $\tilde{C}_{\text{sum}}$ is achieved by treating interference as Gaussian noise.

Lemma 6.2 (Useful Genie). If $\eta^2 I \le (1-\rho^2)P$, then the sum-capacity of the above genie-aided channel is

$$\tilde{C}_{\text{sum}} = I(X_1^*; Y_1^*, T_1^*) + I(X_2^*; Y_2^*, T_2^*).$$

The proof of this lemma is in Appendix 6A.

Remark 6.3. If $\rho = 0$, $\eta = 1$, and $I \le P$, then the genie is always useful.

Continuing the proof of the converse, suppose that the following *smart genie* condition

$$\eta\rho\sqrt{S/P} = 1 + I$$

holds. Note that combined with the (useful genie) condition for the lemma, the smart genie gives the weak interference condition in (6.9). Now by the smart genie condition,

$$\begin{aligned}
\mathsf{E}(T_1^* \,|\, X_1^*, Y_1^*) &= \mathsf{E}\big(T_1^* \,\big|\, X_1^*, \sqrt{I/P}\, X_2^* + Z_1\big) \\
&= \sqrt{I/P}\, X_1^* + \eta\sqrt{I/P}\ \mathsf{E}\big(W_1 \,\big|\, \sqrt{I/P}\, X_2^* + Z_1\big) \\
&= \sqrt{I/P}\, X_1^* + \frac{\eta\rho\sqrt{I/P}}{1+I}\big(\sqrt{I/P}\, X_2^* + Z_1\big) \\
&= \sqrt{I/S}\, Y_1^* \\
&= \mathsf{E}(T_1^* \,|\, Y_1^*).
\end{aligned}$$

Since all random variables involved are jointly Gaussian, this implies that $X_1^* \to Y_1^* \to T_1^*$ form a Markov chain, or equivalently, $I(X_1^*; T_1^* | Y_1^*) = 0$. Similarly $I(X_2^*; T_2^* | Y_2^*) = 0$. Finally, by the useful genie lemma,

$$C_{\text{sum}} \le \tilde{C}_{\text{sum}} = I(X_1^*; Y_1^*, T_1^*) + I(X_2^*; Y_2^*, T_2^*) = I(X_1^*; Y_1^*) + I(X_2^*; Y_2^*).$$

This completes the proof of the converse.

Remark 6.4. The idea of a genie providing each receiver with side information about its intended codeword can be used to obtain outer bounds on the capacity region of the general Gaussian IC; see Problem 6.17. This same idea will be used also in the converse proof for the injective deterministic IC in Section 6.6.

6.5 HAN–KOBAYASHI INNER BOUND

The Han–Kobayashi inner bound is the best-known bound on the capacity region of the DM-IC. It includes all the inner bounds we discussed so far, and is tight for all interference channels with known capacity regions. We consider the following characterization of this inner bound.

Theorem 6.4 (Han–Kobayashi Inner Bound). A rate pair (R_1, R_2) is achievable for the DM-IC $p(y_1, y_2|x_1, x_2)$ if

$$\begin{aligned}
R_1 &< I(X_1; Y_1 | U_2, Q),\\
R_2 &< I(X_2; Y_2 | U_1, Q),\\
R_1 + R_2 &< I(X_1, U_2; Y_1 | Q) + I(X_2; Y_2 | U_1, U_2, Q),\\
R_1 + R_2 &< I(X_2, U_1; Y_2 | Q) + I(X_1; Y_1 | U_1, U_2, Q),\\
R_1 + R_2 &< I(X_1, U_2; Y_1 | U_1, Q) + I(X_2, U_1; Y_2 | U_2, Q),\\
2R_1 + R_2 &< I(X_1, U_2; Y_1 | Q) + I(X_1; Y_1 | U_1, U_2, Q) + I(X_2, U_1; Y_2 | U_2, Q),\\
R_1 + 2R_2 &< I(X_2, U_1; Y_2 | Q) + I(X_2; Y_2 | U_1, U_2, Q) + I(X_1, U_2; Y_1 | U_1, Q)
\end{aligned}$$

for some pmf $p(q)p(u_1, x_1|q)p(u_2, x_2|q)$, where $|\mathcal{U}_1| \le |\mathcal{X}_1| + 4$, $|\mathcal{U}_2| \le |\mathcal{X}_2| + 4$, and $|\mathcal{Q}| \le 6$.

Remark 6.5. The Han–Kobayashi inner bound reduces to the interference-as-noise inner bound in (6.2) by setting $U_1 = U_2 = \emptyset$. At the other extreme, the Han–Kobayashi inner bound reduces to the simultaneous-nonunique-decoding inner bound in (6.5) by setting $U_1 = X_1$ and $U_2 = X_2$. Thus, the bound is tight for the class of DM-ICs with strong interference.

Remark 6.6. The Han–Kobayashi inner bound can be readily extended to the Gaussian IC with average power constraints and evaluated using Gaussian (U_j, X_j), $j = 1, 2$; see Problem 6.16. It is not known, however, if the restriction to the Gaussian distribution is sufficient.

6.5.1 Proof of the Han–Kobayashi Inner Bound

The proof uses rate splitting. We represent each message M_j, $j = 1, 2$, by independent "public" message M_{j0} at rate R_{j0} and "private" message M_{jj} at rate R_{jj}. Thus, $R_j = R_{j0} + R_{jj}$. These messages are sent via superposition coding, whereby the cloud center U_j represents the public message M_{j0} and the satellite codeword X_j represents the message pair (M_{j0}, M_{jj}). The public messages are to be recovered by both receivers, while each private message is to be recovered only by its intended receiver. We first show that $(R_{10}, R_{20}, R_{11}, R_{22})$ is achievable if

$$\begin{aligned}
R_{11} &< I(X_1; Y_1|U_1, U_2, Q),\\
R_{11} + R_{10} &< I(X_1; Y_1|U_2, Q),\\
R_{11} + R_{20} &< I(X_1, U_2; Y_1|U_1, Q),\\
R_{11} + R_{10} + R_{20} &< I(X_1, U_2; Y_1|Q),\\
R_{22} &< I(X_2; Y_2|U_1, U_2, Q),\\
R_{22} + R_{20} &< I(X_2; Y_2|U_1, Q),\\
R_{22} + R_{10} &< I(X_2, U_1; Y_2|U_2, Q),\\
R_{22} + R_{20} + R_{10} &< I(X_2, U_1; Y_2|Q)
\end{aligned}$$

for some pmf $p(q)p(u_1, x_1|q)p(u_2, x_2|q)$.

Codebook generation. Fix a pmf $p(q)p(u_1, x_1|q)p(u_2, x_2|q)$. Generate a sequence $q^n \sim \prod_{i=1}^n p_Q(q_i)$. For $j = 1, 2$, randomly and conditionally independently generate $2^{nR_{j0}}$ sequences $u_j^n(m_{j0})$, $m_{j0} \in [1 : 2^{nR_{j0}}]$, each according to $\prod_{i=1}^n p_{U_j|Q}(u_{ji}|q_i)$. For each m_{j0}, randomly and conditionally independently generate $2^{nR_{jj}}$ sequences $x_j^n(m_{j0}, m_{jj})$, $m_{jj} \in [1 : 2^{nR_{jj}}]$, each according to $\prod_{i=1}^n p_{X_j|U_j,Q}(x_{ji}|u_{ji}(m_{j0}), q_i)$.

Encoding. To send $m_j = (m_{j0}, m_{jj})$, encoder $j = 1, 2$ transmits $x_j^n(m_{j0}, m_{jj})$.

Decoding. We use simultaneous nonunique decoding. Upon receiving y_1^n, decoder 1 finds the unique message pair $(\hat{m}_{10}, \hat{m}_{11})$ such that $(q^n, u_1^n(\hat{m}_{10}), u_2^n(m_{20}), x_1^n(\hat{m}_{10}, \hat{m}_{11}), y_1^n) \in \mathcal{T}_\epsilon^{(n)}$ for some $m_{20} \in [1 : 2^{nR_{20}}]$; otherwise it declares an error. Decoder 2 finds the message pair $(\hat{m}_{20}, \hat{m}_{22})$ similarly.

Analysis of the probability of error. Assume message pair $((1, 1), (1, 1))$ is sent. We bound the average probability of error for each decoder. First consider decoder 1. As shown in Table 6.1, we have eight cases to consider (here conditioning on q^n is suppressed). Cases 3 and 4, and 6 and 7, respectively, share the same pmf, and case 8 does not cause an error. Thus, we are left with only five error events and decoder 1 makes an error only if one or more of the following events occur:

$$\begin{aligned}
\mathcal{E}_{10} &= \{(Q^n, U_1^n(1), U_2^n(1), X_1^n(1, 1), Y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\},\\
\mathcal{E}_{11} &= \{(Q^n, U_1^n(1), U_2^n(1), X_1^n(1, m_{11}), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_{11} \neq 1\},\\
\mathcal{E}_{12} &= \{(Q^n, U_1^n(m_{10}), U_2^n(1), X_1^n(m_{10}, m_{11}), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_{10} \neq 1, m_{11}\},
\end{aligned}$$

	m_{10}	m_{20}	m_{11}	Joint pmf
1	1	1	1	$p(u_1^n, x_1^n)p(u_2^n)p(y_1^n\|x_1^n, u_2^n)$
2	1	1	$*$	$p(u_1^n, x_1^n)p(u_2^n)p(y_1^n\|u_1^n, u_2^n)$
3	$*$	1	$*$	$p(u_1^n, x_1^n)p(u_2^n)p(y_1^n\|u_2^n)$
4	$*$	1	1	$p(u_1^n, x_1^n)p(u_2^n)p(y_1^n\|u_2^n)$
5	1	$*$	$*$	$p(u_1^n, x_1^n)p(u_2^n)p(y_1^n\|u_1^n)$
6	$*$	$*$	1	$p(u_1^n, x_1^n)p(u_2^n)p(y_1^n)$
7	$*$	$*$	$*$	$p(u_1^n, x_1^n)p(u_2^n)p(y_1^n)$
8	1	$*$	1	$p(u_1^n, x_1^n)p(u_2^n)p(y_1^n\|x_1^n)$

Table 6.1. The joint pmfs induced by different (m_{10}, m_{20}, m_{11}) triples.

$$\mathcal{E}_{13} = \{(Q^n, U_1^n(1), U_2^n(m_{20}), X_1^n(1, m_{11}), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_{20} \neq 1, m_{11} \neq 1\},$$
$$\mathcal{E}_{14} = \{(Q^n, U_1^n(m_{10}), U_2^n(m_{20}), X_1^n(m_{10}, m_{11}), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_{10} \neq 1, m_{20} \neq 1, m_{11}\}.$$

Hence, the average probability of error for decoder 1 is upper bounded as

$$\mathsf{P}(\mathcal{E}_1) \le \mathsf{P}(\mathcal{E}_{10}) + \mathsf{P}(\mathcal{E}_{11}) + \mathsf{P}(\mathcal{E}_{12}) + \mathsf{P}(\mathcal{E}_{13}) + \mathsf{P}(\mathcal{E}_{14}).$$

We bound each term. By the LLN, $\mathsf{P}(\mathcal{E}_{10})$ tends to zero as $n \to \infty$. By the packing lemma, $\mathsf{P}(\mathcal{E}_{11})$ tends to zero as $n \to \infty$ if $R_{11} < I(X_1; Y_1|U_1, U_2, Q) - \delta(\epsilon)$. Similarly, by the packing lemma, $\mathsf{P}(\mathcal{E}_{12})$, $\mathsf{P}(\mathcal{E}_{13})$, and $\mathsf{P}(\mathcal{E}_{14})$ tend to zero as $n \to \infty$ if the conditions $R_{11} + R_{10} < I(X_1; Y_1|U_2, Q) - \delta(\epsilon)$, $R_{11} + R_{20} < I(X_1, U_2; Y_1|U_1, Q) - \delta(\epsilon)$, and $R_{11} + R_{10} + R_{20} < I(X_1, U_2; Y_1|Q) - \delta(\epsilon)$ are satisfied, respectively. The average probability of error for decoder 2 can be bounded similarly. Finally, substituting $R_{11} = R_1 - R_{10}$ and $R_{22} = R_2 - R_{20}$, and using the Fourier–Motzkin procedure with the constraints $0 \le R_{j0} \le R_j$, $j = 1, 2$, to eliminate R_{10} and R_{20} (see Appendix D for the details), we obtain the seven inequalities in Theorem 6.4 and two additional inequalities $R_1 < I(X_1; Y_1|U_1, U_2, Q) + I(X_2, U_1; Y_2|U_2, Q)$ and $R_2 < I(X_1, U_2; Y_1|U_1, Q) + I(X_2; Y_2|U_1, U_2, Q)$. The corresponding inner bound can be shown to be equivalent to the inner bound in Theorem 6.4; see Problem 6.12. The cardinality bound on $\mathcal{Q}$ can be proved using the convex cover method in Appendix C. This completes the proof of the Han–Kobayashi inner bound.

6.6 INJECTIVE DETERMINISTIC IC

Consider the deterministic interference channel depicted in Figure 6.5. The channel outputs are given by the functions

$$Y_1 = y_1(X_1, T_2),$$
$$Y_2 = y_2(X_2, T_1),$$

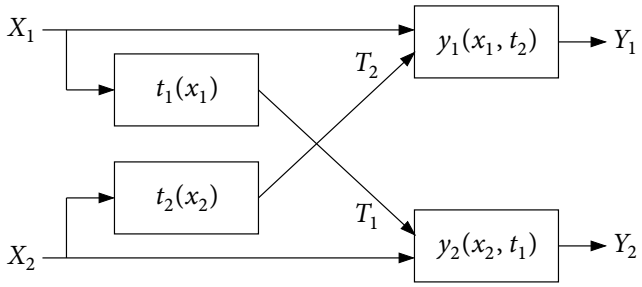


Figure 6.5. Injective deterministic interference channel.

where $T_1 = t_1(X_1)$ and $T_2 = t_2(X_2)$ are functions of X_1 and X_2, respectively. We assume that the functions y_1 and y_2 are injective in t_1 and t_2, respectively, that is, for every $x_1 \in \mathcal{X}_1$, $y_1(x_1, t_2)$ is a one-to-one function of t_2 and for every $x_2 \in \mathcal{X}_2$, $y_2(x_2, t_1)$ is a one-to-one function of t_1. Note that these conditions imply that $H(Y_1|X_1) = H(T_2)$ and $H(Y_2|X_2) = H(T_1)$.

This class of interference channels is motivated by the Gaussian IC, where the functions y_1 and y_2 are additions. Unlike the Gaussian IC, however, the channel is noiseless and its capacity region can be fully characterized.

Theorem 6.5. The capacity region of the injective deterministic interference channel is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned}
R_1 &\le H(Y_1|T_2, Q),\\
R_2 &\le H(Y_2|T_1, Q),\\
R_1 + R_2 &\le H(Y_1|Q) + H(Y_2|T_1, T_2, Q),\\
R_1 + R_2 &\le H(Y_1|T_1, T_2, Q) + H(Y_2|Q),\\
R_1 + R_2 &\le H(Y_1|T_1, Q) + H(Y_2|T_2, Q),\\
2R_1 + R_2 &\le H(Y_1|Q) + H(Y_1|T_1, T_2, Q) + H(Y_2|T_2, Q),\\
R_1 + 2R_2 &\le H(Y_1|T_1, Q) + H(Y_2|Q) + H(Y_2|T_1, T_2, Q)
\end{aligned}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)$.

The proof of achievability follows by noting that the above region coincides with the Han–Kobayashi inner bound (take $U_1 = T_1$, $U_2 = T_2$).

Remark 6.7. By the one-to-one conditions on the functions y_1 and y_2, decoder 1 knows T_2^n after decoding for X_1^n and decoder 2 knows T_1^n after decoding for X_2^n. As such, the interference random variables T_1 and T_2 can be naturally considered as the auxiliary random variables that represent the public messages in the Han–Kobayashi scheme.

Proof of the converse. Consider the first two inequalities in the characterization of the

capacity region. By specializing the outer bound in (6.4), we obtain

$$nR_1 \le nI(X_1; Y_1|X_2, Q) + n\epsilon_n = nH(Y_1|T_2, Q) + n\epsilon_n,$$
$$nR_2 \le nH(Y_2|T_1, Q) + n\epsilon_n,$$

where Q is the usual time-sharing random variable.

Now consider the third inequality. By Fano's inequality,

$$\begin{aligned}
n(R_1 + R_2) &\le I(M_1; Y_1^n) + I(M_2; Y_2^n) + n\epsilon_n \\
&\overset{(a)}{\le} I(M_1; Y_1^n) + I(M_2; Y_2^n, T_2^n) + n\epsilon_n \\
&\le I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n, T_2^n) + n\epsilon_n \\
&\overset{(b)}{\le} I(X_1^n; Y_1^n) + I(X_2^n; T_2^n, Y_2^n|T_1^n) + n\epsilon_n \\
&= H(Y_1^n) - H(Y_1^n|X_1^n) + I(X_2^n; T_2^n|T_1^n) + I(X_2^n; Y_2^n|T_1^n, T_2^n) + n\epsilon_n \\
&\overset{(c)}{=} H(Y_1^n) + H(Y_2^n|T_1^n, T_2^n) + n\epsilon_n \\
&\le \sum_{i=1}^{n} \big(H(Y_{1i}) + H(Y_{2i}|T_{1i}, T_{2i})\big) + n\epsilon_n \\
&= n\big(H(Y_1|Q) + H(Y_2|T_1, T_2, Q)\big) + n\epsilon_n.
\end{aligned}$$

Here step (a) is the key step in the proof. Even if a "genie" gives receiver 2 its common message T_2 as side information to help it find X_2, the capacity region does not change! Step (b) follows by the fact that X_2^n and T_1^n are independent, and (c) follows by the equalities $H(Y_1^n|X_1^n) = H(T_2^n)$ and $I(X_2^n; T_2^n|T_1^n) = H(T_2^n)$. Similarly, for the fourth inequality,

$$n(R_1 + R_2) \le n\big(H(Y_2|Q) + H(Y_1|T_1, T_2, Q)\big) + n\epsilon_n.$$

Consider the fifth inequality

$$\begin{aligned}
n(R_1 + R_2) &\le I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) + n\epsilon_n \\
&= H(Y_1^n) - H(Y_1^n|X_1^n) + H(Y_2^n) - H(Y_2^n|X_1^n) + n\epsilon_n \\
&\overset{(a)}{=} H(Y_1^n) - H(T_2^n) + H(Y_2^n) - H(T_1^n) + n\epsilon_n \\
&\le H(Y_1^n|T_1^n) + H(Y_2^n|T_2^n) + n\epsilon_n \\
&\le n\big(H(Y_1|T_1, Q) + H(Y_2|T_2, Q)\big) + n\epsilon_n,
\end{aligned}$$

where (a) follows by the one-to-one conditions of the injective deterministic IC. Following similar steps, consider the sixth inequality

$$\begin{aligned}
n(2R_1 + R_2) &\le 2I(M_1; Y_1^n) + I(M_2; Y_2^n) + n\epsilon_n \\
&\le I(X_1^n; Y_1^n) + I(X_1^n; Y_1^n, T_1^n|T_2^n) + I(X_2^n; Y_2^n) + n\epsilon_n \\
&= H(Y_1^n) - H(T_2^n) + H(T_1^n) + H(Y_1^n|T_1^n, T_2^n) + H(Y_2^n) - H(T_1^n) + n\epsilon_n \\
&= H(Y_1^n) - H(T_2^n) + H(Y_1^n|T_1^n, T_2^n) + H(Y_2^n) + n\epsilon_n \\
&\le H(Y_1^n) + H(Y_1^n|T_1^n, T_2^n) + H(Y_2^n|T_2^n) + n\epsilon_n \\
&\le n\big(H(Y_1|Q) + H(Y_1|T_1, T_2, Q) + H(Y_2|T_2, Q)\big) + n\epsilon_n.
\end{aligned}$$

Similarly, for the last inequality, we have

$$n(R_1 + 2R_2) \le n\big(H(Y_1|T_1, Q) + H(Y_2|Q) + H(Y_2|T_1, T_2, Q)\big) + n\epsilon_n.$$

This completes the proof of the converse.

6.7 CAPACITY REGION OF THE GAUSSIAN IC WITHIN HALF A BIT

As we have seen, the capacity (region) of the Gaussian IC is known only under certain strong and weak interference conditions and is achieved by extreme special cases of the Han–Kobayashi scheme where no rate splitting is used. How close is the Han–Kobayashi inner bound in its full generality to the capacity region?

We show that even a suboptimal evaluation of the Han–Kobayashi inner bound differs by no more than half a bit per rate component from the capacity region, independent of the channel parameters! We prove this result by first establishing bounds on the capacity region of a class of semideterministic ICs that include both the Gaussian IC and the injective deterministic IC in Section 6.6 as special cases.

6.7.1 Injective Semideterministic IC

Consider the semideterministic interference channel depicted in Figure 6.6. Here again the functions y_1, y_2 satisfy the condition that for every $x_1 \in \mathcal{X}_1$, $y_1(x_1, t_2)$ is a one-to-one function of t_2 and for every $x_2 \in \mathcal{X}_2$, $y_2(x_2, t_1)$ is a one-to-one function of t_1. The generalization comes from making the mappings from X_1 to T_1 and from X_2 to T_2 random.

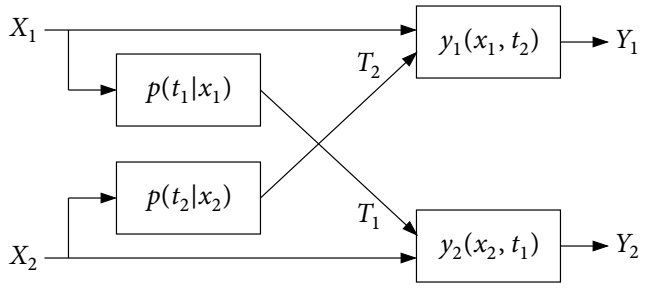


Figure 6.6. Injective semideterministic interference channel.

Note that if we assume the channel variables to be real-valued instead of finite, the Gaussian IC becomes a special case of this semideterministic IC with $T_1 = g_{21}X_1 + Z_2$ and $T_2 = g_{12}X_2 + Z_1$.

Outer bound on the capacity region. Consider the following outer bound on the capacity region of the injective semideterministic IC.

Proposition 6.1. Any achievable rate pair (R_1, R_2) for the injective semideterministic IC must satisfy the inequalities

$$\begin{aligned}
R_1 &\le H(Y_1|X_2, Q) - H(T_2|X_2),\\
R_2 &\le H(Y_2|X_1, Q) - H(T_1|X_1),\\
R_1 + R_2 &\le H(Y_1|Q) + H(Y_2|U_2, X_1, Q) - H(T_1|X_1) - H(T_2|X_2),\\
R_1 + R_2 &\le H(Y_1|U_1, X_2, Q) + H(Y_2|Q) - H(T_1|X_1) - H(T_2|X_2),\\
R_1 + R_2 &\le H(Y_1|U_1, Q) + H(Y_2|U_2, Q) - H(T_1|X_1) - H(T_2|X_2),\\
2R_1 + R_2 &\le H(Y_1|Q) + H(Y_1|U_1, X_2, Q) + H(Y_2|U_2, Q) - H(T_1|X_1) - 2H(T_2|X_2),\\
R_1 + 2R_2 &\le H(Y_2|Q) + H(Y_2|U_2, X_1, Q) + H(Y_1|U_1, Q) - 2H(T_1|X_1) - H(T_2|X_2)
\end{aligned}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)p_{T_1|X_1}(u_1|x_1)p_{T_2|X_2}(u_2|x_2)$.

This outer bound is established by extending the proof of the converse for the injective deterministic IC. We again use a genie argument with U_j conditionally independent of T_j given X_j, $j = 1, 2$. The details are given in Appendix 6B.

Remark 6.8. If we replace each channel $p(t_j|x_j)$, $j = 1, 2$, with a deterministic function $t_j(X_j)$, the above outer bound reduces to the capacity region of the injective deterministic IC in Theorem 6.5 by setting $U_j = T_j$, $j = 1, 2$.

Remark 6.9. The above outer bound is *not* tight under the strong interference condition in (6.7), and tighter outer bounds can be established.

Remark 6.10. We can obtain a corresponding outer bound for the Gaussian IC with differential entropies in place of entropies in the above outer bound.

Inner bound on the capacity region. The Han–Kobayashi inner bound with the restriction that $p(u_1, u_2|q, x_1, x_2) = p_{T_1|X_1}(u_1|x_1)\, p_{T_2|X_2}(u_2|x_2)$ reduces to the following.

Proposition 6.2. A rate pair (R_1, R_2) is achievable for the injective semideterministic IC if

$$\begin{aligned}
R_1 &< H(Y_1|U_2, Q) - H(T_2|U_2, Q),\\
R_2 &< H(Y_2|U_1, Q) - H(T_1|U_1, Q),\\
R_1 + R_2 &< H(Y_1|Q) + H(Y_2|U_1, U_2, Q) - H(T_1|U_1, Q) - H(T_2|U_2, Q),\\
R_1 + R_2 &< H(Y_1|U_1, U_2, Q) + H(Y_2|Q) - H(T_1|U_1, Q) - H(T_2|U_2, Q),\\
R_1 + R_2 &< H(Y_1|U_1, Q) + H(Y_2|U_2, Q) - H(T_1|U_1, Q) - H(T_2|U_2, Q),\\
2R_1 + R_2 &< H(Y_1|Q) + H(Y_1|U_1, U_2, Q) + H(Y_2|U_2, Q)\\
&\qquad - H(T_1|U_1, Q) - 2H(T_2|U_2, Q),
\end{aligned}$$

$$R_1 + 2R_2 < H(Y_2|Q) + H(Y_2|U_1, U_2, Q) + H(Y_1|U_1, Q) - 2H(T_1|U_1, Q) - H(T_2|U_2, Q)$$

for some pmf $p(q)p(x_1|q)p(x_2|q)p_{T_1|X_1}(u_1|x_1)p_{T_2|X_2}(u_2|x_2)$.

Considering the Gaussian IC, we obtain a corresponding inner bound with differential entropies in place of entropies. This inner bound coincides with the outer bound for the injective deterministic interference channel discussed in Section 6.6, where T_1 is a deterministic function of X_1 and T_2 is a deterministic function of X_2 (thus $U_1 = T_1$ and $U_2 = T_2$).

Gap between the inner and outer bounds. For a fixed $(Q, X_1, X_2) \sim p(q)p(x_1|q)p(x_2|q)$, let $\mathscr{R}_{\mathrm{o}}(Q, X_1, X_2)$ be the region defined by the set of inequalities in Proposition 6.1, and let $\mathscr{R}_{\mathrm{i}}(Q, X_1, X_2)$ denote the closure of the region defined by the set of inequalities in Proposition 6.2.

Lemma 6.3. If $(R_1, R_2) \in \mathscr{R}_{\mathrm{o}}(Q, X_1, X_2)$, then

$$\big(R_1 - I(X_2; T_2|U_2, Q),\ R_2 - I(X_1; T_1|U_1, Q)\big) \in \mathscr{R}_{\mathrm{i}}(Q, X_1, X_2).$$

To prove this lemma, we first construct the rate region $\overline{\mathscr{R}}_{\mathrm{o}}(Q, X_1, X_2)$ from the outer bound $\mathscr{R}_{\mathrm{o}}(Q, X_1, X_2)$ by replacing X_j in every positive conditional entropy term in $\mathscr{R}_{\mathrm{o}}(Q, X_1, X_2)$ with U_j for $j = 1, 2$. Clearly $\overline{\mathscr{R}}_{\mathrm{o}}(Q, X_1, X_2) \supseteq \mathscr{R}_{\mathrm{o}}(Q, X_1, X_2)$. Observing that

$$I(X_j; T_j|U_j) = H(T_j|U_j) - H(T_j|X_j), \quad j = 1, 2,$$

and comparing the rate region $\overline{\mathscr{R}}_{\mathrm{o}}(Q, X_1, X_2)$ to the inner bound $\mathscr{R}_{\mathrm{i}}(Q, X_1, X_2)$, we see that $\overline{\mathscr{R}}_{\mathrm{o}}(Q, X_1, X_2)$ can be equivalently characterized as the set of rate pairs (R_1, R_2) that satisfy the statement in Lemma 6.3.

6.7.2 Half-Bit Theorem for the Gaussian IC

We show that the outer bound in Proposition 6.1, when specialized to the Gaussian IC, is achievable within half a bit per dimension. For the Gaussian IC, the auxiliary random variables in the outer bound can be expressed as

$$\begin{aligned} U_1 &= g_{21}X_1 + Z_2' \\ U_2 &= g_{12}X_2 + Z_1', \end{aligned} \tag{6.10}$$

where Z_1' and Z_2' are $\mathrm{N}(0, 1)$, independent of each other and of (X_1, X_2, Z_1, Z_2). Substituting in the outer bound in Proposition 6.1, we obtain an outer bound $\mathscr{R}_{\mathrm{o}}$ on the capacity

region of the Gaussian IC that consists of all rate pairs (R_1, R_2) such that

$$\begin{aligned}
R_1 &\le \mathsf{C}(S_1),\\
R_2 &\le \mathsf{C}(S_2),\\
R_1 + R_2 &\le \mathsf{C}\left(\frac{S_1}{1+I_2}\right) + \mathsf{C}\left(I_2 + S_2\right),\\
R_1 + R_2 &\le \mathsf{C}\left(\frac{S_2}{1+I_1}\right) + \mathsf{C}\left(I_1 + S_1\right),\\
R_1 + R_2 &\le \mathsf{C}\left(\frac{S_1 + I_1 + I_1 I_2}{1+I_2}\right) + \mathsf{C}\left(\frac{S_2 + I_2 + I_1 I_2}{1+I_1}\right),\\
2R_1 + R_2 &\le \mathsf{C}\left(\frac{S_1}{1+I_2}\right) + \mathsf{C}\left(S_1 + I_1\right) + \mathsf{C}\left(\frac{S_2 + I_2 + I_1 I_2}{1+I_1}\right),\\
R_1 + 2R_2 &\le \mathsf{C}\left(\frac{S_2}{1+I_1}\right) + \mathsf{C}\left(S_2 + I_2\right) + \mathsf{C}\left(\frac{S_1 + I_1 + I_1 I_2}{1+I_2}\right).
\end{aligned} \tag{6.11}$$

Now we show that $\mathscr{R}_{\mathrm{o}}$ is achievable with half a bit.

Theorem 6.6 (Half-Bit Theorem). For the Gaussian IC, if $(R_1, R_2) \in \mathscr{R}_{\mathrm{o}}$, then $(R_1 - 1/2, R_2 - 1/2)$ is achievable.

To prove this theorem, consider Lemma 6.3 for the Gaussian IC with the auxiliary random variables in (6.10). Then, for $j = 1, 2$,

$$\begin{aligned}
I(X_j; T_j | U_j, Q) &= h(T_j | U_j, Q) - h(T_j | U_j, X_j, Q)\\
&\le h(T_j - U_j) - h(Z_j)\\
&= \frac{1}{2}.
\end{aligned}$$

6.7.3 Symmetric Degrees of Freedom

Consider the symmetric Gaussian IC with $S_1 = S_2 = S$ and $I_1 = I_2 = I$. Note that S and I fully characterize the channel. Define the *symmetric capacity* of the channel as $C_{\mathrm{sym}} = \max\{R\colon (R, R) \in \mathscr{C}\}$ and the *normalized* symmetric capacity as

$$d_{\mathrm{sym}} = \frac{C_{\mathrm{sym}}}{\mathsf{C}(S)}.$$

We find the *symmetric degrees of freedom* (DoF) d^*_{sym}, which is the limit of d_{sym} as the SNR and INR approach infinity. Note that in taking the limit, we are considering a sequence of channels rather than any particular channel. This limit, however, sheds light on the optimal coding strategies under different regimes of high SNR/INR.

Specializing the outer bound $\mathscr{R}_{\text{o}}$ in (6.11) to the symmetric case yields

$$C_{\text{sym}} \le \overline{C}_{\text{sym}} = \min\Big\{\mathsf{C}(S),\ \frac{1}{2}\,\mathsf{C}\Big(\frac{S}{1+I}\Big) + \frac{1}{2}\,\mathsf{C}(S+I),\ \mathsf{C}\Big(\frac{S+I+I^2}{1+I}\Big),\\ \frac{2}{3}\,\mathsf{C}\Big(\frac{S}{1+I}\Big) + \frac{1}{3}\,\mathsf{C}(S+2I+I^2)\Big\}.$$

By the half-bit theorem,

$$\frac{\overline{C}_{\text{sym}} - 1/2}{\mathsf{C}(S)} \le d_{\text{sym}} \le \frac{\overline{C}_{\text{sym}}}{\mathsf{C}(S)}.$$

Thus, the difference between the upper and lower bounds converges to zero as $S \to \infty$, and the normalized symmetric capacity converges to the degrees of freedom d^*_{sym}. This limit, however, depends on how I scales as $S \to \infty$. Since it is customary to measure SNR and INR in decibels (dBs), we consider the limit for a constant ratio between the logarithms of the INR and SNR

$$\alpha = \frac{\log I}{\log S},$$

or equivalently, $I = S^\alpha$. Then, as $S \to \infty$, the normalized symmetric capacity d_{sym} converges to

$$\begin{aligned} d^*_{\text{sym}}(\alpha) &= \lim_{S\to\infty} \frac{\overline{C}_{\text{sym}}|_{I=S^\alpha}}{\mathsf{C}(S)} \\ &= \min\{1,\ \max\{\alpha/2, 1-\alpha/2\},\ \max\{\alpha, 1-\alpha\},\\ &\qquad \max\{2/3, 2\alpha/3\} + \max\{1/3, 2\alpha/3\} - 2\alpha/3\}. \end{aligned}$$

Since the fourth bound inside the minimum is redundant, we have

$$d^*_{\text{sym}}(\alpha) = \min\{1,\ \max\{\alpha/2, 1-\alpha/2\},\ \max\{\alpha, 1-\alpha\}\}. \tag{6.12}$$

The symmetric DoF as a function of α is plotted in Figure 6.7. Note the unexpected W (instead of V) shape of the DoF curve. When interference is negligible ($\alpha \le 1/2$), the DoF is $1-\alpha$ and corresponds to the limit of the normalized rates achieved by treating interference as noise. For strong interference ($\alpha \ge 1$), the DoF is $\min\{1, \alpha/2\}$ and corresponds to simultaneous decoding. In particular, when interference is very strong ($\alpha \ge 2$), it does not impair the DoF. For moderate interference ($1/2 \le \alpha \le 1$), the DoF corresponds to the Han–Kobayashi rate splitting; see Problem 6.16. However, the DoF first increases until $\alpha = 2/3$ and then decreases to $1/2$ as α is increased to 1. Note that for $\alpha = 1/2$ and $\alpha = 1$, time division is also optimal.

Remark 6.11. In the above analysis, we scaled the channel gains under a fixed power constraint. Alternatively, we can fix the channel gains and scale the power P to infinity. It is not difficult to see that under this high power regime, $\lim_{P\to\infty} d^* = 1/2$, regardless of the values of the channel gains. Thus time division is asymptotically optimal.

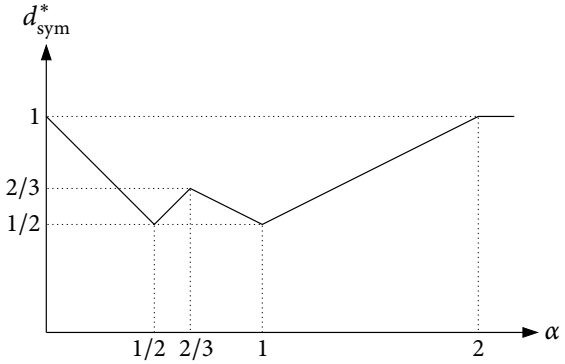


Figure 6.7. Degrees of freedom for symmetric Gaussian IC versus $\alpha = \log I / \log S$.

6.8 DETERMINISTIC APPROXIMATION OF THE GAUSSIAN IC

We introduce the q-ary expansion deterministic (QED) interference channel and show that it closely approximates the Gaussian IC in the limit of high SNR. The inputs to the QED-IC are q-ary L-vectors X_1 and X_2 for some "q-ary digit pipe" number L. We express X_1 as $[X_{1,L-1}, X_{1,L-2}, X_{1,L-3}, \ldots, X_{10}]^T$, where $X_{1l} \in [0 : q-1]$ for $l \in [0 : L-1]$, and similarly for X_2. Consider the symmetric case where the interference is specified by the parameter $\alpha \in [0, 2]$ such that αL is an integer. Define the "shift" parameter $s = (\alpha - 1)L$. The output of the channel depends on whether the shift is negative or positive.

Downshift. Here $s < 0$, i.e., $0 \le \alpha < 1$, and Y_1 is a q-ary L-vector with

$$Y_{1l} = \begin{cases} X_{1l} & \text{if } L + s \le l \le L - 1, \\ X_{1l} + X_{2,l-s} \pmod q & \text{if } 0 \le l \le L + s - 1. \end{cases}$$

This case is depicted in Figure 6.8. The outputs of the channel can be represented as

$$\begin{aligned} Y_1 &= X_1 + G_s X_2, \\ Y_2 &= G_s X_1 + X_2, \end{aligned} \tag{6.13}$$

where G_s is an $L \times L$ (down)shift matrix with $G_s(j, k) = 1$ if $k = j - s$ and $G_s(j, k) = 0$, otherwise.

Upshift. Here $s \ge 0$, i.e., $1 \le \alpha \le 2$, and Y_1 is a q-ary αL-vector with

$$Y_{1l} = \begin{cases} X_{2,l-s} & \text{if } L \le l \le L + s - 1, \\ X_{1l} + X_{2,l-s} \pmod q & \text{if } s \le l \le L - 1, \\ X_{1l} & \text{if } 0 \le l \le s - 1. \end{cases}$$

Again the outputs of the channel can be represented as in (6.13), where G_s is now an $(L + s) \times L$ (up)shift matrix with $G_s(j, k) = 1$ if $j = k$ and $G_s(j, k) = 0$, otherwise.

The capacity region of the symmetric QED-IC can be obtained by a straightforward

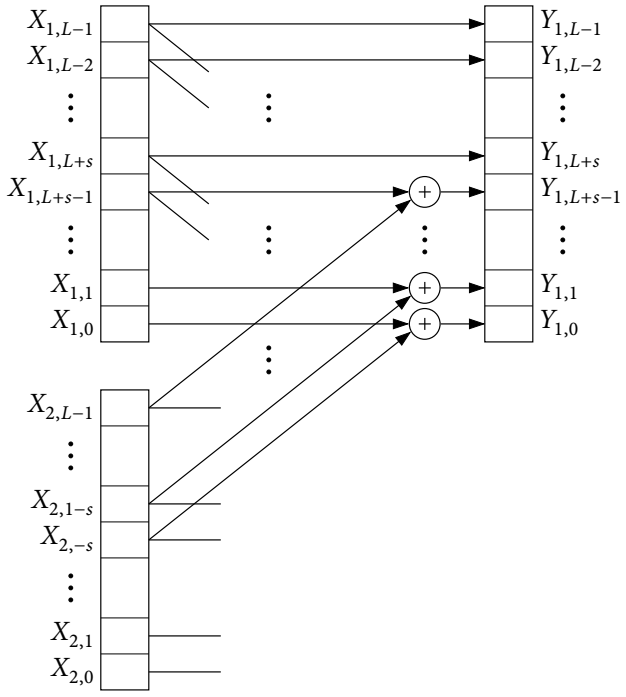


Figure 6.8. The q-ary expansion deterministic interference channel with downshift.

evaluation of the capacity region of the injective deterministic IC in Theorem 6.5. Let $R'_j = R_j/(L \log q)$, $j = 1, 2$. The normalized capacity region $\mathscr{C}'$ is the set of rate pairs (R'_1, R'_2) such that

$$\begin{aligned} R'_1 &\le 1, \\ R'_2 &\le 1, \\ R'_1 + R'_2 &\le \max\{2\alpha,\ 2 - 2\alpha\}, \\ R'_1 + R'_2 &\le \max\{\alpha,\ 2 - \alpha\}, \\ 2R'_1 + R'_2 &\le 2, \\ R'_1 + 2R'_2 &\le 2 \end{aligned} \tag{6.14}$$

for $\alpha \in [1/2, 1]$, and

$$\begin{aligned} R'_1 &\le 1, \\ R'_2 &\le 1, \\ R'_1 + R'_2 &\le \max\{2\alpha,\ 2 - 2\alpha\}, \\ R'_1 + R'_2 &\le \max\{\alpha,\ 2 - \alpha\} \end{aligned} \tag{6.15}$$

for $\alpha \in [0, 1/2) \cup (1, 2]$.

Surprisingly, the capacity region of the symmetric QED-IC can be achieved error-free using a simple single-letter linear coding scheme. We illustrate this scheme for the normalized symmetric capacity $C'_{\text{sym}} = \max\{R\colon (R, R) \in \mathscr{C}'\}$. Encoder $j = 1, 2$ represents its "single-letter" message by a q-ary LC'_{sym}-vector U_j and transmits $X_j = AU_j$, where A is an $L \times LC'_{\text{sym}}$ q-ary matrix A. Decoder j multiplies its received symbol Y_j by a corresponding $LC'_{\text{sym}} \times L$ matrix B to recover U_j perfectly! For example, consider a binary expansion deterministic IC with $q = 2$, $L = 12$, and $\alpha = 5/6$. The symmetric capacity for this case is $C_{\text{sym}} = 7$ bits/transmission. For encoding, we use the matrix

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

Note that the first 3 bits of U_j are sent twice, while $X_{1,2} = X_{1,3} = 0$. The transmitted symbol X_j and the two signal components of the received vector Y_j are illustrated in Figure 6.9. Decoding for U_1 can also be performed sequentially as follows (see Figure 6.9):

1. $U_{1,6} = Y_{1,11}$, $U_{1,5} = Y_{1,10}$, $U_{1,1} = Y_{1,1}$, and $U_{1,0} = Y_{1,0}$. Also $U_{2,6} = Y_{1,3}$ and $U_{2,5} = Y_{1,2}$.
2. $U_{1,4} = Y_{1,9} \oplus U_{2,6}$ and $U_{2,4} = Y_{1,4} \oplus U_{1,6}$.
3. $U_{1,3} = Y_{1,8} \oplus U_{2,5}$ and $U_{1,2} = Y_{1,7} \oplus U_{2,4}$.

This decoding procedure corresponds to multiplying the output by the matrix

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

Note that $BA = I$ and $BG_sA = 0$, and hence interference is canceled out while the intended signal is recovered perfectly.

Under the choice of the input $X_j = AU_j$, $j = 1, 2$, where U_j is uniformly distributed over the set of binary vectors of length LC'_{sym}, the symmetric capacity can be expressed as

$$C_{\text{sym}} = H(U_j) = I(U_j; Y_j) = I(X_j; Y_j), \quad j = 1, 2.$$

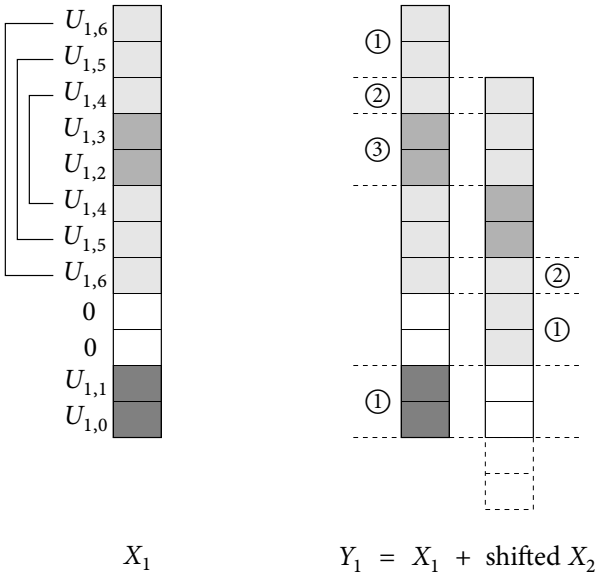


Figure 6.9. Transmitted symbol X_j and the received vector Y_j. The circled numbers denote the order of decoding.

Hence, the symmetric capacity is achieved error-free simply by treating interference as noise! In fact, the same linear coding technique can achieve the entire capacity region, which is generally characterized as the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< I(X_1; Y_1), \\ R_2 &< I(X_2; Y_2) \end{aligned} \tag{6.16}$$

for some pmf $p(x_1)p(x_2)$. A similar linear coding technique can be readily developed for any q-ary alphabet, dimension L, and $\alpha \in [0, 2]$ that achieves the entire capacity region by treating interference as noise.

6.8.1* QED-IC Approximation of the Gaussian IC

Considering the normalized capacity region characterization in (6.14) and (6.15), we can show that the normalized symmetric capacity of the symmetric QED-IC is

$$C'_{\text{sym}} = \min\{1,\ \max\{\alpha/2,\ 1 - \alpha/2\},\ \max\{\alpha,\ 1 - \alpha\}\} \tag{6.17}$$

for $\alpha \in [0, 2]$. This matches the DoF $d^*_{\text{sym}}(\alpha)$ of the symmetric Gaussian IC in (6.12) exactly. It can be shown that the Gaussian IC can be closely approximated by a QED-IC. Therefore, if a normalized rate pair is achievable for the QED-IC, then it is achievable for the corresponding Gaussian IC in the high SNR/INR limit, and vice versa.

We only sketch the proof that achievability carries over from the QED-IC to the Gaussian IC. Consider the q-ary expansions of the inputs and outputs of the Gaussian IC, e.g., $X_1 = X_{1,L-1}X_{1,L-2}\cdots X_{1,1}X_{1,0}\,.\,X_{1,-1}X_{1,-2}\cdots$, where $X_{1l} \in [0 : q-1]$ are q-ary digits.

Assuming $P = 1$, we express the channel outputs as $Y_1 = \sqrt{S}X_1 + \sqrt{I}X_2 + Z_1$ and $Y_2 = \sqrt{I}X_1 + \sqrt{S}X_2 + Z_2$. Suppose that $\sqrt{S}$ and $\sqrt{I}$ are powers of q. Then the digits of X_1, X_2, Y_1, and Y_2 align with each other. We further assume that the noise Z_1 is peak-power-constrained. Then, only the least-significant digits of Y_1 are affected by the noise. These digits are considered unusable for transmission. Now, we restrict each input digit to values from $[0 : \lfloor (q-1)/2 \rfloor]$. Thus, the signal additions at the q-ary digit-level are independent of each other, that is, there are no carry-overs, and the additions are effectively modulo-q. Note that this assumption does not affect the rate significantly because $\log\left(\lfloor (q-1)/2 \rfloor\right) / \log q$ can be made arbitrarily close to one by choosing q sufficiently large. Under the above assumptions, we arrive at a QED-IC, whereby the (random coding) achievability proof for rate pairs in (6.16) carries over to the Gaussian IC.

Remark 6.12. Recall that the capacity region of the QED-IC can be achieved by a simple single-letter linear coding technique (treating interference as noise) without using the full Han–Kobayashi coding scheme. Hence, the approximate capacity region and the DoF of the Gaussian IC can be both achieved simply by treating interference as noise. The resulting approximation gap, however, is significantly larger than half a bit.

6.9 EXTENSIONS TO MORE THAN TWO USER PAIRS

Interference channels with more than two user pairs are far less understood. For example, the notion of strong interference does not seem to naturally extend to more than two user pairs. These channels also exhibit the interesting property that decoding at each receiver is impaired by the *joint* effect of interference from the other senders rather by each sender's signal separately. Consequently, coding schemes that deal directly with the effect of the *combined interference signal* are expected to achieve higher rates. One such coding scheme is *interference alignment*, whereby the code is designed so that the combined interfering signal at each receiver is confined (*aligned*) to a subset of the receiver signal space. The subspace that contains the combined interference is discarded, while the desired signal is reconstructed from the orthogonal subspace. We illustrate this scheme in the following example.

Example 6.5 (k-User-pair symmetric QED-IC). Consider the k-user-pair QED-IC

$$Y_j = X_j + G_s \sum_{j' \neq j} X_{j'}, \quad j \in [1 : k],$$

where $X_1, \ldots, X_k$ are q-ary L vectors, $Y_1, \ldots, Y_k$ are q-ary L_s vectors, $L_s = \max\{L, L + s\}$, and G_s is the $L_s \times L$ s-shift matrix for some $s \in [-L, L]$. As before, let $\alpha = (L + s)/L$. If $\alpha = 1$, then the received signals are identical and the normalized symmetric capacity is $C'_{\text{sym}} = 1/k$, which is achieved via time division. However, if $\alpha \neq 1$, then the normalized symmetric capacity is

$$C'_{\text{sym}} = \min\{1, \max\{\alpha, 1 - \alpha\}, \max\{\alpha/2, 1 - \alpha/2\}\},$$

which is equal to the normalized symmetric capacity for the 2-user-pair case, regardless

of k! To show this, consider the single-letter linear coding technique described earlier for the 2-user-pair case. Then it is easy to check that the symmetric capacity is achievable (error-free), since the interfering signals from other senders are aligned in the same subspace and can be filtered out simultaneously.

Using the same approximation procedure detailed for the 2-user-pair case, this deterministic IC example shows that the DoF of the symmetric k-user-pair Gaussian IC is

$$d^*_{\text{sym}}(\alpha) = \begin{cases} 1/k & \text{if } \alpha = 1, \\ \min\{1, \max\{\alpha, 1-\alpha\}, \max\{\alpha/2, 1-\alpha/2\}\} & \text{otherwise.} \end{cases}$$

The DoF is achieved simply by treating interference as noise with a carefully chosen input pmf.

SUMMARY

- Discrete memoryless interference channel (DM-IC)
- Simultaneous nonunique decoding is optimal under strong interference
- Coded time sharing can strictly outperform time sharing
- Han–Kobayashi coding scheme:
  - Rate splitting and superposition coding
  - Fourier–Motzkin elimination
  - Optimal for injective deterministic ICs
- Gaussian interference channel:
  - Capacity region under strong interference achieved via simultaneous decoding
  - Sum-capacity under weak interference achieved by treating interference as noise
  - Genie-based converse proof
  - Han–Kobayashi coding scheme achieves within half a bit of the capacity region
  - Symmetric degrees of freedom
  - Approximation by the q-ary expansion deterministic IC in high SNR
  - Interference alignment
- **Open problems:**

  6.1. What is the capacity region of the Gaussian IC with weak interference?

  6.2. What is the generalization of strong interference to three or more user pairs?

6.3. What is the capacity region of the 3-user-pair injective deterministic IC?

6.4. Is the Han–Kobayashi inner bound tight in general?

BIBLIOGRAPHIC NOTES

The interference channel was first studied by Ahlswede (1974), who established basic inner and outer bounds including the simultaneous decoding inner bound in (6.3). The outer bound in (6.4) is based on a simple observation by L. Coviello that improves upon the outer bound in Sato (1977) by reversing the order of the union (over the input pmfs) and the intersection (over the channel pmfs). Carleial (1975) introduced the notion of very strong interference for the Gaussian IC and showed that the capacity region is the intersection of the capacity regions for the two component Gaussian MACs. The capacity region of the Gaussian IC with strong interference was established by Sato (1978b) and Han and Kobayashi (1981). Costa and El Gamal (1987) extended these results to the DM-IC.

Carleial (1978) introduced the idea of rate splitting and established an inner bound using successive cancellation decoding and (uncoded) time sharing. His inner bound was improved through simultaneous decoding and coded time sharing by Han and Kobayashi (1981). The inner bound in the Han–Kobayashi paper used four auxiliary random variables representing public and private messages and involved more inequalities than in Theorem 6.4. The equivalent characterization with only two auxiliary random variables and a reduced set of inequalities in Theorem 6.4 is due to Chong, Motani, Garg, and El Gamal (2008). The injective deterministic IC in Section 6.6 was introduced by El Gamal and Costa (1982), who used the genie argument to show that the Han–Kobayashi inner bound is tight.

Kramer (2004) developed a genie-based outer bound for the Gaussian IC. Shang, Kramer, and Chen (2009), Annapureddy and Veeravalli (2009), and Motahari and Khandani (2009) independently established the sum-capacity of the Gaussian IC with weak interference in Theorem 6.3. Our proof using the genie method follows the one by Annapureddy and Veeravalli (2009). The half-bit theorem was first established by Etkin, Tse, and Wang (2008) using the Han–Kobayashi inner bound and a variant of the genie-based outer bound by Kramer (2004). The proof in Section 6.7 using the injective semideterministic IC is due to Telatar and Tse (2007).

The approximation of the Gaussian IC by the q-ary expansion deterministic channel was first proposed by Avestimehr, Diggavi, and Tse (2011). Bresler, Parekh, and Tse (2010) applied this approach to approximate the many-to-one Gaussian IC. This approximation method was further refined by Jafar and Vishwanath (2010) and Bresler and Tse (2008). The symmetric capacity achieving linear coding scheme for the QED-IC is due to Jafar and Vishwanath (2010). Bandemer (2009) showed that the entire capacity region can be achieved by this linear coding scheme.

Interference alignment has been investigated for several classes of Gaussian channels by Maddah-Ali, Motahari, and Khandani (2008), Cadambe and Jafar (2008), Ghasemi,

Motahari, and Khandani (2010), Motahari, Gharan, Maddah-Ali, and Khandani (2009), Gou and Jafar (2010), and Nazer, Gastpar, Jafar, and Vishwanath (2009), and for QED-ICs by Jafar and Vishwanath (2010), Cadambe, Jafar, and Shamai (2009) and Bandemer, Vazquez-Vilar, and El Gamal (2009). Depending on the specific channel, this alignment is achieved via linear subspaces (Maddah-Ali, Motahari, and Khandani 2008), signal scale levels (Cadambe, Jafar, and Shamai 2009), time delay slots (Cadambe and Jafar 2008), or number-theoretic irrational bases (Motahari, Gharan, Maddah-Ali, and Khandani 2009). In each case, the subspace that contains the combined interference is disregarded, while the desired signal is reconstructed from the orthogonal subspace.

There are very few results on the IC with more than two user pairs beyond interference alignment. A straightforward extension of the Han–Kobayashi coding scheme is shown to be optimal for the deterministic IC (Gou and Jafar 2009), where the received signal is one-to-one to *all* interference signals given the intended signal. More interestingly, each receiver can decode for the combined (not individual) interference, which is achieved using structured codes for the many-to-one Gaussian IC (Bresler, Parekh, and Tse 2010). Decoding for the combined interference has been also applied to deterministic ICs with more than two user pairs (Bandemer and El Gamal 2011).

PROBLEMS

6.1. Establish the interference-as-noise inner bound in (6.2).

6.2. Prove the outer bound in (6.4).

6.3. Prove Lemma 6.1.

6.4. Verify the outer bound on the capacity region of the Gaussian IC in (6.11).

6.5. Show that the normalized capacity region of the QED-IC reduces to the regions in (6.14) and (6.15) and that the normalized symmetric capacity is given by (6.17).

6.6. *Successive cancellation decoding vs. simultaneous decoding.* Consider a DM-IC $p(y_1, y_2|x_1, x_2)$. As in the simple coding schemes discussed in Section 6.2, suppose that point-to-point codes are used. Consider the successive cancellation decoding scheme, where receiver 1 first decodes for M_2 and then decodes for its own message M_1. Likewise receiver 2 first decodes for M_1 and then for M_2.

(a) Find the rate region achieved by successive cancellation decoding.

(b) Show that this region is always contained in the simultaneous-decoding inner bound in (6.3).

6.7. *Successive cancellation decoding for the Gaussian IC.* In Chapter 4 we found that for the DM-MAC, successive cancellation decoding with time sharing achieves the same inner bound as simultaneous decoding. In this problem, we show that this is not the case for the interference channel.

Consider the Gaussian IC with SNRs S_1 and S_2 and INRs I_1 and I_2.

(a) Write down the rate region achieved by successive cancellation decoding with Gaussian codes and no power control.

(b) Under what conditions is this region equal to the simultaneous-nonunique-decoding inner bound in Section 6.4?

(c) How much worse can successive cancellation decoding be than simultaneous nonunique decoding?

6.8. *Handoff.* Consider two symmetric Gaussian ICs, one with SNR S and INR $I > S$, and the other with SNR I and INR S. Thus, the second Gaussian IC is equivalent to the setting where the messages are sent to the other receivers in the first Gaussian IC. Which channel has a larger capacity region?

6.9. *Power control.* Consider the symmetric Gaussian IC with SNR S and INR I.

(a) Write down the rate region achieved by treating interference as noise with time sharing between two transmission subblocks and power control. Express the region in terms of three parameters: time-sharing fraction $\alpha \in [0, 1]$ and two power allocation parameters $\beta_1, \beta_2 \in [0, 1]$.

(b) Similarly, write down the rate region achieved by simultaneous nonunique decoding with time sharing between two transmission subblocks and power control in terms of α, β_1, β_2.

6.10. *Gaussian Z interference channel.* Consider the Gaussian IC depicted in Figure 6.10 with SNRs S_1, S_2, and INR I_1. (Here the INR $I_2 = 0$.)

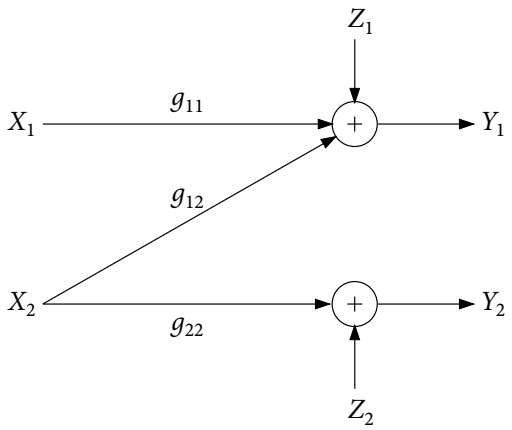


Figure 6.10. Gaussian interference channel with $I_2 = 0$.

(a) Find the capacity region when $S_2 \le I_1$.

(b) Find the sum-capacity when $I_1 \le S_2$.

(c) Find the capacity region when $S_2 \le I_1/(1 + S_1)$.

6.11. *Minimum-energy-per-bit region.* Consider the Gaussian IC with channel gains g_{11}, g_{12}, g_{21}, and g_{22}. Find the minimum-energy-per-bit region, that is, the set of all energy pairs $(E_1, E_2) = (P_1/R_1, P_2/R_2)$ such that the rate pair (R_1, R_2) is achievable with average code power pair (P_1, P_2).

6.12. *An equivalent characterization of the Han–Kobayashi inner bound.* Consider the inner bound on the capacity region of the DM-IC that consists of all rate pairs (R_1, R_2) such that

$$
\begin{aligned}
R_1 &< I(X_1; Y_1|U_2, Q),\\
R_1 &< I(X_1; Y_1|U_1, U_2, Q) + I(X_2, U_1; Y_2|U_2, Q),\\
R_2 &< I(X_2; Y_2|U_1, Q),\\
R_2 &< I(X_1, U_2; Y_1|U_1, Q) + I(X_2; Y_2|U_1, U_2, Q),\\
R_1 + R_2 &< I(X_1, U_2; Y_1|Q) + I(X_2; Y_2|U_1, U_2, Q),\\
R_1 + R_2 &< I(X_2, U_1; Y_2|Q) + I(X_1; Y_1|U_1, U_2, Q),\\
R_1 + R_2 &< I(X_1, U_2; Y_1|U_1, Q) + I(X_2, U_1; Y_2|U_2, Q),\\
2R_1 + R_2 &< I(X_1, U_2; Y_1|Q) + I(X_1; Y_1|U_1, U_2, Q) + I(X_2, U_1; Y_2|U_2, Q),\\
R_1 + 2R_2 &< I(X_2, U_1; Y_2|Q) + I(X_2; Y_2|U_1, U_2, Q) + I(X_1, U_2; Y_1|U_1, Q)
\end{aligned}
$$

for some pmf $p(q)p(u_1, x_1|q)p(u_2, x_2|q)$. Show that this inner bound is equivalent to the characterization of the Han–Kobayashi inner bound in Theorem 6.4. (Hint: Show that if $R_1 \ge I(X_1; Y_1|U_1, U_2, Q) + I(X_2, U_1; Y_2|U_2, Q)$ then the inequalities in Theorem 6.4 imply the above set of inequalities restricted to the choice of $U_1 = \emptyset$, and similarly for the case $R_2 \ge I(X_1, U_2; Y_1|U_1, Q) + I(X_2; Y_2|U_1, U_2, Q)$.)

6.13. *A semideterministic interference channel.* Consider the DM-IC depicted in Figure 6.11. Assume that $H(Y_2|X_2) = H(T)$. A message $M_j \in [1 : 2^{nR_j}]$ is to be sent from sender X_j to receiver Y_j for $j = 1, 2$. The messages are uniformly distributed and mutually independent. Find the capacity region of this DM-IC. (Hint: To prove achievability, simplify the Han–Kobayashi inner bound.)

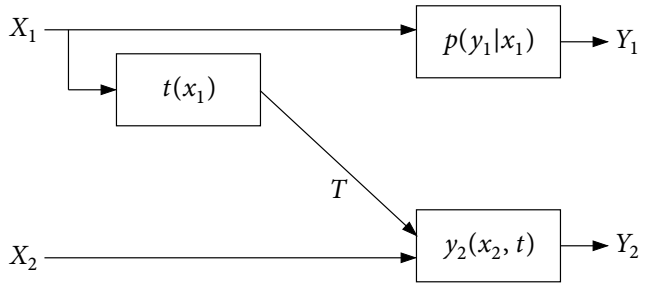


Figure 6.11. Semideterministic DM-IC.

6.14. *Binary injective deterministic interference channel.* Consider an injective deterministic IC with binary inputs X_1 and X_2 and ternary outputs $Y_1 = X_1 + X_2$ and $Y_2 = X_1 - X_2 + 1$. Find the capacity region of the channel.

6.15. *Deterministic interference channel with strong interference.* Find the conditions on the functions of the injective deterministic IC in Section 6.6 under which the channel has strong interference.

6.16. *Han–Kobayashi inner bound for the Gaussian IC.* Consider the Gaussian IC with SNRs S_1, S_2 and INRs I_1, I_2.

(a) Show that the Han–Kobayashi inner bound, when evaluated with Gaussian random variables, reduces to the set of rate pairs (R_1, R_2) such that

$$
\begin{aligned}
R_1 &< \mathsf{E}_Q\left[\mathsf{C}\left(\frac{S_1}{1+\lambda_{2Q} I_1}\right)\right],\\
R_2 &< \mathsf{E}_Q\left[\mathsf{C}\left(\frac{S_2}{1+\lambda_{1Q} I_2}\right)\right],\\
R_1 + R_2 &< \mathsf{E}_Q\left[\mathsf{C}\left(\frac{S_1 + \bar{\lambda}_{2Q} I_1}{1+\lambda_{2Q} I_1}\right) + \mathsf{C}\left(\frac{\lambda_{2Q} S_2}{1+\lambda_{1Q} I_2}\right)\right],\\
R_1 + R_2 &< \mathsf{E}_Q\left[\mathsf{C}\left(\frac{S_2 + \bar{\lambda}_{1Q} I_2}{1+\lambda_{1Q} I_2}\right) + \mathsf{C}\left(\frac{\lambda_{1Q} S_1}{1+\lambda_{2Q} I_1}\right)\right],\\
R_1 + R_2 &< \mathsf{E}_Q\left[\mathsf{C}\left(\frac{\lambda_{1Q} S_1 + \bar{\lambda}_{2Q} I_1}{1+\lambda_{2Q} I_1}\right) + \mathsf{C}\left(\frac{\lambda_{2Q} S_2 + \bar{\lambda}_{1Q} I_2}{1+\lambda_{1Q} I_2}\right)\right],\\
2R_1 + R_2 &\le \mathsf{E}_Q\left[\mathsf{C}\left(\frac{S_1 + \bar{\lambda}_{2Q} I_1}{1+\lambda_{2Q} I_1}\right) + \mathsf{C}\left(\frac{\lambda_{1Q} S_1}{1+\lambda_{2Q} I_1}\right) + \mathsf{C}\left(\frac{\lambda_{2Q} S_2 + \bar{\lambda}_{1Q} I_2}{1+\lambda_{1Q} I_2}\right)\right],\\
R_1 + 2R_2 &\le \mathsf{E}_Q\left[\mathsf{C}\left(\frac{S_2 + \bar{\lambda}_{1Q} I_2}{1+\lambda_{1Q} I_2}\right) + \mathsf{C}\left(\frac{\lambda_{2Q} S_2}{1+\lambda_{1Q} I_2}\right) + \mathsf{C}\left(\frac{\lambda_{1Q} S_1 + \bar{\lambda}_{2Q} I_1}{1+\lambda_{2Q} I_1}\right)\right]
\end{aligned}
$$

for some $\lambda_{1Q}, \lambda_{2Q} \in [0, 1]$ and pmf $p(q)$ with $|\mathcal{Q}| \le 6$.

(b) Suppose that $S_1 = S_2 = S$ and $I_1 = I_2 = I$. By further specializing the inner bound in part (a), show that the symmetric capacity is lower bounded as

$$
\begin{aligned}
C_{\text{sym}} \ge \max_{\lambda \in [0,1]} \min \Bigg\{ &\mathsf{C}\left(\frac{S}{1+\lambda I}\right), \mathsf{C}\left(\frac{\lambda S + \bar{\lambda} I}{1+\lambda I}\right),\\
&\frac{1}{2}\left(\mathsf{C}\left(\frac{S + \bar{\lambda} I}{1+\lambda I}\right) + \mathsf{C}\left(\frac{\lambda S}{1+\lambda I}\right)\right)\Bigg\}.
\end{aligned}
$$

(c) Use part (b) to show that the symmetric DoF is lower bounded as

$$
d^*_{\text{sym}}(\alpha) \ge \max\{1-\alpha,\ \min\{1-\alpha/2, \alpha\},\ \min\{1, \alpha/2\}\},
$$

which coincides with (6.12). (Hint: Consider $\lambda = 0, 1$, and $1/(1+S^{\alpha})$.)

6.17. *Genie-aided outer bound for the Gaussian IC.* Consider the symmetric Gaussian IC with SNR S and INR I. Establish the outer bound on the capacity region that consists of the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\le \mathsf{C}(S), \\ R_2 &\le \mathsf{C}(S), \\ R_1 + R_2 &\le \mathsf{C}(S) + \mathsf{C}(S/(1+I)), \\ R_1 + R_2 &\le 2\,\mathsf{C}(I + S/(1+I)), \\ 2R_1 + R_2 &\le \mathsf{C}(S+I) + \mathsf{C}(I + S/(1+I)) + \mathsf{C}(S) - \mathsf{C}(I), \\ R_1 + 2R_2 &\le \mathsf{C}(S+I) + \mathsf{C}(I + S/(1+I)) + \mathsf{C}(S) - \mathsf{C}(I). \end{aligned}$$

(Hint: For the last two inequalities, suppose that receiver 1 has side information $T_1 = \sqrt{I/P}X_1 + W_1$ and receiver 2 has side information $T_2 = \sqrt{I/P}X_2 + W_2$, where W_1 and W_2 are i.i.d. $\mathrm{N}(0,1)$, independent of (Z_1, Z_2).)
Remark: This bound, which is tighter than the outer bound in (6.11), is due to Etkin, Tse, and Wang (2008).

6.18. *Rate splitting for the more capable DM-BC.* Consider the alternative characterization of the capacity region in Section 5.6. Prove achievability of this region using rate splitting and Fourier–Motzkin elimination. (Hint: Divide M_1 into two independent messages M_{10} at rate R_{10} and M_{11} at rate R_{11}. Represent (M_{10}, M_2) by U and (M_{10}, M_{11}, M_2) by X.)

APPENDIX 6A PROOF OF LEMMA 6.2

The sum-capacity $\tilde{C}_{\text{sum}}$ is achieved by treating interference as Gaussian noise. Thus we only need to prove the converse. Let $Q \sim \mathrm{Unif}[1:n]$ be a time-sharing random variable independent of all other random variables and define $(T_1, T_2, Y_1, Y_2) = (T_{1Q}, T_{2Q}, Y_{1Q}, Y_{2Q})$. Thus, $(T_1, T_2, Y_1, Y_2) = (T_{1i}, T_{2i}, Y_{1i}, Y_{2i})$ with probability $1/n$ for $i \in [1:n]$. Suppose that a rate pair $(\tilde{R}_1, \tilde{R}_2)$ is achievable for the genie-aided channel. Then by Fano's inequality,

$$\begin{aligned} n\tilde{R}_1 &\le I(X_1^n; Y_1^n, T_1^n) + n\epsilon_n \\ &= I(X_1^n; T_1^n) + I(X_1^n; Y_1^n | T_1^n) + n\epsilon_n \\ &= h(T_1^n) - h(T_1^n | X_1^n) + h(Y_1^n | T_1^n) - h(Y_1^n | T_1^n, X_1^n) + n\epsilon_n \\ &\le h(T_1^n) - h(T_1^n | X_1^n) + \sum_{i=1}^n h(Y_{1i} | T_1^n) - h(Y_1^n | T_1^n, X_1^n) + n\epsilon_n \\ &\overset{(a)}{\le} h(T_1^n) - h(T_1^n | X_1^n) + \sum_{i=1}^n h(Y_{1i} | T_1) - h(Y_1^n | T_1^n, X_1^n) + n\epsilon_n \\ &\overset{(b)}{\le} h(T_1^n) - h(T_1^n | X_1^n) + nh(Y_1^* | T_1^*) - h(Y_1^n | T_1^n, X_1^n) + n\epsilon_n \\ &\overset{(c)}{=} h(T_1^n) - nh(T_1^* | X_1^*) + nh(Y_1^* | T_1^*) - h(Y_1^n | T_1^n, X_1^n) + n\epsilon_n, \end{aligned}$$

where (a) follows since $h(Y_{1i}|T_1^n) = h(Y_{1i}|T_1^n, Q) \le h(Y_{1i}|T_{1Q}, Q) \le h(Y_{1i}|T_{1Q})$, (b) follows by the maximum differential entropy lemma and concavity, and (c) follows since $h(T_1^n|X_1^n) = h(\eta\sqrt{I/P}\, W_1^n) = nh(\eta\sqrt{I/P}\, W_1) = nh(T_1^*|X_1^*)$. Similarly,

$$n\tilde{R}_2 \le h(T_2^n) - nh(T_2^*|X_2^*) + nh(Y_2^*|T_2^*) - h(Y_2^n|T_2^n, X_2^n) + n\epsilon_n.$$

Thus, we can upper bound the sum-rate as

$$\begin{aligned} n(\tilde{R}_1 + \tilde{R}_2) \le{}& h(T_1^n) - h(Y_2^n|T_2^n, X_2^n) - nh(T_1^*|X_1^*) + nh(Y_1^*|T_1^*) \\ &+ h(T_2^n) - h(Y_1^n|T_1^n, X_1^n) - nh(T_2^*|X_2^*) + nh(Y_2^*|T_2^*) + n\epsilon_n. \end{aligned}$$

Evaluating the first two terms, we obtain

$$\begin{aligned} h(T_1^n) - h(Y_2^n|T_2^n, X_2^n) &= h\big(\sqrt{I/P}\, X_1^n + \eta\sqrt{I/P}\, W_1^n\big) - h\big(\sqrt{I/P}\, X_1^n + Z_2^n \,\big|\, W_2^n\big) \\ &= h\big(\sqrt{I/P}\, X_1^n + V_1^n\big) - h\big(\sqrt{I/P}\, X_1^n + V_2^n\big), \end{aligned}$$

where $V_1^n = \eta\sqrt{I/P}\, W_1^n$ is i.i.d. $\mathrm{N}(0, \eta^2 I/P)$ and $V_2^n = Z_2^n - \mathsf{E}(Z_2^n|W_2^n)$ is i.i.d. $\mathrm{N}(0, 1-\rho^2)$. Given the useful genie condition $\eta^2 I/P \le 1-\rho^2$, express $V_2^n = V_1^n + V^n$, where V^n is i.i.d. $\mathrm{N}(0, 1-\rho^2-\eta^2 I/P)$, independent of V_1^n. Now let $(V, V_1, V_2, X_1) = (V_Q, V_{1Q}, V_{2Q}, X_{1Q})$ and consider

$$\begin{aligned} h(T_1^n) - h(Y_2^n|T_2^n, X_2^n) &= h\big(\sqrt{I/P}\, X_1^n + V_1^n\big) - h\big(\sqrt{I/P}\, X_1^n + V_1^n + V^n\big) \\ &= -I\left(V^n; \sqrt{I/P}\, X_1^n + V_1^n + V^n\right) \\ &= -nh(V) + h\big(V^n \,\big|\, \sqrt{I/P}\, X_1^n + V_1^n + V^n\big) \\ &\le -nh(V) + \sum_{i=1}^n h\big(V_i \,\big|\, \sqrt{I/P}\, X_1^n + V_1^n + V^n\big) \\ &\le -nh(V) + \sum_{i=1}^n h\big(V_i \,\big|\, \sqrt{I/P}\, X_{1i} + V_{1i} + V_i\big) \\ &\le -nh(V) + nh\big(V \,\big|\, \sqrt{I/P}\, X_1 + V_1 + V\big) \\ &\overset{(a)}{\le} -nI\big(V; \sqrt{I/P}\, X_1^* + V_1 + V\big) \\ &= nh\big(\sqrt{I/P}\, X_1^* + V_1\big) - nh\big(\sqrt{I/P}\, X_1^* + V_1 + V\big) \\ &= nh(T_1^*) - nh(Y_2^*|T_2^*, X_2^*), \end{aligned}$$

where (a) follows since Gaussian is the worst noise with a given average power in an additive noise channel with Gaussian input; see Problem 2.12. The other terms $h(T_2^n) - h(Y_1^n|T_1^n, X_1^n)$ can be bounded in the same manner. This completes the proof of the lemma.

APPENDIX 6B PROOF OF PROPOSITION 6.1

Consider a sequence of $(2^{nR_1}, 2^{nR_2})$ codes with $\lim_{n\to\infty} P_e^{(n)} = 0$. Furthermore, let X_1^n, X_2^n, T_1^n, T_2^n, Y_1^n, Y_2^n denote the random variables resulting from encoding and transmitting

the independent messages M_1 and M_2. Define random variables U_1^n, U_2^n such that U_{ji} is jointly distributed with X_{ji} according to $p_{T_j|X_j}(u_{ji}|x_{ji})$, conditionally independent of T_{ji} given X_{ji} for $j = 1, 2$ and $i \in [1 : n]$. By Fano's inequality,

$$\begin{aligned} nR_j &= H(M_j) \\ &\le I(M_j; Y_j^n) + n\epsilon_n \\ &\le I(X_j^n; Y_j^n) + n\epsilon_n. \end{aligned}$$

This directly yields a multiletter outer bound of the capacity region. We are looking for a nontrivial single-letter upper bound.

Observe that

$$\begin{aligned} I(X_1^n; Y_1^n) &= H(Y_1^n) - H(Y_1^n|X_1^n) \\ &= H(Y_1^n) - H(T_2^n|X_1^n) \\ &= H(Y_1^n) - H(T_2^n) \\ &\le \sum_{i=1}^n H(Y_{1i}) - \boxed{H(T_2^n)}, \end{aligned}$$

since Y_1^n and T_2^n are one-to-one given X_1^n, and T_2^n is independent of X_1^n. The second term $H(T_2^n)$, however, is not easily upper-bounded in a single-letter form. Now consider the following augmentation

$$\begin{aligned} I(X_1^n; Y_1^n) &\le I(X_1^n; Y_1^n, U_1^n, X_2^n) \\ &= I(X_1^n; U_1^n) + I(X_1^n; X_2^n|U_1^n) + I(X_1^n; Y_1^n|U_1^n, X_2^n) \\ &= H(U_1^n) - H(U_1^n|X_1^n) + H(Y_1^n|U_1^n, X_2^n) - H(Y_1^n|X_1^n, U_1^n, X_2^n) \\ &\overset{(a)}{=} H(T_1^n) - H(U_1^n|X_1^n) + H(Y_1^n|U_1^n, X_2^n) - H(T_2^n|X_2^n) \\ &\le \boxed{H(T_1^n)} - \sum_{i=1}^n H(U_{1i}|X_{1i}) + \sum_{i=1}^n H(Y_{1i}|U_{1i}, X_{2i}) - \sum_{i=1}^n H(T_{2i}|X_{2i}). \end{aligned}$$

The second and fourth terms in (a) represent the output of a memoryless channel given its input. Thus they readily single-letterize with equality. The third term can be upper-bounded in a single-letter form. The first term $H(T_1^n)$ will be used to cancel boxed terms such as $H(T_2^n)$ above. Similarly, we can write

$$\begin{aligned} I(X_1^n; Y_1^n) &\le I(X_1^n; Y_1^n, U_1^n) \\ &= I(X_1^n; U_1^n) + I(X_1^n; Y_1^n|U_1^n) \\ &= H(U_1^n) - H(U_1^n|X_1^n) + H(Y_1^n|U_1^n) - H(Y_1^n|X_1^n, U_1^n) \\ &= H(T_1^n) - H(U_1^n|X_1^n) + H(Y_1^n|U_1^n) - H(T_2^n) \\ &\le \boxed{H(T_1^n)} - \boxed{H(T_2^n)} - \sum_{i=1}^n H(U_{1i}|X_{1i}) + \sum_{i=1}^n H(Y_{1i}|U_{1i}), \end{aligned}$$

and

$$\begin{aligned} I(X_1^n; Y_1^n) &\le I(X_1^n; Y_1^n, X_2^n) \\ &= I(X_1^n; X_2^n) + I(X_1^n; Y_1^n | X_2^n) \\ &= H(Y_1^n | X_2^n) - H(Y_1^n | X_1^n, X_2^n) \\ &= H(Y_1^n | X_2^n) - H(T_2^n | X_2^n) \\ &\le \sum_{i=1}^n H(Y_{1i} | X_{2i}) - \sum_{i=1}^n H(T_{2i} | X_{2i}). \end{aligned}$$

By symmetry, similar bounds can be established for $I(X_2^n; Y_2^n)$, namely,

$$\begin{aligned} I(X_2^n; Y_2^n) &\le \sum_{i=1}^n H(Y_{2i}) - \boxed{H(T_1^n)}, \\ I(X_2^n; Y_2^n) &\le \boxed{H(T_2^n)} - \sum_{i=1}^n H(U_{2i} | X_{2i}) + \sum_{i=1}^n H(Y_{2i} | U_{2i}, X_{1i}) - \sum_{i=1}^n H(T_{1i} | X_{1i}), \\ I(X_2^n; Y_2^n) &\le \boxed{H(T_2^n)} - \boxed{H(T_1^n)} - \sum_{i=1}^n H(U_{2i} | X_{2i}) + \sum_{i=1}^n H(Y_{2i} | U_{2i}), \\ I(X_2^n; Y_2^n) &\le \sum_{i=1}^n H(Y_{2i} | X_{1i}) - \sum_{i=1}^n H(T_{1i} | X_{1i}). \end{aligned}$$

Now consider linear combinations of the above inequalities where all boxed terms are canceled. Combining them with the bounds using Fano's inequality and using a time-sharing variable $Q \sim \text{Unif}[1 : n]$ completes the proof of the outer bound.

CHAPTER 14

Joint Source–Channel Coding

In Chapters 4 through 9, we studied reliable communication of independent messages over noisy single-hop networks (channel coding), and in Chapters 10 through 13, we studied the dual setting of reliable communication of uncompressed sources over noiseless single-hop networks (source coding). These settings are special cases of the more general information flow problem of reliable communication of uncompressed sources over noisy single-hop networks. As we have seen in Section 3.9, separate source and channel coding is asymptotically sufficient for communicating a DMS over a DMC. Does such separation hold in general for communicating a k-DMS over a DM single-hop network?

In this chapter, we show that such separation does not hold in general. Thus in some multiuser settings it is advantageous to perform joint source–channel coding. We demonstrate this breakdown in separation through examples of lossless communication of a 2-DMS over a DM-MAC and over a DM-BC.

For the DM-MAC case, we show that joint source–channel coding can help communication by utilizing the correlation between the sources to induce statistical cooperation between the transmitters. We present a joint source–channel coding scheme that outperforms separate source and channel coding. We then show that this scheme can be improved when the sources have a common part, that is, a source that both senders can agree on with probability one.

For the DM-BC case, we show that joint source–channel coding can help communication by utilizing the statistical compatibility between the sources and the channel. We first consider a separate source and channel coding scheme based on the Gray–Wyner source coding system and Marton's channel coding scheme. The optimal rate–region for the Gray–Wyner system naturally leads to several definitions of common information between correlated sources. We then describe a joint source–channel coding scheme that outperforms the separate Gray–Wyner and Marton coding scheme.

Finally, we present a general single-hop network that includes as special cases many of the multiuser source and channel settings we discussed in previous chapters. We describe a hybrid source–channel coding scheme for this network.

14.1 LOSSLESS COMMUNICATION OF A 2-DMS OVER A DM-MAC

Consider the multiple access communication system depicted in Figure 14.1, where a 2-DMS (U_1, U_2) is to be communicated losslessly over a 2-sender DM-MAC $p(y|x_1, x_2)$.

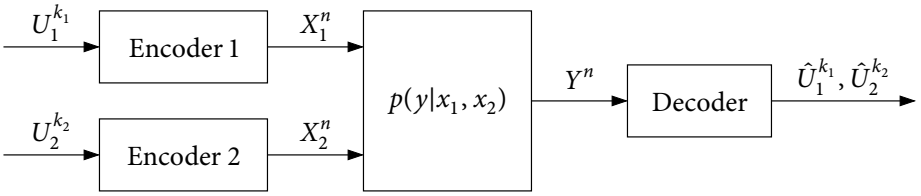


Figure 14.1. Communication of a 2-DMS over a 2-sender DM-MAC.

A $(|\mathcal{U}_1|^{k_1}, |\mathcal{U}_2|^{k_2}, n)$ joint source–channel code of rate pair $(r_1, r_2) = (k_1/n, k_2/n)$ for this setup consists of

- two encoders, where encoder $j = 1, 2$ assigns a sequence $x_j^n(u_j^{k_j}) \in \mathcal{X}_j^n$ to each sequence $u_j^{k_j} \in \mathcal{U}_j^{k_j}$, and
- a decoder that assigns an estimate $(\hat{u}_1^{k_1}, \hat{u}_2^{k_2}) \in \hat{\mathcal{U}}_1^{k_1} \times \hat{\mathcal{U}}_2^{k_2}$ to each sequence $y^n \in \mathcal{Y}^n$.

The probability of error is defined as $P_e^{(n)} = \mathsf{P}\{(\hat{U}_1^{k_1}, \hat{U}_2^{k_2}) \neq (U_1^{k_1}, U_2^{k_2})\}$. We say that the sources are communicated losslessly over the DM-MAC if there exists a sequence of $(|\mathcal{U}_1|^{k_1}, |\mathcal{U}_2|^{k_2}, n)$ codes such that $\lim_{n\to\infty} P_e^{(n)} = 0$. The problem is to find the necessary and sufficient condition for lossless communication. For simplicity, we assume henceforth the rates $r_1 = r_2 = 1$ symbol/transmission.

First consider the following sufficient condition for separate source and channel coding. We know that the capacity region $\mathscr{C}$ of the DM-MAC is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\le I(X_1; Y|X_2, Q), \\ R_2 &\le I(X_2; Y|X_1, Q), \\ R_1 + R_2 &\le I(X_1, X_2; Y|Q) \end{aligned}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)$. We also know from the Slepian–Wolf theorem that the optimal rate region $\mathscr{R}^*$ for distributed lossless source coding is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\ge H(U_1|U_2), \\ R_2 &\ge H(U_2|U_1), \\ R_1 + R_2 &\ge H(U_1, U_2). \end{aligned}$$

Hence, if the intersection of the interiors of $\mathscr{C}$ and $\mathscr{R}^*$ is not empty, that is, there exists a pmf $p(q)p(x_1|q)p(x_2|q)$ such that

$$\begin{aligned} H(U_1|U_2) &< I(X_1; Y|X_2, Q), \\ H(U_2|U_1) &< I(X_2; Y|X_1, Q), \\ H(U_1, U_2) &< I(X_1, X_2; Y|Q), \end{aligned} \tag{14.1}$$

then the 2-DMS (U_1, U_2) can be communicated losslessly over the DM-MAC using separate source and channel coding. The encoders use Slepian–Wolf coding (binning) to encode (U_1^n, U_2^n) into the bin indices $(M_1, M_2) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$. The encoders then transmit the codeword pair $(x_1^n(M_1), x_2^n(M_2))$ selected from a randomly generated channel codebook; see Section 4.5. The decoder first performs joint typicality decoding to find (M_1, M_2) and then recovers (U_1^n, U_2^n) by finding the unique jointly typical sequence pair in the product bin with index pair (M_1, M_2). Since the rate pair (R_1, R_2) satisfies the conditions for both lossless source coding and reliable channel coding, the end-to-end probability of error tends to zero as $n \to \infty$. Note that although the joint pmf on (M_1, M_2) is not necessarily uniform, the message pair can still be reliably transmitted to the receiver if $(R_1, R_2) \in \mathscr{C}$ (see Problem 4.13).

Consider the following examples for which this sufficient condition for separate source and channel coding is also necessary.

Example 14.1 (MAC with orthogonal components). Let (U_1, U_2) be an arbitrary 2-DMS and $p(y|x_1, x_2) = p(y_1|x_1)p(y_2|x_2)$ be a DM-MAC with output $Y = (Y_1, Y_2)$ that consists of two separate DMCs, $p(y_1|x_1)$ with capacity C_1 and $p(y_2|x_2)$ with capacity C_2. The sources can be communicated losslessly over this MAC if

$$\begin{aligned} H(U_1|U_2) &< C_1, \\ H(U_2|U_1) &< C_2, \\ H(U_1, U_2) &< C_1 + C_2. \end{aligned}$$

Conversely, if one of the following inequalities is satisfied:

$$\begin{aligned} H(U_1|U_2) &> C_1, \\ H(U_2|U_1) &> C_2, \\ H(U_1, U_2) &> C_1 + C_2, \end{aligned}$$

then the sources cannot be communicated losslessly over the channel. Thus source–channel separation holds for this case.

Example 14.2 (Independent sources). Let U_1 and U_2 be independent sources with entropies $H(U_1)$ and $H(U_2)$, respectively, and $p(y|x_1, x_2)$ be an arbitrary DM-MAC. Source channel separation again holds in this case. That is, the sources can be communicated losslessly over the DM-MAC by separate source and channel coding if

$$\begin{aligned} H(U_1) &< I(X_1; Y|X_2, Q), \\ H(U_2) &< I(X_2; Y|X_1, Q), \\ H(U_1) + H(U_2) &< I(X_1, X_2; Y|Q), \end{aligned}$$

for some pmf $p(q)p(x_1|q)p(x_2|q)$, and the converse holds in general.

Does source–channel separation hold in general for lossless communication of an arbitrary 2-DMS (U_1, U_2) over an arbitrary DM-MAC $p(y|x_1, x_2)$? In other words, is it always the case that if the intersection of $\mathscr{R}^*$ and $\mathscr{C}$ is empty for a 2-DMS and a DM-MAC,

then the 2-DMS cannot be communicated losslessly over the DM-MAC? To answer this question, consider the following.

Example 14.3. Let (U_1, U_2) be a 2-DMS with $\mathcal{U}_1 = \mathcal{U}_2 = \{0, 1\}$, $p_{U_1,U_2}(0, 0) = p_{U_1,U_2}(0, 1) = p_{U_1,U_2}(1, 1) = 1/3$, and $p_{U_1,U_2}(1, 0) = 0$. Let $p(y|x_1, x_2)$ be a binary erasure MAC with $\mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}$, $\mathcal{Y} = \{0, 1, 2\}$, and $Y = X_1 + X_2$ (see Example 4.2). The optimal rate region $\mathscr{R}^*$ for this 2-DMS and the capacity region of the binary erasure MAC are sketched in Figure 14.2. Note that the intersection of these two regions is empty since $H(U_1, U_2) = \log 3 = 1.585$ and $\max_{p(x_1)p(x_2)} I(X_1, X_2; Y) = 1.5$. Hence, $H(U_1, U_2) > \max_{p(x_1)p(x_2)} I(X_1, X_2; Y)$ and (U_1, U_2) cannot be communicated losslessly over the erasure DM-MAC using separate source and channel coding.

Now consider an uncoded transmission scheme in which the encoders transmit $X_{1i} = U_{1i}$ and $X_{2i} = U_{2i}$ in time $i \in [1 : n]$. It is easy to see that this scheme achieves *error-free* communication! Thus using separate source and channel coding for sending a 2-DMS over a DM-MAC is *not* optimal in general.

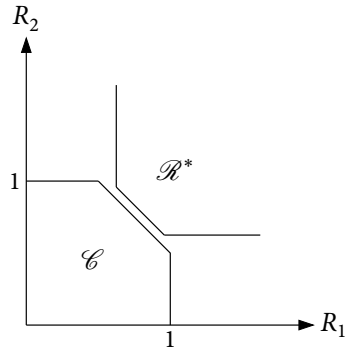


Figure 14.2. Separate source and channel coding fails since $\mathscr{R}^* \cap \mathscr{C} = \emptyset$.

A general necessary and sufficient condition for lossless communication of a 2-DMS over a DM-MAC is not known. In the following we present joint source–channel coding schemes that include as special cases the aforementioned separate source and channel coding scheme and the uncoded transmission scheme in Example 14.3.

14.1.1 A Joint Source–Channel Coding Scheme

We establish the following sufficient condition for lossless communication of a 2-DMS over a DM-MAC.

Theorem 14.1. A 2-DMS (U_1, U_2) can be communicated losslessly over a DM-MAC $p(y|x_1, x_2)$ at rates $r_1 = r_2 = 1$ if

$$H(U_1|U_2) < I(X_1; Y|U_2, X_2, Q),$$
$$H(U_2|U_1) < I(X_2; Y|U_1, X_1, Q),$$

$$H(U_1, U_2) < I(X_1, X_2; Y|Q)$$

for some conditional pmf $p(q, x_1, x_2|u_1, u_2) = p(q)p(x_1|u_1, q)p(x_2|u_2, q)$ with $|\mathcal{Q}| \le 3$.

This theorem recovers the following as special cases:

- Separate source and channel coding: We set $p(x_1|u_1, q)p(x_2|u_2, q) = p(x_1|q)p(x_2|q)$, that is, (X_1, X_2, Q) is independent of (U_1, U_2). Then, the set of inequalities in the theorem simplifies to (14.1).
- Example 14.3: Set $Q = \emptyset$, $X_1 = U_1$, and $X_2 = U_2$.

14.1.2 Proof of Theorem 14.1

We establish achievability for $|\mathcal{Q}| = 1$; the rest of the proof follows by time sharing.

Codebook generation. Fix a conditional pmf $p(x_1|u_1)p(x_2|u_2)$. For each $u_1^n \in \mathcal{U}_1^n$, randomly and independently generate a sequence $x_1^n(u_1^n)$ according to $\prod_{i=1}^n p_{X_1|U_1}(x_{1i}|u_{1i})$. Similarly, generate a sequence $x_2^n(u_2^n)$, $u_2^n \in \mathcal{U}_2^n$, according to $\prod_{i=1}^n p_{X_2|U_2}(x_{2i}|u_{2i})$.

Encoding. Upon observing u_1^n, encoder 1 transmits $x_1^n(u_1^n)$. Similarly encoder 2 transmits $x_2^n(u_2^n)$. Note that with high probability, no more than $2^{n(H(U_1,U_2)+\delta(\epsilon))}$ codeword pairs (x_1^n, x_2^n) can simultaneously occur.

Decoding. The decoder declares $(\hat{u}_1^n, \hat{u}_2^n)$ to be the source pair estimate if it is the unique pair such that $(\hat{u}_1^n, \hat{u}_2^n, x_1^n(\hat{u}_1^n), x_2^n(\hat{u}_2^n), y^n) \in \mathcal{T}_\epsilon^{(n)}$; otherwise it declares an error.

Analysis of the probability of error. The decoder makes an error iff one or more of the following events occur:

$$\begin{aligned}
\mathcal{E}_1 &= \{(U_1^n, U_2^n, X_1^n(U_1^n), X_2^n(U_2^n), Y^n) \notin \mathcal{T}_\epsilon^{(n)}\},\\
\mathcal{E}_2 &= \{(\tilde{u}_1^n, U_2^n, X_1^n(\tilde{u}_1^n), X_2^n(U_2^n), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{u}_1^n \neq U_1^n\},\\
\mathcal{E}_3 &= \{(U_1^n, \tilde{u}_2^n, X_1^n(U_1^n), X_2^n(\tilde{u}_2^n), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{u}_2^n \neq U_2^n\},\\
\mathcal{E}_4 &= \{(\tilde{u}_1^n, \tilde{u}_2^n, X_1^n(\tilde{u}_1^n), X_2^n(\tilde{u}_2^n), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{u}_1^n \neq U_1^n, \tilde{u}_2^n \neq U_2^n\}.
\end{aligned}$$

Thus, the average probability of error is upper bounded as

$$\mathsf{P}(\mathcal{E}) \le \mathsf{P}(\mathcal{E}_1) + \mathsf{P}(\mathcal{E}_2) + \mathsf{P}(\mathcal{E}_3) + \mathsf{P}(\mathcal{E}_4).$$

By the LLN, $\mathsf{P}(\mathcal{E}_1)$ tends to zero as $n \to \infty$. Next consider the second term. By the union of events bound,

$$\begin{aligned}
\mathsf{P}(\mathcal{E}_2) &= \sum_{u_1^n} p(u_1^n)\, \mathsf{P}\{(\tilde{u}_1^n, U_2^n, X_1^n(\tilde{u}_1^n), X_2^n(U_2^n), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{u}_1^n \neq u_1^n \,\big|\, U_1^n = u_1^n\}\\
&\le \sum_{u_1^n} p(u_1^n) \sum_{\tilde{u}_1^n \neq u_1^n} \mathsf{P}\{(\tilde{u}_1^n, U_2^n, X_1^n(\tilde{u}_1^n), X_2^n(U_2^n), Y^n) \in \mathcal{T}_\epsilon^{(n)} \,\big|\, U_1^n = u_1^n\}.
\end{aligned}$$

Now conditioned on $\{U_1^n = u_1^n\}$, $(U_2^n, X_1^n(\tilde{u}_1^n), X_2^n(U_2^n), Y^n) \sim p(u_2^n, x_2^n, y^n|u_1^n)p(x_1^n|\tilde{u}_1^n) = \prod_{i=1}^n p_{U_2,X_2,Y|U_1}(u_{2i}, x_{2i}, y_i|u_{1i})p_{X_1|U_1}(x_{1i}|\tilde{u}_{1i})$ for all $\tilde{u}_1^n \neq u_1^n$. Thus

$$\begin{aligned}
\mathsf{P}(\mathcal{E}_2) &\le \sum_{u_1^n} p(u_1^n) \sum_{\substack{\tilde{u}_1^n \neq u_1^n \\ (\tilde{u}_1^n, u_2^n, x_1^n, x_2^n, y^n) \in \mathcal{T}_\epsilon^{(n)}}} p(u_2^n, x_2^n, y^n|u_1^n)p(x_1^n|\tilde{u}_1^n) \\
&= \sum_{(\tilde{u}_1^n, u_2^n, x_1^n, x_2^n, y^n) \in \mathcal{T}_\epsilon^{(n)}} \sum_{u_1^n \neq \tilde{u}_1^n} p(u_1^n, u_2^n, x_2^n, y^n)p(x_1^n|\tilde{u}_1^n) \\
&\le \sum_{(\tilde{u}_1^n, u_2^n, x_1^n, x_2^n, y^n) \in \mathcal{T}_\epsilon^{(n)}} \sum_{u_1^n} p(u_1^n, u_2^n, x_2^n, y^n)p(x_1^n|\tilde{u}_1^n) \\
&= \sum_{(\tilde{u}_1^n, u_2^n, x_1^n, x_2^n, y^n) \in \mathcal{T}_\epsilon^{(n)}} p(u_2^n, x_2^n, y^n)p(x_1^n|\tilde{u}_1^n) \\
&= \sum_{(u_2^n, x_2^n, y^n) \in \mathcal{T}_\epsilon^{(n)}} p(u_2^n, x_2^n, y^n) \sum_{(\tilde{u}_1^n, x_1^n) \in \mathcal{T}_\epsilon^{(n)}(U_1, X_1|u_2^n, x_2^n, y^n)} p(x_1^n|\tilde{u}_1^n) \\
&\le \sum_{(\tilde{u}_1^n, x_1^n) \in \mathcal{T}_\epsilon^{(n)}(U_1, X_1|u_2^n, x_2^n, y^n)} p(x_1^n|\tilde{u}_1^n) \\
&\le 2^{n(H(U_1,X_1|U_2,X_2,Y) - H(X_1|U_1) + 2\delta(\epsilon))}.
\end{aligned}$$

Collecting the entropy terms, we have

$$\begin{aligned}
&H(U_1, X_1|U_2, X_2, Y) - H(X_1|U_1) \\
&\quad = H(U_1, X_1|U_2, X_2, Y) - H(U_1, X_1|U_2, X_2) - H(X_1|U_1) + H(U_1, X_1|U_2, X_2) \\
&\quad \overset{(a)}{=} -I(U_1, X_1; Y|U_2, X_2) + H(U_1|U_2) \\
&\quad \overset{(b)}{=} -I(X_1; Y|U_2, X_2) + H(U_1|U_2),
\end{aligned}$$

where (a) follows since $X_1 \to U_1 \to U_2 \to X_2$ form a Markov chain and (b) follows since $(U_1, U_2) \to (X_1, X_2) \to Y$ form a Markov chain. Thus $\mathsf{P}(\mathcal{E}_2)$ tends to zero as $n \to \infty$ if $H(U_1|U_2) < I(X_1; Y|U_2, X_2) - 2\delta(\epsilon)$. Similarly, $\mathsf{P}(\mathcal{E}_3)$ and $\mathsf{P}(\mathcal{E}_4)$ tend to zero as $n \to \infty$ if $H(U_2|U_1) < I(X_2; Y|U_1, X_1) - 2\delta(\epsilon)$ and $H(U_1, U_2) < I(X_1, X_2; Y) - 3\delta(\epsilon)$. This completes the proof of Theorem 14.1.

Suboptimality of the coding scheme. The coding scheme used in the above proof is not optimal in general. Suppose $U_1 = U_2 = U$. Then Theorem 14.1 reduces to the sufficient condition

$$\begin{aligned}
H(U) &< \max_{p(q)p(x_1|q,u)p(x_2|q,u)} I(X_1, X_2; Y|Q) \\
&= \max_{p(x_1|u)p(x_2|u)} I(X_1, X_2; Y). \qquad (14.2)
\end{aligned}$$

However, since both senders observe the same source, they can first encode the source losslessly at rate $H(U)$ and then transmit the source description using cooperative channel

coding; see Problem 4.9. Thus, the source can be communicated losslessly if

$$H(U) < \max_{p(x_1,x_2)} I(X_1, X_2; Y),$$

which is a less stringent condition than that in (14.2). Hence, when U_1 and U_2 have a *common part*, we can improve upon the joint source–channel coding scheme for Theorem 14.1. In the following subsection, we formally define the common part between two correlated sources. Subsequently, we present separate and joint source–channel coding schemes that incorporate this common part.

14.1.3 Common Part of a 2-DMS

Let (U_1, U_2) be a pair of random variables. Arrange $p(u_1, u_2)$ in a block diagonal form with the maximum possible number k of nonzero blocks, as shown in Figure 14.3. The *common part* between U_1 and U_2 is the random variable U_0 that takes the value u_0 if (U_1, U_2) is in block $u_0 \in [1 : k]$. Note that U_0 can be determined by U_1 or U_2 alone.

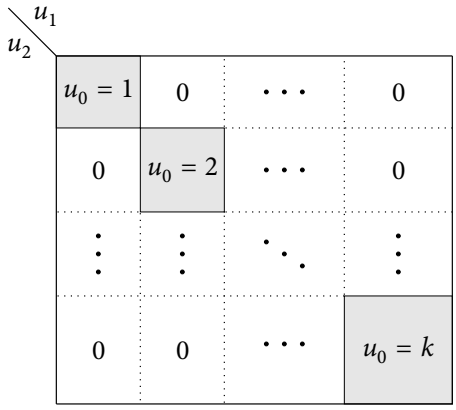


Figure 14.3. Block diagonal arrangement of the joint pmf $p(u_1, u_2)$.

Formally, let $g_1 : \mathcal{U}_1 \to [1 : k]$ and $g_2 : \mathcal{U}_2 \to [1 : k]$ be two functions with the largest integer k such that $\mathsf{P}\{g_1(U_1) = u_0\} > 0$, $\mathsf{P}\{g_2(U_2) = u_0\} > 0$ for $u_0 \in [1 : k]$ and $\mathsf{P}\{g_1(U_1) = g_2(U_2)\} = 1$. The common part between U_1 and U_2 is defined as $U_0 = g_1(U_1) = g_2(U_2)$, which is unique up to relabeling of the symbols.

To better understand this definition, consider the following.

Example 14.4. Let (U_1, U_2) be a pair of random variables with the joint pmf in Table 14.1. Here $k = 2$ and the common part U_0 has the pmf $p_{U_0}(1) = 0.7$ and $p_{U_0}(2) = 0.3$.

Now let (U_1, U_2) be a 2-DMS. What is the common part between the sequences U_1^n and U_2^n? It turns out that this common part is always U_0^n (up to relabeling). Thus we say that U_0 is the common part of the 2-DMS (U_1, U_2).

		$u_0 = 1$		$u_0 = 2$	
	u_1 / u_2	1	2	3	4
	1	0.1	0.2	0	0
$u_0 = 1$	2	0.1	0.1	0	0
	3	0.1	0.1	0	0
$u_0 = 2$	4	0	0	0.2	0.1

Table 14.1. Joint pmf for Example 14.4.

14.1.4 Three-Index Separate Source and Channel Coding Scheme

Taking the common part into consideration, we can generalize the 2-index separate source and channel coding scheme discussed earlier in this section into a 3-index scheme. Source coding is performed by encoding U_1^n into an index pair (M_0, M_1) and U_2^n into an index pair (M_0, M_2) such that (U_1^n, U_2^n) can be losslessly recovered from the index triple (M_0, M_1, M_2) as depicted in Figure 14.4.

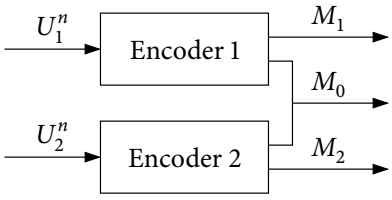


Figure 14.4. Source encoding setup for the 3-index separate source and channel coding scheme. The 2-DMS can be losslessly recovered from (M_0, M_1, M_2).

Since M_0 must be a function only of U_0^n, it can be easily shown that the optimal rate region $\mathscr{R}^*$ is the set of rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_1 &\geq H(U_1|U_2), \\ R_2 &\geq H(U_2|U_1), \\ R_1 + R_2 &\geq H(U_1, U_2|U_0), \\ R_0 + R_1 + R_2 &\geq H(U_1, U_2). \end{aligned} \tag{14.3}$$

At the same time, the capacity region $\mathscr{C}$ for a DM-MAC $p(y|x_1, x_2)$ with a common message (see Problem 5.19) is the set of rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_1 &\leq I(X_1; Y|X_2, W), \\ R_2 &\leq I(X_2; Y|X_1, W), \end{aligned}$$

$$R_1 + R_2 \le I(X_1, X_2; Y|W),$$
$$R_0 + R_1 + R_2 \le I(X_1, X_2; Y)$$

for some pmf $p(w)p(x_1|w)p(x_2|w)$, where $|\mathcal{W}| \le \min\{|\mathcal{X}_1|\cdot|\mathcal{X}_2| + 2, |\mathcal{Y}| + 3\}$. Hence, if the intersection of the interiors of $\mathscr{R}^*$ and $\mathscr{C}$ is not empty, separate source and channel coding using three indices can be used to communicate the 2-DMS losslessly over the DM-MAC. Note that this coding scheme is not optimal in general as already shown in Example 14.3.

14.1.5 A Joint Source–Channel Coding Scheme with Common Part

By generalizing the coding schemes in Sections 14.1.1 and 14.1.4, we obtain the following sufficient condition for lossless communication of a 2-DMS over a DM-MAC.

Theorem 14.2. A 2-DMS (U_1, U_2) with common part U_0 can be communicated losslessly over a DM-MAC $p(y|x_1, x_2)$ if

$$H(U_1|U_2) < I(X_1; Y|X_2, U_2, W),$$
$$H(U_2|U_1) < I(X_2; Y|X_1, U_1, W),$$
$$H(U_1, U_2|U_0) < I(X_1, X_2; Y|U_0, W),$$
$$H(U_1, U_2) < I(X_1, X_2; Y)$$

for some conditional pmf $p(w)p(x_1|u_1, w)p(x_2|u_2, w)$.

In this sufficient condition, the common part U_0 is represented by the independent auxiliary random variable W, which is chosen to maximize cooperation between the senders.

Remark 14.1. Although the auxiliary random variable W represents the common part U_0, there is no benefit in making it statistically correlated with U_0. This is a consequence of Shannon's source–channel separation theorem in Section 3.9.

Remark 14.2. The above sufficient condition does not change by introducing a time-sharing random variable Q.

Proof of Theorem 14.2 (outline). For each u_0^n, randomly and independently generate $w^n(u_0^n)$ according to $\prod_{i=1}^n p_W(w_i)$. For each (u_0^n, u_1^n), randomly and independently generate $x_1^n(u_0^n, u_1^n)$ according to $\prod_{i=1}^n p_{X_1|U_1,W}(x_{1i}|u_{1i}, w_i(u_0^n))$. Similarly, for (u_0^n, u_2^n), randomly and independently generate $x_2^n(u_0^n, u_2^n)$. The decoder declares $(\hat{u}_0^n, \hat{u}_1^n, \hat{u}_2^n)$ to be the estimate of the sources if it is the unique triple such that $(\hat{u}_0^n, \hat{u}_1^n, \hat{u}_2^n, w^n(\hat{u}_0^n), x_1^n(\hat{u}_0^n, \hat{u}_1^n), x_2^n(\hat{u}_0^n, \hat{u}_2^n), y^n) \in \mathcal{T}_\epsilon^{(n)}$ (this automatically implies that $\hat{u}_0^n$ is the common part of $\hat{u}_1^n$ and $\hat{u}_2^n$). Following the steps in the proof of the previous coding scheme, it can be shown that the above inequalities are sufficient for the probability of error to tend to zero as $n \to \infty$.

Remark 14.3. The above coding scheme is not optimal in general either.

14.2 LOSSLESS COMMUNICATION OF A 2-DMS OVER A DM-BC

Now consider the broadcast communication system depicted in Figure 14.5, where a 2-DMS (U_1, U_2) is to be communicated losslessly over a 2-receiver DM-BC $p(y_1, y_2|x)$. The definitions of a code, probability of error, and lossless communication for this setup are along the same lines as those for the MAC case. As before, assume rates $r_1 = r_2 = 1$ symbol/transmission.

Since the private-message capacity region of the DM-BC is not known in general (see Chapter 8), the necessary and sufficient condition for lossless communication of a 2-DMS over a DM-BC is not known even when the sources are independent. We will show nevertheless that separation does not hold in general for sending a 2-DMS over a DM-BC.

Consider the following separate source and channel coding scheme for this setup. The encoder first assigns an index triple $(M_0, M_1, M_2) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$ to the source sequence pair (U_1^n, U_2^n) such that U_1^n can be recovered losslessly from the pair of indices (M_0, M_1) and U_2^n can be recovered losslessly from the pair of indices (M_0, M_2). The encoder then transmits a codeword $x^n(M_0, M_1, M_2)$ from a channel codebook. Decoder 1 first decodes for (M_0, M_1) and then recovers U_1^n. Similarly decoder 2 first decodes for (M_0, M_2) and then recovers U_2^n. The source coding part of this scheme is discussed in the following subsection.

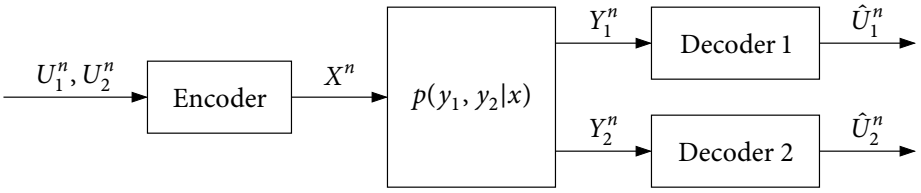


Figure 14.5. Communication of a 2-DMS over a 2-receiver DM-BC.

14.2.1 Gray–Wyner System

The Gray–Wyner system depicted in Figure 14.6 is a distributed lossless source coding setup in which a 2-DMS (U_1, U_2) is described by three encoders so that decoder 1, who receives the descriptions M_0 and M_1, can losslessly recover U_1^n and decoder 2, who receives the descriptions M_0 and M_2, can losslessly recover U_2^n. We wish to find the optimal rate region for this distributed lossless source coding setup.

A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ code for the Gray–Wyner system consists of

- three encoders, where encoder $j = 0, 1, 2$ assigns the index $m_j(u_1^n, u_2^n) \in [1 : 2^{nR_j})$ to each sequence pair $(u_1^n, u_2^n) \in \mathcal{U}_1^n \times \mathcal{U}_2^n$, and
- two decoders, where decoder 1 assigns an estimate $\hat{u}_1^n(m_0, m_1)$ to each index pair

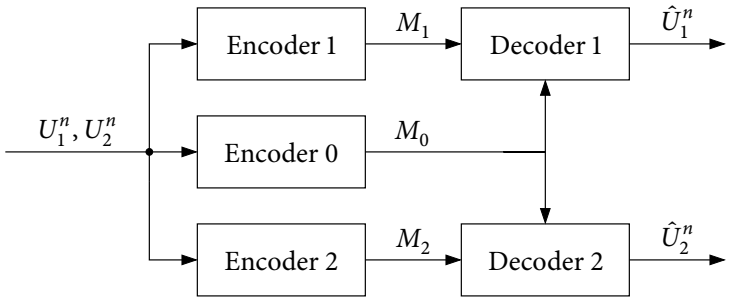


Figure 14.6. Gray–Wyner system.

$(m_0, m_1) \in [1 : 2^{nR_0}) \times [1 : 2^{nR_1})$ and decoder 2 assigns an estimate $\hat{u}_2^n(m_0, m_2)$ to each index pair $(m_0, m_2) \in [1 : 2^{nR_0}) \times [1 : 2^{nR_2})$.

The probability of error is defined as $P_e^{(n)} = \mathsf{P}\{(\hat{U}_1^n, \hat{U}_2^n) \neq (U_1^n, U_2^n)\}$. A rate triple (R_0, R_1, R_2) is said to be achievable if there exists a sequence of $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ codes such that $\lim_{n\to\infty} P_e^{(n)} = 0$. The optimal rate region $\mathscr{R}^*$ for the Gray–Wyner system is the closure of the set of achievable rate triples.

The optimal rate region for the Gray–Wyner system is given in the following.

Theorem 14.3. The optimal rate region $\mathscr{R}^*$ for the Gray–Wyner system with 2-DMS (U_1, U_2) is the set of rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_0 &\geq I(U_1, U_2; V), \\ R_1 &\geq H(U_1|V), \\ R_2 &\geq H(U_2|V) \end{aligned}$$

for some conditional pmf $p(v|u_1, u_2)$ with $|\mathcal{V}| \leq |\mathcal{U}_1|\cdot|\mathcal{U}_2| + 2$.

The optimal rate region has the following extreme points:

- $R_0 = 0$: By taking $V = \emptyset$, the region reduces to $R_1 \geq H(U_1)$ and $R_2 \geq H(U_2)$.
- $R_1 = 0$: By taking $V = U_1$, the region reduces to $R_0 \geq H(U_1)$ and $R_2 \geq H(U_2|U_1)$.
- $R_2 = 0$: By taking $V = U_2$, the region reduces to $R_0 \geq H(U_2)$ and $R_1 \geq H(U_1|U_2)$.
- $(R_1, R_2) = (0, 0)$: By taking $V = (U_1, U_2)$, the region reduces to $R_0 \geq H(U_1, U_2)$.

Proof of Theorem 14.3. To prove achievability, we use joint typicality encoding to find a $v^n(m_0)$, $m_0 \in [1 : 2^{nR_0}]$, jointly typical with (u_1^n, u_2^n). The index m_0 is sent to both decoders. Given $v^n(m_0)$, we assign indices $m_1 \in [1 : 2^{nR_1}]$ and $m_2 \in [1 : 2^{nR_2}]$ to the sequences in $\mathcal{T}_\epsilon^{(n)}(U_1|v^n(m_0))$ and $\mathcal{T}_\epsilon^{(n)}(U_2|v^n(m_0))$, respectively, and send them to decoders 1 and 2, respectively. For the proof of the converse, we use standard arguments with the auxiliary

random variable identification $V_i = (M_0, U_1^{i-1}, U_2^{i-1})$. The cardinality bound on $\mathcal{V}$ can be proved using the convex cover method in Appendix C.

14.2.2 Common Information

A rate triple (R_0, R_1, R_2) in the optimal rate region for the Gray–Wyner system must satisfy the inequalities

$$\begin{aligned} R_0 + R_1 &\geq H(U_1), \\ R_0 + R_2 &\geq H(U_2), \\ R_0 + R_1 + R_2 &\geq H(U_1, U_2), \\ 2R_0 + R_1 + R_2 &\geq H(U_1) + H(U_2). \end{aligned}$$

Each of these inequalities is tight as seen from the extreme points above. Interestingly, the corresponding common rate R_0 on these extreme points of $\mathscr{R}^*$ leads to several notions of *common information*.

- **Gács–Körner–Witsenhausen common information.** The maximum common rate R_0 subject to $R_0 + R_1 = H(U_1)$ and $R_0 + R_2 = H(U_2)$ is the entropy $H(U_0)$ of the common part between U_1 and U_2 (as defined in Section 14.1.3), denoted by $K(U_1; U_2)$.
- **Mutual information.** The maximum common rate R_0 subject to $2R_0 + R_1 + R_2 = H(U_1) + H(U_2)$ is the mutual information $I(U_1; U_2)$.
- **Wyner's common information.** The minimum common rate R_0 subject to $R_0 + R_1 + R_2 = H(U_1, U_2)$ is

$$J(U_1; U_2) = \min I(U_1, U_2; V), \tag{14.4}$$

  where the minimum is over all conditional pmfs $p(v|u_1, u_2)$ with $|\mathcal{V}| \leq |\mathcal{U}_1| \cdot |\mathcal{U}_2|$ such that $I(U_1; U_2|V) = 0$, i.e., $U_1 \to V \to U_2$. Recall that this Markov structure appeared in the converse proofs for the quadratic Gaussian distributed source coding and multiple description coding problems in Sections 12.3 and 13.4, respectively.

The above three quantities represent common information between the random variables U_1 and U_2 in different contexts. The Gács–Körner–Witsenhausen common information $K(X; Y)$ captures the amount of common randomness that can be extracted by knowing U_1 and U_2 separately. In comparison, Wyner's common information captures the amount of common randomness that is needed to generate U_1 and U_2 separately. Mutual information, as we have seen in the Slepian–Wolf theorem, captures the amount of information about U_1 provided by observing U_2 and vice versa.

In general, it can be easily shown that

$$0 \leq K(U_1; U_2) \leq I(U_1; U_2) \leq J(U_1; U_2) \leq H(U_1, U_2), \tag{14.5}$$

and these inequalities can be strict. Furthermore, $K(U_1; U_2) = I(U_1; U_2) = J(U_1; U_2)$ iff $U_1 = (V, V_1)$ and $U_2 = (V, V_2)$ for some pmf $p(v_1)p(v|v_1)p(v_2|v)$.

Example 14.5. Let (U_1, U_2) be a DSBS(p), $p \in [0, 1/2]$. Then it can be easily shown that $J(U_1; U_2) = 1 + H(p) - 2H(\alpha)$, where $\alpha \star \alpha = p$. The minimum in (14.4) is attained by setting $V \sim \text{Bern}(1/2)$, $V_1 \sim \text{Bern}(\alpha)$, and $V_2 \sim \text{Bern}(\alpha)$ to be mutually independent and $U_j = V \oplus V_j$, $j = 1, 2$.

Example 14.6. Let (U_1, U_2) be binary with $p(0, 0) = p(0, 1) = p(1, 1) = 1/3$. Then it can be shown that $J(U_1; U_2) = 2/3$, which is attained by setting $V \sim \text{Bern}(1/2)$, and $U_1 = 0$, $U_2 \sim \text{Bern}(2/3)$ if $V = 0$, and $U_1 \sim \text{Bern}(1/3)$, $U_2 = 1$ if $V = 1$.

14.2.3 A Separate Source–Channel Coding Scheme

We return to the discussion on sending a 2-DMS over a DM-BC using separate source and channel coding. Recall that Marton's inner bound in Section 8.4 is the best-known inner bound on the capacity region of the DM-BC. Denote this inner bound as $\mathscr{R} \subseteq \mathscr{C}$. Then, a 2-DMS can be communicated losslessly over a DM-BC if the intersection of the interiors of Marton's inner bound $\mathscr{R}$ and the optimal rate region $\mathscr{R}^*$ for the Gray–Wyner system is not empty, that is, if

$$\begin{aligned}
I(U_1, U_2; V) + H(U_1|V) &< I(W_0, W_1; Y_1),\\
I(U_1, U_2; V) + H(U_2|V) &< I(W_0, W_2; Y_2),\\
I(U_1, U_2; V) + H(U_1|V) + H(U_2|V) &< I(W_0, W_1; Y_1) + I(W_2; Y_2|W_0) - I(W_1; W_2|W_0),\\
I(U_1, U_2; V) + H(U_1|V) + H(U_2|V) &< I(W_1; Y_1|W_0) + I(W_0, W_2; Y_2) - I(W_1; W_2|W_0),\\
2I(U_1, U_2; V) + H(U_1|V) + H(U_2|V) &< I(W_0, W_1; Y_1) + I(W_0, W_2; Y_2) - I(W_1; W_2|W_0)
\end{aligned} \tag{14.6}$$

for some pmfs $p(v|u_1, u_2)$ and $p(w_0, w_1, w_2)$, and function $x(w_0, w_1, x_2)$. This separate source–channel coding scheme is optimal for some classes of sources and channels.

- More capable BC: Suppose that Y_1 is more capable than Y_2, i.e., $I(X; Y_1) \geq I(X; Y_2)$ for all $p(x)$. Then the 2-DMS (U_1, U_2) can be communicated losslessly if

$$\begin{aligned}
H(U_1, U_2) &< I(X; Y_1),\\
H(U_1, U_2) &< I(X; Y_1|W) + I(W; Y_2),\\
H(U_2) &< I(W; Y_2)
\end{aligned}$$

  for some pmf $p(w, x)$.

- Nested sources: Suppose that $U_1 = (V_1, V_2)$ and $U_2 = V_2$ for some $(V_1, V_2) \sim p(v_1, v_2)$. Then the 2-DMS (U_1, U_2) can be communicated losslessly if

$$\begin{aligned}
H(V_1, V_2) = H(U_1) &< I(X; Y_1),\\
H(V_1, V_2) = H(U_1) &< I(X; Y_1|W) + I(W; Y_2),\\
H(V_2) = H(U_2) &< I(W; Y_2)
\end{aligned}$$

  for some pmf $p(w, x)$.

In both cases, achievability follows by representing (U_1^n, U_2^n) by a message pair (M_1, M_2) at rates $R_2 = H(U_2)$ and $R_1 = H(U_1|U_2)$, respectively, and using superposition coding. The converse proofs are essentially the same as the converse proofs for the more capable BC and degraded message sets BC, respectively.

Source–channel separation is not optimal in general, however, as demonstrated in the following.

Example 14.7. Consider the 2-DMS (U_1, U_2) with $\mathcal{U}_1 = \mathcal{U}_2 = \{0, 1\}$ and $p_{U_1,U_2}(0, 0) = p_{U_1,U_2}(0, 1) = p_{U_1,U_2}(1, 1) = 1/3$ and the Blackwell channel in Example 8.2 defined by $\mathcal{X} = \{0, 1, 2\}$, $\mathcal{Y}_1 = \mathcal{Y}_2 = \{0, 1\}$, and $p_{Y_1,Y_2|X}(0, 0|0) = p_{Y_1,Y_2|X}(0, 1|1) = p_{Y_1,Y_2|X}(1, 1|2) = 1$. The capacity region of this channel is contained in the set of rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_0 + R_1 &\le 1, \\ R_0 + R_2 &\le 1, \\ R_0 + R_1 + R_2 &\le \log 3. \end{aligned}$$

However, as we found in Example 14.6, the sources require $R_0 \ge J(U_1; U_2) = 2/3$ when $R_0 + R_1 + R_2 = \log 3$, or equivalently, $2R_0 + R_1 + R_2 \ge \log 3 + 2/3 = 2.252$, which implies that $R_0 + R_1 \ge 1.126$ or $R_0 + R_2 \ge 1.126$.

Hence, the intersection of the optimal rate region $\mathscr{R}^*$ for the Gray–Wyner system and the capacity region $\mathscr{C}$ is empty and this 2-DMS cannot be communicated losslessly over the Blackwell channel using separate source and channel coding.

By contrast, setting $X = U_1 + U_2$ achieves error-free transmission since Y_1 and Y_2 uniquely determine U_1 and U_2, respectively. Thus joint source–channel coding can strictly outperform separate source and channel coding for sending a 2-DMS over a DM-BC.

14.2.4 A Joint Source–Channel Coding Scheme

We describe a general joint source–channel coding scheme that improves upon separate Gray–Wyner source coding and Marton's channel coding.

Theorem 14.4. A 2-DMS (U_1, U_2) can be communicated losslessly over a DM-BC $p(y_1, y_2|x)$ if

$$\begin{aligned} H(U_1|U_2) &< I(U_1, W_0, W_1; Y_1) - I(U_1, W_0, W_1; U_2), \\ H(U_2|U_1) &< I(U_2, W_0, W_2; Y_2) - I(U_2, W_0, W_2; U_1), \\ H(U_1, U_2) &< I(U_1, W_0, W_1; Y_1) + I(U_2, W_2; Y_2|W_0) - I(U_1, W_1; U_2, W_2|W_0), \\ H(U_1, U_2) &< I(U_1, W_1; Y_1|W_0) + I(U_2, W_0, W_2; Y_2) - I(U_1, W_1; U_2, W_2|W_0), \\ H(U_1, U_2) &< I(U_1, W_0, W_1; Y_1) + I(U_2, W_0, W_2; Y_2) - I(U_1, W_1; U_2, W_2|W_0) \\ &\quad - I(U_1, U_2; W_0) \end{aligned}$$

for some conditional pmf $p(w_0, w_1, w_2|u_1, u_2)$ and function $x(u_1, u_2, w_0, w_1, w_2)$.

This theorem recovers the following as special cases:

- Separate source and channel coding: We set $p(w_0, w_1, w_2|u_0, u_1) = p(w_0, w_1, w_2)$ and $x(u_1, u_2, w_0, w_1, w_2) = x(w_0, w_1, w_2)$, i.e., (W_0, W_1, W_2, X) is independent of (U_1, U_2). Then, the set of inequalities in the theorem simplifies to (14.6).
- Example 14.7: Set $W_0 = \emptyset$, $W_1 = U_1$, $W_2 = U_2$, $X = U_1 + U_2$.

Remark 14.4. The sufficient condition in Theorem 14.4 does not improve by time sharing.

14.2.5 Proof of Theorem 14.4

Codebook generation. Fix a conditional pmf $p(w_0, w_1, w_2|u_1, u_2)$ and function $x(u_1, u_2, w_0, w_1, w_2)$. Randomly and independently generate 2^{nR_0} sequences $w_0^n(m_0)$, $m_0 \in [1 : 2^{nR_0}]$, each according to $\prod_{i=1}^n p_{W_0}(w_{0i})$. For each $u_1^n \in \mathcal{U}_1^n$ and $m_0 \in [1 : 2^{nR_0}]$, randomly and independently generate 2^{nR_1} sequences $w_1^n(u_1^n, m_0, m_1)$, $m_1 \in [1 : 2^{nR_1}]$, each according to $\prod_{i=1}^n p_{W_1|U_1,W_0}(w_{1i}|u_{1i}, w_{0i}(m_0))$. Similarly, for each $u_2^n \in \mathcal{U}_2^n$ and $m_0 \in [1 : 2^{nR_0}]$, randomly and independently generate 2^{nR_2} sequences $w_2^n(u_2^n, m_0, m_2)$, $m_2 \in [1 : 2^{nR_2}]$, each according to $\prod_{i=1}^n p_{W_2|U_2,W_0}(w_{2i}|u_{2i}, w_{0i}(m_0))$.

Encoding. For each sequence pair (u_1^n, u_2^n), choose a triple $(m_0, m_1, m_2) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$ such that $(u_1^n, u_2^n, w_0^n(m_0), w_1^n(u_1^n, m_0, m_1), w_2^n(u_2^n, m_0, m_2)) \in \mathcal{T}_{\epsilon'}^{(n)}$. If there is no such triple, choose $(m_0, m_1, m_2) = (1, 1, 1)$. Then the encoder transmits $x_i = x(u_{1i}, u_{2i}, w_{0i}(m_0), w_{1i}(u_1^n, m_0, m_1), w_{2i}(u_2^n, m_0, m_2))$ for $i \in [1 : n]$.

Decoding. Let $\epsilon > \epsilon'$. Decoder 1 declares $\hat{u}_1^n$ to be the estimate of u_1^n if it is the unique sequence such that $(\hat{u}_1^n, w_0^n(m_0), w_1^n(\hat{u}_1^n, m_0, m_1), y_1^n) \in \mathcal{T}_\epsilon^{(n)}$ for some $(m_0, m_1) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}]$. Similarly, decoder 2 declares $\hat{u}_2^n$ to be the estimate of u_2^n if it is the unique sequence such that $(\hat{u}_2^n, w_0^n(m_0), w_2^n(\hat{u}_2^n, m_0, m_2), y_2^n) \in \mathcal{T}_\epsilon^{(n)}$ for some $(m_0, m_2) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_2}]$.

Analysis of the probability of error. Assume (M_0, M_1, M_2) is selected at the encoder. Then decoder 1 makes an error only if one or more of the following events occur:

$$\begin{aligned}
\mathcal{E}_0 &= \{(U_1^n, U_2^n, W_0^n(m_0), W_1^n(U_1^n, m_0, m_1), W_2^n(U_2^n, m_0, m_2)) \notin \mathcal{T}_{\epsilon'}^{(n)} \\
&\qquad \text{for all } m_0, m_1, m_2\}, \\
\mathcal{E}_{11} &= \{(U_1^n, W_0^n(M_0), W_1^n(U_1^n, M_0, M_1), Y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \\
\mathcal{E}_{12} &= \{(\tilde{u}_1^n, W_0^n(M_0), W_1^n(\tilde{u}_1^n, M_0, m_1), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{u}_1^n \neq U_1^n, m_1\}, \\
\mathcal{E}_{13} &= \{(\tilde{u}_1^n, W_0^n(m_0), W_1^n(\tilde{u}_1^n, m_0, m_1), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{u}_1^n \neq U_1^n, m_0 \neq M_0, m_1\}.
\end{aligned}$$

Thus the probability of error $\mathsf{P}(\mathcal{E}_1)$ for decoder 1 is upper bounded as

$$\mathsf{P}(\mathcal{E}_1) \le \mathsf{P}(\mathcal{E}_0) + \mathsf{P}(\mathcal{E}_0^c \cap \mathcal{E}_{11}) + \mathsf{P}(\mathcal{E}_{12}) + \mathsf{P}(\mathcal{E}_{13}).$$

The first term tends to zero by the following variant of the multivariate covering lemma in Section 8.6.

Lemma 14.1. The probability $\mathsf{P}(\mathcal{E}_0)$ tends to zero as $n \to \infty$ if

$$\begin{aligned} R_0 &> I(U_1, U_2; W_0) + \delta(\epsilon'), \\ R_0 + R_1 &> I(U_1, U_2; W_0) + I(U_2; W_1|U_1, W_0) + \delta(\epsilon'), \\ R_0 + R_2 &> I(U_1, U_2; W_0) + I(U_1; W_2|U_2, W_0) + \delta(\epsilon'), \\ R_0 + R_1 + R_2 &> I(U_1, U_2; W_0) + I(U_2; W_1|U_1, W_0) + I(U_1, W_1; W_2|U_2, W_0) + \delta(\epsilon'). \end{aligned}$$

The proof of this lemma is given in Appendix 14A.

By the conditional typicality lemma, $\mathsf{P}(\mathcal{E}_0^c \cap \mathcal{E}_{11})$ tends to zero as $n \to \infty$. Following steps similar to the DM-MAC joint source–channel coding, it can be shown that $\mathsf{P}(\mathcal{E}_{12})$ tends to zero as $n \to \infty$ if $H(U_1) + R_1 < I(U_1, W_1; Y_1|W_0) + I(U_1; W_0) - \delta(\epsilon)$, and $\mathsf{P}(\mathcal{E}_{13})$ tends to zero as $n \to \infty$ if $H(U_1) + R_0 + R_1 < I(U_1, W_0, W_1; Y_1) + I(U_1; W_0) - \delta(\epsilon)$.

Similarly, the probability of error for decoder 2 tends to zero as $n \to \infty$ if $H(U_2) + R_2 < I(U_2, W_2; Y_2|W_0) + I(U_2; W_0) - \delta(\epsilon)$ and $H(U_2) + R_0 + R_2 < I(U_2, W_0, W_2; Y_2) + I(U_2; W_0) - \delta(\epsilon)$. The rest of the proof follows by combining the above inequalities and eliminating (R_0, R_1, R_2) by the Fourier–Motzkin procedure in Appendix D.

14.3 A GENERAL SINGLE-HOP NETWORK

We end our discussion of single-hop networks with a general network model that includes many of the setups we studied in previous chapters. Consider the 2-sender 2-receiver communication system with general source transmission demand depicted in Figure 14.7. Let (U_1, U_2) be a 2-DMS with common part U_0, $p(y_1, y_2|x_1, x_2)$ be a DM single-hop network, and $d_{11}(u_1, \hat{u}_{11})$, $d_{12}(u_1, \hat{u}_{12})$, $d_{21}(u_2, \hat{u}_{21})$, $d_{22}(u_2, \hat{u}_{22})$ be four distortion measures. For simplicity, assume transmission rates $r_1 = r_2 = 1$ symbol/transmission. Sender 1 observes the source sequence U_1^n and sender 2 observes the source sequence U_2^n. Receiver 1 wishes to reconstruct (U_1^n, U_2^n) with distortions (D_{11}, D_{21}) and receiver 2 wishes to reconstruct (U_1^n, U_2^n) with distortions (D_{12}, D_{22}). We wish to determine the necessary and sufficient condition for sending the sources within prescribed distortions.

This general network includes the following special cases we discussed earlier.

- Lossless communication of a 2-DMS over a DM-MAC: Assume that $Y_2 = \emptyset$, d_{11} and d_{21} are Hamming distortion measures, and $D_{11} = D_{21} = 0$. As we have seen, this setup

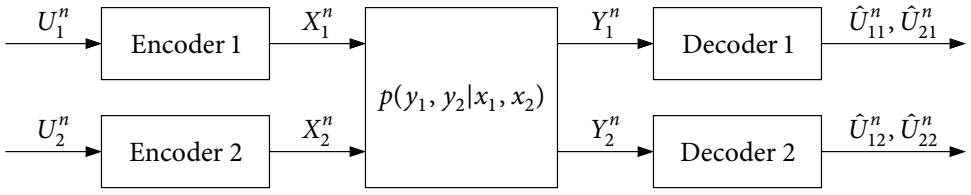


Figure 14.7. A general single-hop communication network.

in turn includes as special cases communication of independent and common messages over a DM-MAC in Problem 5.19 and distributed lossless source coding in Chapter 10.

- Lossy communication of a 2-DMS over a DM-MAC: Assume $Y_2 = \emptyset$ and relabel d_{11} as d_1 and d_{21} as d_2. This setup includes distributed lossy source coding discussed in Chapter 12 as a special case.
- Lossless communication of a 2-DMS over a DM-BC: Assume that $X_2 = U_2 = \emptyset$, $U_1 = (V_1, V_2)$, d_{11} and d_{21} are Hamming distortion measures on V_1 and V_2, respectively, and $D_{11} = D_{21} = 0$. As we have seen, this setup includes sending private and common messages over a DM-BC in Chapter 8 and the Gray–Wyner system in Section 14.2.1 as special cases.
- Lossy communication of a 2-DMS over a DM-BC: Assume that $X_2 = U_2 = \emptyset$, and relabel d_{11} as d_1 and d_{21} as d_2. This setup includes several special cases of the multiple-description coding problem in Chapter 13 such as successive refinement.
- Interference channel: Assume that U_1 and U_2 are independent, d_{11} and d_{22} are Hamming distortion measures, and $D_{11} = D_{22} = 0$. This yields the DM-IC in Chapter 6.

14.3.1 Separate Source and Channel Coding Scheme

We define separate source and channel coding for this general single-hop network as follows. A $(2^{nR_0}, 2^{nR_{10}}, 2^{nR_{11}}, 2^{nR_{20}}, 2^{nR_{22}}, n)$ source code consists of

- two source encoders, where source encoder 1 assigns an index triple $(m_0, m_{10}, m_{11}) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_{10}}] \times [1 : 2^{nR_{11}}]$ to every u_1^n and source encoder 2 assigns an index triple $(m_0, m_{20}, m_{22}) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_{20}}] \times [1 : 2^{nR_{22}}]$ to every u_2^n (here m_0 is a common index that is a function only of the common part u_0^n), and
- two source decoders, where source decoder 1 assigns an estimate $(\hat{u}_{11}^n, \hat{u}_{21}^n)$ to every index quadruple $(m_0, m_{10}, m_{11}, m_{20})$ and source decoder 2 assigns an estimate $(\hat{u}_{12}^n, \hat{u}_{22}^n)$ to every index quadruple $(m_0, m_{10}, m_{20}, m_{22})$.

Achievability and the rate–distortion region $\mathscr{R}(D_{11}, D_{12}, D_{21}, D_{22})$ are defined as for other lossy source coding problems. A $(2^{nR_0}, 2^{nR_{10}}, 2^{nR_{11}}, 2^{nR_{20}}, 2^{nR_{22}}, n)$ channel code consists of

- five message sets $[1 : 2^{nR_0}]$, $[1 : 2^{nR_{10}}]$, $[1 : 2^{nR_{11}}]$, $[1 : 2^{nR_{20}}]$, and $[1 : 2^{nR_{22}}]$,
- two channel encoders, where channel encoder 1 assigns a codeword $x_1^n(m_0, m_{10}, m_{11})$ to every message triple $(m_0, m_{10}, m_{11}) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_{10}}] \times [1 : 2^{nR_{11}}]$ and channel encoder 2 assigns a codeword $x_2^n(m_0, m_{20}, m_{22})$ to every message triple $(m_0, m_{20}, m_{22}) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_{20}}] \times [1 : 2^{nR_{22}}]$, and
- two channel decoders, where channel decoder 1 assigns an estimate $(\hat{m}_{01}, \hat{m}_{101}, \hat{m}_{11}, \hat{m}_{201})$ to every received sequence y_1^n and channel decoder 2 assigns an estimate $(\hat{m}_{02}, \hat{m}_{102}, \hat{m}_{202}, \hat{m}_{22})$ to every received sequence y_2^n.

The average probability of error, achievability, and the capacity region $\mathscr{C}$ are defined as for other channel coding settings.

The sources can be communicated over the channel with distortion quadruple $(D_{11}, D_{12}, D_{21}, D_{22})$ using separate source and channel coding if the intersection of the interiors of $\mathscr{R}(D_{11}, D_{12}, D_{21}, D_{22})$ and $\mathscr{C}$ is nonempty. As we have already seen, source–channel separation does not hold in general, that is, there are cases where this intersection is empty, yet the sources can be still communicated over the channel as specified.

14.3.2* A Hybrid Source–Channel Coding Scheme

In separate source and channel coding, channel codewords are conditionally independent of the source sequences given the descriptions (indices). Hence, the correlation between the sources is not utilized in channel coding. The hybrid source–channel coding scheme we discuss here captures this correlation in channel coding, while utilizing the wealth of known lossy source coding and channel coding schemes. Each sender first performs source encoding on its source sequences. It then maps the resulting codewords and the source sequence symbol-by-symbol into a channel input sequence and transmits it. Each receiver performs channel decoding for the codewords generated through source encoding and then maps the codeword estimates and the received sequence symbol-by-symbol into reconstructions of the desired source sequences.

For simplicity of presentation, we describe this scheme only for the special case of lossy communication of a 2-DMS over a DM-MAC.

Proposition 14.1. Let (U_1, U_2) be a 2-DMS and $d_1(u_1, \hat{u}_1)$, $d_2(u_2, \hat{u}_2)$ be two distortion measures. The 2-DMS (U_1, U_2) can be communicated over a DM-MAC $p(y|x_1, x_2)$ with distortion pair (D_1, D_2) if

$$\begin{aligned} I(U_1; V_1|Q) &< I(V_1; Y, V_2|Q), \\ I(U_2; V_2|Q) &< I(V_2; Y, V_1|Q), \\ I(U_1; V_1|Q) + I(U_2; V_2|Q) &< I(V_1, V_2; Y|Q) + I(V_1; V_2|Q) \end{aligned}$$

for some conditional pmf $p(q, v_1, v_2|u_1, u_2) = p(q)p(v_1|u_1, q)p(v_2|u_2, q)$ and functions $x_1(u_1, v_1, q)$, $x_2(u_2, v_2, q)$, $\hat{u}_1(v_1, v_2, y, q)$, and $\hat{u}_2(v_1, v_2, y, q)$ such that $\mathsf{E}(d_j(U_j, \hat{U}_j)) \le D_j$, $j = 1, 2$.

Proof outline. The coding scheme used to prove this proposition is depicted in Figure 14.8. For simplicity, let $Q = \emptyset$. Fix a conditional pmf $p(v_1|u_1)p(v_2|u_2)$ and functions $x_1(u_1, v_1)$, $x_2(u_2, v_2)$, $\hat{u}_1(v_1, v_2, y)$, and $\hat{u}_2(v_1, v_2, y)$. For $j = 1, 2$, randomly and independently generate 2^{nR_j} sequences $v_j^n(m_j)$, $m_j \in [1 : 2^{nR_j}]$, each according to $\prod_{i=1}^n p_{V_j}(v_{ji})$. Given u_j^n, encoder $j = 1, 2$ finds an index $m_j \in [1 : 2^{nR_j}]$ such that $(u_j^n, v_j^n(m_j)) \in \mathcal{T}_{\epsilon'}^{(n)}$. By the covering lemma, the probability of error for this joint typicality encoding step tends

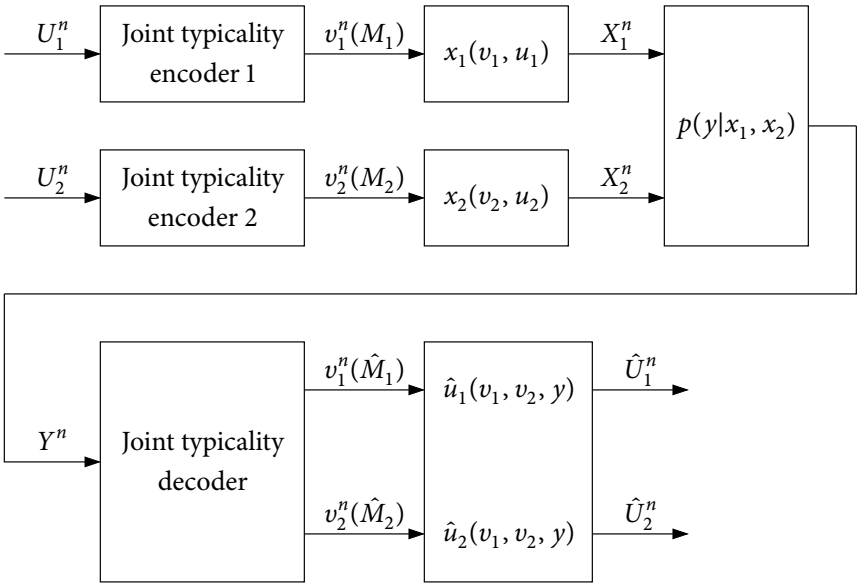


Figure 14.8. Hybrid source–channel coding for communicating a 2-DMS over a DM-MAC.

to zero as $n \to \infty$ if

$$R_1 > I(U_1; V_1) + \delta(\epsilon'),$$
$$R_2 > I(U_2; V_2) + \delta(\epsilon').$$

Encoder $j = 1, 2$ then transmits $x_{ji} = x_j(u_{ji}, v_{ji}(m_j))$ for $i \in [1 : n]$. Upon receiving y^n, the decoder finds the unique index pair $(\hat{m}_1, \hat{m}_2)$ such that $(v_1^n(\hat{m}_1), v_2^n(\hat{m}_2), y^n) \in \mathcal{T}_\epsilon^{(n)}$. It can be shown that the probability of error for this joint typicality decoding step tends to zero as $n \to \infty$ if

$$R_1 < I(V_1; Y, V_2) - \delta(\epsilon),$$
$$R_2 < I(V_2; Y, V_1) - \delta(\epsilon),$$
$$R_1 + R_2 < I(V_1, V_2; Y) + I(V_1; V_2) - \delta(\epsilon).$$

The decoder then sets the reconstruction sequences as $\hat{u}_{ji} = \hat{u}_j(v_{1i}(\hat{m}_1), v_{2i}(\hat{m}_2), y_i)$, $i \in [1 : n]$, for $j = 1, 2$. Eliminating R_1 and R_2 and following similar arguments to the achievability proof for distributed lossy source coding completes the proof.

Remark 14.5. By setting $V_j = (U_j, X_j)$ and $\hat{U}_j = U_j$, $j = 1, 2$, Proposition 14.1 reduces to Theorem 14.1.

Remark 14.6. Due to the dependence between the codebook $\{U_j^n(m_j) \colon m_j \in [1 : 2^{nR_j}]\}$ and the index M_j, $j = 1, 2$, the analysis of the probability error for joint typicality decoding requires nontrivial extensions of the packing lemma and the proof of achievability for the DM-MAC.

Remark 14.7. This hybrid coding scheme can be readily extended to the case of sources with a common part. It can be extended also to the general single-hop network depicted in Figure 14.7 by utilizing the source coding and channel coding schemes discussed in previous chapters.

SUMMARY

- Source–channel separation does not hold in general for communicating correlated sources over multiuser channels
- Joint source–channel coding schemes that utilize the correlation between the sources for cooperative transmission
- Common part of a 2-DMS
- Gray–Wyner system
- Notions of common information:
  - Gács–Körner–Witsenhausen common information $K(X; Y)$
  - Wyner's common information $J(X; Y)$
  - Mutual information $I(X; Y)$
  - $K(X; Y) \le I(X; Y) \le J(X; Y)$
- Joint Gray–Wyner–Marton coding for lossless communication of a 2-DMS over a DM-BC
- Hybrid source–channel coding scheme for a general single-hop network

BIBLIOGRAPHIC NOTES

The joint source–channel coding schemes for sending a 2-DMS over a DM-MAC in Theorems 14.1 and 14.2 are due to Cover, El Gamal, and Salehi (1980), who also showed via Example 14.3 that source–channel separation does not always hold. The definition of a common part of a 2-DMS and its characterization are due to Gács and Körner (1973) and Witsenhausen (1975). Dueck (1981a) showed via an example that the coding scheme used in the proof of Theorem 14.2, which utilizes the common part, is still suboptimal.

Theorem 14.3 is due to Gray and Wyner (1974), who also established the rate–distortion region for the lossy case. The definitions of common information and their properties can be found in Wyner (1975a). Examples 14.5 and 14.6 are due to Wyner (1975a) and Witsenhausen (1976a). Theorem 14.4 was established by Han and Costa (1987); see also Kramer and Nair (2009). The proof in Section 14.2.5 is due to Minero and Kim (2009). The hybrid source–channel coding scheme in Section 14.3.2 was proposed by Lim, Minero, and Kim (2010), who also established Proposition 14.1.

PROBLEMS

14.1. Establish the necessarily condition for lossless communication of an arbitrary 2-DMS (U_1, U_2) over a DM-MAC with orthogonal components $p(y_1|x_1)p(y_2|x_2)$ in Example 14.1.

14.2. Consider the 3-index lossless source coding setup in Section 14.1.4. Show that the optimal rate region is given by (14.3).

14.3. Provide the details of the proof of Theorem 14.2.

14.4. Consider the sufficient condition for lossless communication of a 2-DMS (U_1, U_2) over a DM-MAC $p(y|x_1, x_2)$ in Theorem 14.2. Show that the condition does not change by considering conditional pmfs $p(w|u_0)p(x_1|u_1, w)p(x_2|u_2, w)$. Hence, joint source–channel coding of the common part U_0^n via the codeword W^n does not help.

14.5. Provide the details of the proof of Theorem 14.3.

14.6. Show that the optimal rate region $\mathscr{R}^*$ of the Gray–Wyner system can be equivalently characterized by the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_0 + R_1 &\geq H(U_1), \\ R_0 + R_2 &\geq H(U_2), \\ R_0 + R_1 + R_2 &\geq H(U_1, U_2). \end{aligned}$$

14.7. *Separate source and channel coding over a DM-BC.* Consider the sufficient condition for lossless communication of a 2-DMS over a DM-BC via separate source and channel coding in (14.6).

(a) Show that, when specialized to a noiseless BC, the condition simplifies to the set of rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_0 + R_1 &\geq I(U_1, U_2; V) + H(U_1|V), \\ R_0 + R_2 &\geq I(U_1, U_2; V) + H(U_2|V), \\ R_0 + R_1 + R_2 &\geq I(U_1, U_2; V) + H(U_1|V) + H(U_2|V), \end{aligned}$$

for some conditional pmf $p(v|u_1, u_2)$.

(b) Show that the above region is equivalent to the optimal rate region for the Gray–Wyner system in Theorem 14.3.

14.8. *Common information.* Consider the optimal rate region $\mathscr{R}^*$ of the Gray–Wyner system in Theorem 14.3.

(a) Complete the derivations of the three measures of common information as extreme points of $\mathscr{R}^*$.

(b) Show that the three measures of common information satisfy the inequalities

$$0 \leq K(U_1; U_2) \leq I(U_1; U_2) \leq J(U_1; U_2) \leq H(U_1, U_2).$$

(c) Show that $K(U_1; U_2) = I(U_1; U_2) = J(U_1; U_2)$ iff $U_1 = (V, V_1)$ and $U_2 = (V, V_2)$ for some $(V, V_1, V_2) \sim p(v)p(v_1|v)p(v_2|v)$.

14.9. *Lossy Gray–Wyner system.* Consider the Gray–Wyner system in Section 14.2.1 for a 2-DMS (U_1, U_2) and two distortion measures d_1 and d_2. The sources are to be reconstructed with prescribed distortion pair (D_1, D_2). Show that the rate–distortion region $\mathscr{R}(D_1, D_2)$ is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_0 &\geq I(U_1, U_2; V), \\ R_1 &\geq I(U_1; \hat{U}_1|V), \\ R_2 &\geq I(U_2; \hat{U}_2|V) \end{aligned}$$

for some conditional pmf $p(v|u_1, u_2)p(\hat{u}_1|u_1, v)p(\hat{u}_2|u_2, v)$ that satisfy the constraints $\mathsf{E}(d_j(U_j, \hat{U}_j)) \leq D_j$, $j = 1, 2$.

14.10. *Nested sources over a DM-MAC.* Let (U_1, U_2) be a 2-DMS with common part $U_0 = U_2$. We wish to send this 2-DMS over a DM-MAC $p(y|x_1, x_2)$ at rates $r_1 = r_2 = r$ symbol/transmission. Show that source–channel separation holds for this setting. Remark: This problem was studied by De Bruyn, Prelov, and van der Meulen (1987).

14.11. *Nested sources over a DM-BC.* Consider the nested 2-DMS (U_1, U_2) in the previous problem. We wish to communicated this 2-DMS over a DM-BC $p(y_1, y_2|x)$ at rates $r_1 = r_2 = r$. Show that source–channel separation holds again for this setting.

14.12. *Lossy communication of a Gaussian source over a Gaussian BC.* Consider a Gaussian broadcast channel $Y_1 = X + Z_1$ and $Y_2 = X + Z_2$, where $Z_1 \sim \mathrm{N}(0, N_1)$ and $Z_2 \sim \mathrm{N}(0, N_2)$ are noise components with $N_2 > N_1$. Assume average power constraint P on X. We wish to communicate a WGN(P) source U with mean squared error distortions D_1 to Y_1 and D_2 to Y_2 at rate $r = 1$ symbol/transmission.

(a) Find the minimum achievable individual distortions D_1 and D_2 in terms of P, N_1, and N_2.

(b) Suppose we use separate source and channel coding by first using successive refinement coding for the quadratic Gaussian source in Example 13.3 and then using optimal Gaussian BC codes for independent messages. Characterize the set of achievable distortion pairs (D_1, D_2) using this scheme.

(c) Now suppose we send the source with no coding, i.e., set $X_i = U_i$ for $i \in [1 : n]$, and use the linear MMSE estimate $\hat{U}_{1i}$ at Y_1 and $\hat{U}_{2i}$ at Y_2. Characterize the set of achievable distortion pairs (D_1, D_2) using this scheme.

(d) Does source–channel separation hold for communicating a Gaussian source over a Gaussian BC with squared error distortion measure?

APPENDIX 14A PROOF OF LEMMA 14.1

The proof follows similar steps to the mutual covering lemma in Section 8.3. For each $(u_1^n, u_2^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2)$, define

$$\mathcal{A}(u_1^n, u_2^n) = \{(m_0, m_1, m_2) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}] \times [1 : 2^{nR_2}] : \\ (u_1^n, u_2^n, W_0^n(m_0), W_1^n(u_1^n, m_0, m_1), W_2^n(u_2^n, m_0, m_2)) \in \mathcal{T}_{\epsilon'}^{(n)}\}.$$

Then

$$\mathsf{P}(\mathcal{E}_0) \le \mathsf{P}\{(U_1^n, U_2^n) \notin \mathcal{T}_{\epsilon'}^{(n)}\} + \sum_{(u_1^n, u_2^n) \in \mathcal{T}_{\epsilon'}^{(n)}} p(u_1^n, u_2^n)\, \mathsf{P}\{|\mathcal{A}(u_1^n, u_2^n)| = 0\}.$$

By the LLN, the first term tends to zero as $n \to \infty$. To bound the second term, recall from the proof of the mutual covering lemma that

$$\mathsf{P}\{|\mathcal{A}(u_1^n, u_2^n)| = 0\} \le \frac{\mathrm{Var}(|\mathcal{A}(u_1^n, u_2^n)|)}{(\mathsf{E}(|\mathcal{A}(u_1^n, u_2^n)|))^2}.$$

Now, define the indicator function

$$E(m_0, m_1, m_2) = \begin{cases} 1 & \text{if } \big(u_1^n, u_2^n, W_0^n(m_0), W_1^n(u_1^n, m_0, m_1), W_2^n(u_2^n, m_0, m_2)\big) \in \mathcal{T}_{\epsilon'}^{(n)}, \\ 0 & \text{otherwise} \end{cases}$$

for each (m_0, m_1, m_2). We can then write

$$|\mathcal{A}(u_1^n, u_2^n)| = \sum_{m_0, m_1, m_2} E(m_0, m_1, m_2),$$

Let

$$\begin{aligned} p_1 &= \mathsf{E}[E(1,1,1)] \\ &= \mathsf{P}\big\{\big(u_1^n, u_2^n, W_0^n(m_0), W_1^n(u_1^n, m_0, m_1), W_2^n(u_2^n, m_0, m_2)\big) \in \mathcal{T}_{\epsilon'}^{(n)}\big\}, \\ p_2 &= \mathsf{E}[E(1,1,1)E(1,2,1)], \\ p_3 &= \mathsf{E}[E(1,1,1)E(1,1,2)], \\ p_4 &= \mathsf{E}[E(1,1,1)E(1,2,2)], \\ p_5 &= \mathsf{E}[E(1,1,1)E(2,1,1)] = \mathsf{E}[E(1,1,1)E(2,1,2)] \\ &= \mathsf{E}[E(1,1,1)E(2,2,1)] = \mathsf{E}[E(1,1,1)E(2,2,2)] = p_1^2. \end{aligned}$$

Then

$$\mathsf{E}(|\mathcal{A}(u_1^n, u_2^n)|) = \sum_{m_0, m_1, m_2} \mathsf{E}[E(m_0, m_1, m_2)] = 2^{n(R_0+R_1+R_2)} p_1$$

and

$$\begin{aligned}
\mathsf{E}(|\mathcal{A}(u_1^n, u_2^n)|^2) = &\sum_{m_0,m_1,m_2} \mathsf{E}[E(m_0, m_1, m_2)] \\
&+ \sum_{m_0,m_1,m_2} \sum_{m_1' \neq m_1} \mathsf{E}[E(m_0, m_1, m_2)E(m_0, m_1', m_2)] \\
&+ \sum_{m_0,m_1,m_2} \sum_{m_2' \neq m_2} \mathsf{E}[E(m_0, m_1, m_2)E(m_0, m_1, m_2')] \\
&+ \sum_{m_0,m_1,m_2} \sum_{m_1' \neq m_1, m_2' \neq m_2} \mathsf{E}[E(m_0, m_1, m_2)E(m_0, m_1', m_2')] \\
&+ \sum_{m_0,m_1,m_2} \sum_{m_0' \neq m_0, m_1', m_2'} \mathsf{E}[E(m_0, m_1, m_2)E(m_0', m_1', m_2')] \\
\le\ & 2^{n(R_0+R_1+R_2)} p_1 + 2^{n(R_0+2R_1+R_2)} p_2 + 2^{n(R_0+R_1+2R_2)} p_3 \\
&+ 2^{n(R_0+2R_1+2R_2)} p_4 + 2^{2n(R_0+R_1+R_2)} p_5.
\end{aligned}$$

Hence

$$\mathrm{Var}(|\mathcal{A}(u_1^n, u_2^n)|) \le 2^{n(R_0+R_1+R_2)} p_1 + 2^{n(R_0+2R_1+R_2)} p_2 + 2^{n(R_0+R_1+2R_2)} p_3 + 2^{n(R_0+2R_1+2R_2)} p_4.$$

Now by the joint typicality lemma, we have

$$\begin{aligned}
p_1 &\le 2^{-n(I(U_1,U_2;W_0)+I(U_2;W_1|U_1,W_0)+I(U_1,W_1;W_2|U_2,W_0)+\delta(\epsilon'))}, \\
p_2 &\le 2^{-n(I(U_1,U_2;W_0)+2I(U_2,W_2;W_1|U_1,W_0)+I(U_1;W_2|U_2,W_0)-\delta(\epsilon'))}, \\
p_3 &\le 2^{-n(I(U_1,U_2;W_0)+I(U_2;W_1|U_1,W_0)+2I(U_1,W_1,U_1;W_2|U_2,W_0)-\delta(\epsilon'))}, \\
p_4 &\le 2^{-n(I(U_1,U_2;W_0)+2I(U_2;W_1|U_1,W_0)+2I(U_1,W_1;W_2|U_2,W_0)-\delta(\epsilon'))}.
\end{aligned}$$

Hence

$$\begin{aligned}
\frac{\mathrm{Var}(|\mathcal{A}(u_1^n, u_2^n)|)}{(\mathsf{E}(|\mathcal{A}(u_1^n, u_2^n)|))^2} \le\ & 2^{-n(R_0+R_1+R_2-I(U_1,U_2;W_0)-I(U_2;W_1|U_1,W_0)-I(U_1,W_1;W_2|U_2,W_0)-\delta(\epsilon'))} \\
&+ 2^{-n(R_0+R_2-I(U_1,U_2;W_0)-I(U_1;W_2|U_2,W_0)-3\delta(\epsilon'))} \\
&+ 2^{-n(R_0+R_1-I(U_1,U_2;W_0)-I(U_2;W_1|U_1,W_0)-3\delta(\epsilon'))} \\
&+ 2^{-n(R_0-I(U_1,U_2;W_0)-3\delta(\epsilon'))}.
\end{aligned}$$

Therefore, $\mathsf{P}\{|\mathcal{A}(u_1^n, u_2^n)| = 0\}$ tends to zero as $n \to \infty$ if

$$\begin{aligned}
R_0 &> I(U_1, U_2; W_0) + 3\delta(\epsilon'), \\
R_0 + R_1 &> I(U_1, U_2; W_0) + I(U_2; W_1|U_1, W_0) + 3\delta(\epsilon'), \\
R_0 + R_2 &> I(U_1, U_2; W_0) + I(U_1; W_2|U_2, W_0) + 3\delta(\epsilon'), \\
R_0 + R_1 + R_2 &> I(U_1, U_2; W_0) + I(U_2; W_1|U_1, W_0) + I(U_1, W_1; W_2|U_2, W_0) + \delta(\epsilon').
\end{aligned}$$

This completes the proof of Lemma 14.1.

CHAPTER 19

Gaussian Networks

In this chapter, we discuss models for wireless multihop networks that generalize the Gaussian channel models we studied earlier. We extend the cutset bound and the noisy network coding inner bound on the capacity region of the multimessage DMN presented in Chapter 18 to Gaussian networks. We show through a Gaussian two-way relay channel example that noisy network coding can outperform decode–forward and amplify–forward, achieving rates within a constant gap of the cutset bound while the inner bounds achieved by these other schemes can have an arbitrarily large gap to the cutset bound. More generally, we show that noisy network coding for the Gaussian multimessage multicast network achieves rates within a constant gap of the capacity region independent of network topology and channel gains. For Gaussian networks with other messaging demands, e.g., general multiple-unicast networks, however, no such constant gap results exist in general. Can we still obtain some guarantees on the capacity of these networks?

To address this question, we introduce the scaling-law approach to capacity, where we seek to find the order of capacity scaling as the number of nodes in the network becomes large. In addition to providing some guarantees on network capacity, the study of capacity scaling sheds light on the role of cooperation through relaying in combating interference and path loss in large wireless networks. We first illustrate the scaling-law approach via a simple unicast network example that shows how relaying can dramatically increase the capacity by reducing the effect of high path loss. We then present the Gupta–Kumar random network model in which the nodes are randomly distributed over a geographical area and the goal is to determine the capacity scaling law that holds for most such networks. We establish lower and upper bounds on the capacity scaling law for the multiple-unicast case. The lower bound is achieved via a cellular time-division scheme in which the messages are sent simultaneously using a simple multihop scheme with nodes in cells along the lines from each source to its destination acting as relays. We show that this scheme achieves much higher rates than direct transmission with time division, which demonstrates the role of relaying in mitigating interference in large networks. This cellular time-division scheme also outperforms noncellular multihop through spatial reuse of time enabled by high path loss. Finally, we derive an upper bound on the capacity scaling law using the cutset bound and a network augmentation technique. This upper bound becomes tighter as the path loss exponent increases and has essentially the same order as the cellular time-division lower bound under the absorption path loss model.

19.1 GAUSSIAN MULTIMESSAGE NETWORK

Consider an N-node Gaussian network

$$Y_k = \sum_{j=1}^{N} g_{kj} X_j + Z_k, \quad k \in [1:N],$$

where g_{kj} is the gain from the transmitter of node j to the receiver of node k, and the noise components $Z_k \sim \mathrm{N}(0,1)$, $k \in [1:N]$ are i.i.d. $\mathrm{N}(0,1)$. We assume expected average power constraint P on each X_j, i.e., $\sum_{i=1}^{n} \mathsf{E}(x_{ji}^2(m_j, Y_j^{i-1})) \le nP$, $m_j \in [1:2^{nR_j}]$, $j \in [1:N]$. We consider a general multimessage demand where each node j wishes to send a message M_j to a set of destination nodes $\mathcal{D}_j$. The definitions of a code, probability of error, achievability, and capacity region follow those for the multimessage DMN in Section 18.4.

Consider the following special cases:

- If $X_N = \emptyset$ and $\mathcal{D}_j = \{N\}$ for $j \in [1:N-1]$, then the network reduces to the $(N-1)$-sender Gaussian MAC with *generalized* feedback.
- If $N = 2k$, $X_{k+1} = \cdots = X_N = Y_1 = \cdots = Y_k = \emptyset$, $\mathcal{D}_j = \{j+k\}$ for $j \in [1:k]$, then the network reduces to the k-user-pair Gaussian IC.
- If $N = 3$, $X_3 = Y_1 = \emptyset$, $\mathcal{D}_1 = \{3\}$, and $R_2 = 0$, then the network reduces to the Gaussian RC.

The Gaussian network can be equivalently written in a vector form

$$Y^N = GX^N + Z^N, \tag{19.1}$$

where X^N is the channel input vector, $G \in \mathbb{R}^{N \times N}$ is the channel gain matrix, and Z^N is a vector of i.i.d. $\mathrm{N}(0,1)$ noise components. Using this vector form, the cutset bound in Theorem 18.4 can be easily adapted to the Gaussian network model.

Theorem 19.1 (Cutset Bound for the Gaussian Multimessage Network). If a rate tuple $(R_1, \ldots, R_N)$ is achievable for the Gaussian multimessage network with destination sets $(\mathcal{D}_1, \ldots, \mathcal{D}_N)$, then it must satisfy the inequality

$$\sum_{j \in \mathcal{S}: \mathcal{D}_j \cap \mathcal{S}^c \neq \emptyset} R_j \le \frac{1}{2} \log |I + G(\mathcal{S}) K(\mathcal{S}|\mathcal{S}^c) G^T(\mathcal{S})|$$

for all $\mathcal{S}$ such that $\mathcal{S}^c \cap \mathcal{D}(\mathcal{S}) \neq \emptyset$ for some covariance matrix $K \succeq 0$ with $K_{jj} \le P$, $j \in [1:N]$. Here $\mathcal{D}(\mathcal{S}) = \bigcup_{j \in \mathcal{S}} \mathcal{D}_j$, $K(\mathcal{S}|\mathcal{S}^c)$ is the conditional covariance matrix of $X(\mathcal{S})$ given $X(\mathcal{S}^c)$ for $X^N \sim \mathrm{N}(0, K)$, and $G(\mathcal{S})$ is defined such that

$$\begin{bmatrix} Y(\mathcal{S}) \\ Y(\mathcal{S}^c) \end{bmatrix} = \begin{bmatrix} G'(\mathcal{S}) & G(\mathcal{S}^c) \\ G(\mathcal{S}) & G'(\mathcal{S}^c) \end{bmatrix} \begin{bmatrix} X(\mathcal{S}) \\ X(\mathcal{S}^c) \end{bmatrix} + \begin{bmatrix} Z(\mathcal{S}) \\ Z(\mathcal{S}^c) \end{bmatrix},$$

for some gain submatrices $G'(\mathcal{S})$ and $G'(\mathcal{S}^c)$.

When no cooperation between the nodes is possible, the cutset bound can be tightened as for the DMN by conditioning on a time-sharing random variable Q and considering $X^N|\{Q = q\} \sim \mathrm{N}(0, K(q))$, where $K(q)$ is diagonal and $\mathsf{E}_Q(K_{jj}(Q)) \le P$. This yields the improved bound with conditions

$$\sum_{j\in\mathcal{S}:\mathcal{D}_j\cap\mathcal{S}^c\neq\emptyset} R_j \le \frac{1}{2}\,\mathsf{E}_Q(\log|I + G(\mathcal{S})K(\mathcal{S}|Q)G^T(\mathcal{S})|)$$

for all $\mathcal{S}$ such that $\mathcal{S}^c \cap \mathcal{D}(\mathcal{S}) \neq \emptyset$, where $K(\mathcal{S}|Q)$ is the (random) covariance matrix of $X(\mathcal{S})$ given Q.

19.1.1 Noisy Network Coding Lower Bound

The inner bound on the capacity region of the DM multimessage multicast network in Theorem 18.5 can be also adapted to Gaussian networks. By adding the power constraints, we can readily obtain the noisy network coding inner bound that consists of all rate tuples $(R_1, \ldots, R_N)$ such that

$$\sum_{j\in\mathcal{S}} R_j < \min_{k\in\mathcal{S}^c\cap\mathcal{D}} I(X(\mathcal{S}); \hat{Y}(\mathcal{S}^c), Y_k|X(\mathcal{S}^c), Q) - I(Y(\mathcal{S}); \hat{Y}(\mathcal{S})|X^N, \hat{Y}(\mathcal{S}^c), Y_k, Q) \quad (19.2)$$

for all $\mathcal{S}$ satisfying $\mathcal{S}^c \cap \mathcal{D} \neq \emptyset$ for some conditional distribution $p(q)\prod_{j=1}^N F(x_j|q) \cdot F(\hat{y}_j|y_j, x_j, q)$ such that $\mathsf{E}(X_j^2) \le P$ for $j \in [1 : N]$. The optimizing conditional distribution of the inner bound in (19.2) is not known in general. To compare this noisy network coding inner bound to the cutset bound in Theorem 19.1 and to other inner bounds, we set $Q = \emptyset$, X_j, $j \in [1 : N]$, i.i.d. $\mathrm{N}(0, P)$, and

$$\hat{Y}_k = Y_k + \hat{Z}_k, \quad k \in [1 : N],$$

where $\hat{Z}_k \sim \mathrm{N}(0, 1)$, $k \in [1 : N]$, are independent of each other and of (X^N, Y^N). Substituting in (19.2), we have

$$\begin{aligned} I(Y(\mathcal{S}); \hat{Y}(\mathcal{S})|X^N, \hat{Y}(\mathcal{S}^c), Y_k) &\overset{(a)}{\le} I(\hat{Y}(\mathcal{S}); Y(\mathcal{S})|X^N) \\ &= h(\hat{Y}(\mathcal{S})|X^N) - h(\hat{Y}(\mathcal{S})|Y(\mathcal{S}), X^N) \\ &= \frac{|\mathcal{S}|}{2}\log(4\pi e) - \frac{|\mathcal{S}|}{2}\log(2\pi e) \\ &= \frac{|\mathcal{S}|}{2} \end{aligned}$$

for each $k \in \mathcal{D}$ and $\mathcal{S}$ such that $\mathcal{S}^c \cap \mathcal{D} \neq \emptyset$. Here step (a) follows since $(\hat{Y}(\mathcal{S}^c), Y_k) \to (X^N, Y(\mathcal{S})) \to \hat{Y}(\mathcal{S})$ form a Markov chain. Furthermore

$$\begin{aligned} I(X(\mathcal{S}); \hat{Y}(\mathcal{S}^c), Y_k|X(\mathcal{S}^c)) &\ge I(X(\mathcal{S}); \hat{Y}(\mathcal{S}^c)|X(\mathcal{S}^c)) \\ &= h(\hat{Y}(\mathcal{S}^c)|X(\mathcal{S}^c)) - h(\hat{Y}(\mathcal{S}^c)|X^N) \\ &= \frac{1}{2}\log\Big((2\pi e)^{|\mathcal{S}^c|}\,\big|2I + PG(\mathcal{S})G^T(\mathcal{S})\big|\Big) - \frac{|\mathcal{S}^c|}{2}\log(4\pi e) \\ &= \frac{1}{2}\log\Big|I + \frac{P}{2}G(\mathcal{S})G^T(\mathcal{S})\Big|. \end{aligned}$$

Hence, we obtain the inner bound characterized by the set of inequalities

$$\sum_{j\in\mathcal{S}} R_j < \frac{1}{2}\log\left|I + \frac{P}{2}G(\mathcal{S})G^T(\mathcal{S})\right| - \frac{|\mathcal{S}|}{2} \tag{19.3}$$

for all $\mathcal{S}$ with $\mathcal{S}^c \cap \mathcal{D} \neq \emptyset$.

Remark 19.1. As in the compress–forward lower bound for the Gaussian RC in Section 16.7, the choice of $\hat{Y}_k = Y_k + \hat{Z}_k$ with $\hat{Z}_k \sim \mathrm{N}(0, 1)$ can be improved upon by optimizing over the average powers of $\hat{Z}_k$, $k \in [1 : N]$, for the given channel gain matrix. The bound can be improved also by time sharing. It is not known, however, if Gaussian test channels are optimal.

In the following, we compare this noisy network coding inner bound to the cutset bound and other inner bounds on the capacity region.

19.1.2 Gaussian Two-Way Relay Channel

Consider the 3-node Gaussian two-way relay channel with no direct links depicted in Figure 19.1 with outputs

$$\begin{aligned} Y_1 &= g_{13}X_3 + Z_1,\\ Y_2 &= g_{23}X_3 + Z_2,\\ Y_3 &= g_{31}X_1 + g_{32}X_2 + Z_3, \end{aligned}$$

where the noise components Z_k, $k = 1, 2, 3$, are i.i.d. $\mathrm{N}(0, 1)$. We assume expected average power constraint P on each of X_1, X_2, and X_3. Denote the received SNR for the signal from node j to node k as $S_{kj} = g_{kj}^2 P$. Node 1 wishes to communicate a message M_1 to node 2 and node 2 wishes to communicate a message M_2 to node 1 with the help of relay node 3, i.e., $\mathcal{D} = \{1, 2\}$; see Problem 18.8 for a more general DM counterpart.

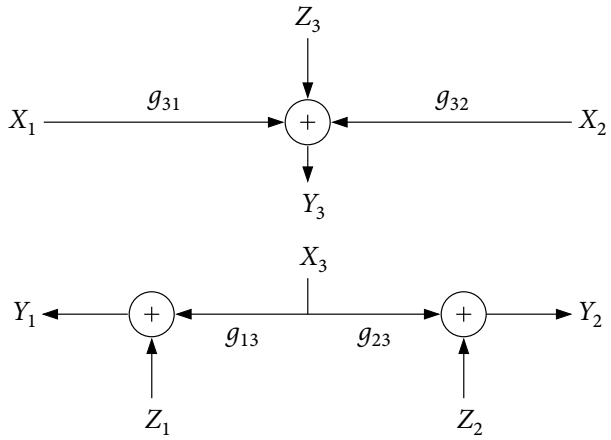


Figure 19.1. Gaussian two-way relay channel with no direct links.

The capacity region of this multimessage multicast network is not known in general. We compare the following outer and inner bounds on the capacity region.

Cutset bound. The cutset bound in Theorem 19.1 can be readily specialized to this Gaussian two-way channel. If a rate pair (R_1, R_2) is achievable, then it must satisfy the inequalities

$$\begin{aligned} R_1 &\le \min\{\mathsf{C}(S_{31}),\ \mathsf{C}(S_{23})\}, \\ R_2 &\le \min\{\mathsf{C}(S_{32}),\ \mathsf{C}(S_{13})\}. \end{aligned} \tag{19.4}$$

Decode–forward inner bound. The decode–forward coding scheme for the DM-RC in Section 16.4 can be extended to this two-way relay channel. Node 3 recovers both M_1 and M_2 over the multiple access channel $Y_3 = g_{31}X_1 + g_{32}X_2 + Z_3$ and broadcasts them. It can be easily shown that a rate pair (R_1, R_2) is achievable if

$$\begin{aligned} R_1 &< \min\{\mathsf{C}(S_{31}),\ \mathsf{C}(S_{23})\}, \\ R_2 &< \min\{\mathsf{C}(S_{32}),\ \mathsf{C}(S_{13})\}, \\ R_1 + R_2 &< \mathsf{C}(S_{31} + S_{32}). \end{aligned} \tag{19.5}$$

Amplify–forward inner bound. The amplify–forward relaying scheme for the RFD Gaussian RC in Section 16.8 can be easily extended to this setting by having node 3 send a scaled version of its received symbol. The corresponding inner bound consists of all rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< \mathsf{C}\left(\frac{S_{23}S_{31}}{1 + S_{23} + S_{31} + S_{32}}\right), \\ R_2 &< \mathsf{C}\left(\frac{S_{13}S_{32}}{1 + S_{13} + S_{31} + S_{32}}\right). \end{aligned} \tag{19.6}$$

Noisy network coding inner bound. By setting $Q = \emptyset$ and $\hat{Y}_3 = Y_3 + \hat{Z}_3$, where $\hat{Z}_3 \sim \mathrm{N}(0, \sigma^2)$ is independent of (X^3, Y^3), in (19.2), we obtain the inner bound that consists of all rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< \min\{\mathsf{C}(S_{31}/(1 + \sigma^2)), \mathsf{C}(S_{23}) - \mathsf{C}(1/\sigma^2)\}, \\ R_2 &< \min\{\mathsf{C}(S_{32}/(1 + \sigma^2)), \mathsf{C}(S_{13}) - \mathsf{C}(1/\sigma^2)\} \end{aligned} \tag{19.7}$$

for some $\sigma^2 > 0$.

Figure 19.2 compares the cutset bound to the decode–forward, amplify–forward, and noisy network coding bounds on the sum-capacity (with optimized parameters). The plots in the figure assume that nodes 1 and 2 are unit distance apart and node 3 is distance $r \in [0, 1]$ from node 1 along the line between nodes 1 and 2; the channel gains are of the form $g_{kj} = r_{kj}^{-3/2}$, where r_{kj} is the distance between nodes j and k, hence $g_{13} = g_{31} = r^{-3/2}$, $g_{23} = g_{32} = (1 - r)^{-3/2}$; and the power $P = 10$. Note that noisy network coding outperforms amplify–forward and decode–forward when the relay is sufficiently far from both destination nodes.

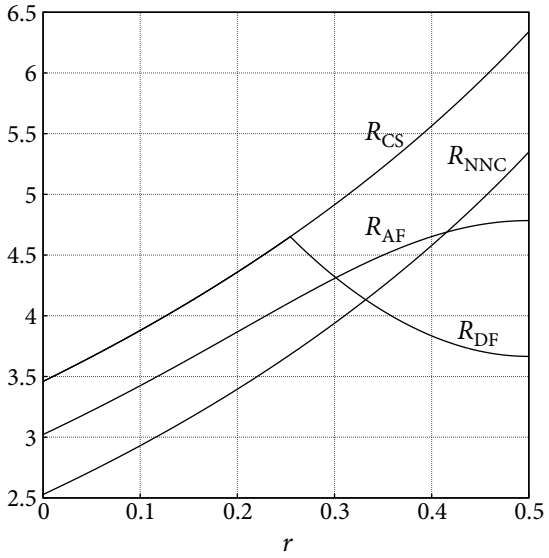


Figure 19.2. Comparison of the cutset bound R_{CS}, decode–forward lower bound R_{DF}, amplify–forward lower bound R_{AF}, and noisy network coding lower bound R_{NNC} on the sum-capacity of the Gaussian two-way relay channel as the function of the distance r between nodes 1 and 3.

In general, it can be shown that noisy network coding achieves the capacity region within 1/2 bit per dimension, while the other schemes have an *unbounded* gap to the cutset bound as $P \to \infty$ (see Problem 19.2).

Remark 19.2. Unlike the case of the RFD Gaussian relay channel studied in Section 16.8, noisy network coding does not always outperform amplify–forward. The reason is that both destination nodes are required to recover the compression index and hence its rate is limited by the worse channel. This limitation can be overcome by sending *layered* descriptions of Y_3^n such that the weaker receiver recovers the coarser description while the stronger receiver recovers both descriptions.

19.1.3 Multimessage Multicast Capacity Region within a Constant Gap

We show that noisy network coding achieves the capacity region of the Gaussian multimessage network $Y^N = GX^N + Z^N$ within a constant gap uniformly for any channel gain matrix G.

Theorem 19.2 (Constant Gap for Gaussian Multimessage Multicast Network). For the Gaussian multimessage multicast network, if a rate tuple $(R_1, \ldots, R_N)$ is in the cutset bound in Theorem 19.1, then the rate tuple $(R_1 - \Delta, \ldots, R_N - \Delta)$ is achievable, where $\Delta = (N/2) \log 6$.

Proof. Note that the cutset bound in Theorem 19.1 can be loosened as

$$\begin{aligned}
\sum_{j\in\mathcal{S}} R_j &\le \frac{1}{2}\log\left|I + G(\mathcal{S})K_{X(\mathcal{S})}G^T(\mathcal{S})\right| \\
&= \frac{1}{2}\log\left|I + K_{X(\mathcal{S})}G^T(\mathcal{S})G(\mathcal{S})\right| \\
&\le \frac{1}{2}\log\left|I + K_{X(\mathcal{S})}G^T(\mathcal{S})G(\mathcal{S}) + \frac{2}{P}K_{X(\mathcal{S})} + \frac{P}{2}G^T(\mathcal{S})G(\mathcal{S})\right| \\
&= \frac{1}{2}\log\left(\left|I + \frac{2}{P}K_{X(\mathcal{S})}\right|\left|I + \frac{P}{2}G^T(\mathcal{S})G(\mathcal{S})\right|\right) \\
&\overset{(a)}{\le} \frac{|\mathcal{S}|}{2}\log 3 + \frac{1}{2}\log\left|I + \frac{P}{2}G(\mathcal{S})G^T(\mathcal{S})\right| \\
&\le \frac{N}{2}\log 3 + \frac{1}{2}\log\left|I + \frac{P}{2}G(\mathcal{S})G^T(\mathcal{S})\right| \qquad (19.8)
\end{aligned}$$

for all $\mathcal{S}$ such that $\mathcal{D}\cap\mathcal{S}^c \neq \emptyset$, where $K_{X(\mathcal{S})}$ denotes the covariance matrix of $X(\mathcal{S})$ when $X^N \sim \mathrm{N}(0, K)$, and (a) follows by Hadamard's inequality. In the other direction, by loosening the inner bound in (19.3), a rate tuple $(R_1, \ldots, R_N)$ is achievable if

$$\sum_{j\in\mathcal{S}} R_j < \frac{1}{2}\log\left|I + \frac{P}{2}G(\mathcal{S})G^T(\mathcal{S})\right| - \frac{N}{2} \qquad (19.9)$$

for all $\mathcal{S}$ such that $\mathcal{D}\cap\mathcal{S}^c \neq \emptyset$. Comparing (19.8) and (19.9) completes the proof of Theorem 19.2.

19.2 CAPACITY SCALING LAWS

As we have seen, the capacity of Gaussian networks is known only in very few special cases. For the multimessage multicast case, we are able to show that the capacity region for any Gaussian network is within a constant gap of the cutset bound. No such constant gap results exist, however, for other multimessage demands. The scaling laws approach to capacity provides another means for obtaining guarantees on the capacity of a Gaussian network. It aims to establish the optimal scaling order of the capacity as the number of nodes grows.

In this section, we focus on Gaussian multiple-unicast networks in which each node in a source-node set $\mathcal{S}$ wishes to communicate a message to a distinct node in a disjoint destination-node set $\mathcal{D}$. The rest of the nodes as well as the source and destination nodes themselves can also act as relays. We define the *symmetric network capacity* $C(N)$ as the supremum of the set of symmetric rates R such that the rate tuple $(R, \ldots, R)$ is achievable. We seek to establish the scaling law for $C(N)$, that is, to find a function $g(N)$ such that $C(N) = \Theta(g(N))$; see Notation.

We illustrate this approach through the following simple example. Consider the N-node Gaussian unicast network depicted in Figure 19.3. Assume the power law path loss (channel gain) $g(r) = r^{-\nu/2}$, where r is the distance and $\nu > 2$ is the path loss exponent.

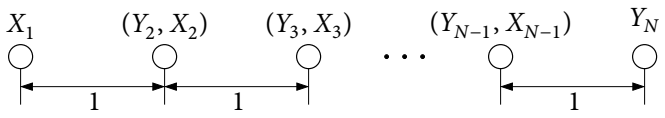


Figure 19.3. Gaussian unicast network.

Hence the received signal at node k is

$$Y_k = \sum_{j=1, j\neq k}^{N-1} |j-k|^{-\nu/2} X_j + Z_k, \quad k \in [2:N].$$

We assume expected average power constraint P on each X_j, $j \in [1:N-1]$.

Source node 1 wishes to communicate a message to destination node N with the other nodes acting as relays to help the communication; thus the source and relay encoders are specified by $x_1^n(m)$ and $x_{ji}(y_j^{i-1})$, $i \in [1:n]$, for $j \in [2:N-1]$. As we discussed in Chapter 16, the capacity of this network is not known for $N = 3$ for any nonzero channel parameter values. How does $C(N)$ scale with N? To answer this question consider the following bounds on $C(N)$.

Lower bounds. Consider a simple multihop relaying scheme, where signals are Gaussian and interference is treated as noise. In each transmission block, the source transmits a new message to the first relay and node $j \in [2:N-1]$ transmits its most recently received message to node $j+1$. Then $C(N) \geq \min_j \mathsf{C}(P/(I_j+1))$. Now the interference power at node $j \in [2:N]$ is $I_j = \sum_{k=1,k\neq j-1,j}^{N-1} |j-k|^{-\nu} P$. Since $\nu > 2$, $I_j = O(1)$ for all j. Hence $C(N) = \Omega(1)$.

Upper bound. Consider the cooperative broadcast upper bound on the capacity

$$\begin{aligned} C(N) &\leq \sup_{F(x^{N-1}):\mathsf{E}(X_j^2)\leq P, j\in[1:N-1]} I(X_1; Y_2, \ldots, Y_N | X_2, \ldots, X_{N-1}) \\ &\leq \frac{1}{2} \log |I + APA^T| \\ &= \frac{1}{2} \log |I + PA^T A|, \end{aligned}$$

where $A = \begin{bmatrix} 1 & 2^{-\nu/2} & 3^{-\nu/2} & \cdots & (N-1)^{-\nu/2} \end{bmatrix}^T$. Hence

$$C(N) \leq \mathsf{C}\left(\left(\sum_{j=1}^{N-1} \frac{1}{j^\nu} \right) P \right).$$

Since $\nu > 2$, $C(N) = O(1)$, which is the same scaling as achieved by the simple multihop scheme. Thus, we have shown that $C(N) = \Theta(1)$.

Remark 19.3. The maximum rate achievable by direct transmission from the source to the destination using the same total system power NP is $\mathsf{C}(PN(N-1)^{-\nu}) = \Theta(N^{1-\nu})$. Since $\nu > 2$, this rate tends to zero as $N \to \infty$.

This example shows that relaying can dramatically increase the communication rate when the path loss exponent ν is large. Relaying can also help mitigate the effect of interference as we see in the next section.

19.3 GUPTA–KUMAR RANDOM NETWORK

The Gupta–Kumar random network approach aims to establish capacity scaling laws that apply to *most* large ad-hoc wireless networks. The results can help our understanding of the role of cooperation in large networks, which in turn can guide network architecture design and coding scheme development.

We assume a "constant density" network with $2N$ nodes, each randomly and independently placed according to a uniform pdf over a square of area N as illustrated in Figure 19.4. The nodes are randomly partitioned into N source–destination (S-D) pairs. Label the source nodes as $1, 2, \ldots, N$ and the destination nodes as $N + 1, N + 2, \ldots, 2N$.

Once generated, the node locations and the S-D assignments are assumed to be fixed and known to the network architect (code designer). We allow each node, in addition to being either a source or a destination, to act as a relay to help other nodes communicate their messages.

We assume the Gaussian network model in (19.1) with power law path loss, that is, if the distance between nodes j and k is r_{jk}, then the channel gain $g_{jk} = r_{jk}^{-\nu/2}$ for $\nu > 2$. Hence, the output signal at each node $k \in [1 : 2N]$ is

$$Y_k = \sum_{j=1, j\neq k}^{2N} r_{kj}^{-\nu/2} X_j + Z_k.$$

We consider a multiple-unicast setting in which source node $j \in [1 : N]$ wishes to

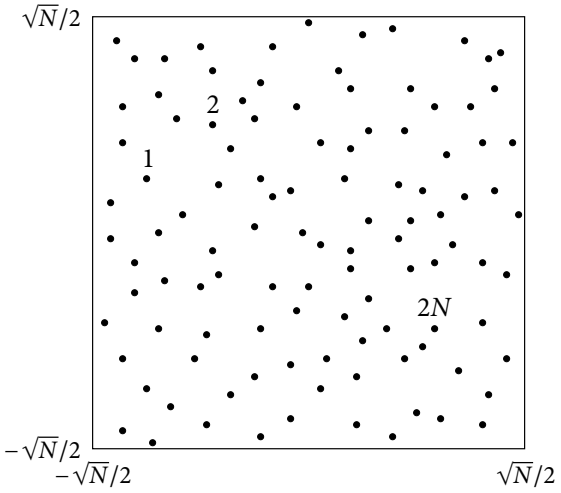


Figure 19.4. Gupta–Kumar random network.

communicate a message $M_j \in [1 : 2^{nR_j}]$ reliably to destination node $j + N$. The messages are assumed to be independent and uniformly distributed. We wish to determine the scaling law for the symmetric capacity $C(N)$ that holds *with high probability* (w.h.p.), that is, with probability $\geq (1 - \epsilon_N)$, where ϵ_N tends to zero as $N \to \infty$. In other words, the scaling law holds for most large networks generated in this random manner.

We establish the following bounds on the symmetric capacity.

Theorem 19.3. The symmetric capacity of the random network model with path loss exponent $\nu > 2$ has the following order bounds:

1. Lower bound: $C(N) = \Omega\big(N^{-1/2}(\log N)^{-(\nu+1)/2}\big)$ w.h.p.
2. Upper bound: $C(N) = O\big(N^{-1/2+1/\nu} \log N\big)$ w.h.p.

In other words, there exist constants $a_1, a_2 > 0$ such that

$$\lim_{N\to\infty} \mathsf{P}\{a_1 N^{-1/2}(\log N)^{-(\nu+1)/2} \leq C(N) \leq a_2 N^{-1/2+1/\nu} \log N\} = 1.$$

Before proving the upper and lower order bounds on the symmetric capacity scaling, consider the following simple transmission schemes.

Direct transmission. Suppose that there is only a single randomly chosen S-D pair. Then it can be readily checked that the S-D pair is $\Omega(N^{-1/2})$ apart w.h.p. and thus direct transmission achieves the rate $\Omega(N^{-\nu/2})$ w.h.p. Hence, for N S-D pairs, using time division with power control achieves the symmetric rate $\Omega(N^{-\nu/2})$ w.h.p.

Multihop relaying. Consider a single randomly chosen S-D pair. As we mentioned above, the S-D pair is $\Omega(N^{-1/2})$ apart. Furthermore, it can be shown that with high probability, there are roughly $\Omega((N/\log N)^{1/2})$ relays placed close to the straight line from the source to the destination with distance $O((\log N)^{1/2})$ between every two consecutive relays. Using the multihop scheme in Section 19.2 with these relays, we can show that $\Omega((\log N)^{-\nu/2})$ is achievable w.h.p. Hence, using time division and multihop relaying (without power control), we can achieve the lower bound on the symmetric capacity $C(N) = \Omega((\log N)^{-\nu/2}/N)$ w.h.p., which is a huge improvement over direct transmission when the path loss exponent $\nu > 2$ is large.

Remark 19.4. Using relaying, each node transmits at a much lower power than using direct transmission. This has the added benefit of reducing interference between the nodes, which can be exploited through *spatial reuse* of time/frequency to achieve higher rates.

19.3.1 Proof of the Lower Bound

To prove the lower bound in Theorem 19.3, consider the cellular time-division scheme illustrated in Figure 19.5 with cells of area $\log N$ (to guarantee that no cell is empty w.h.p.). As shown in the figure, the cells are divided into nine groups. We assume equal transmission rates for all S-D pairs. A block Markov transmission scheme is used, where each

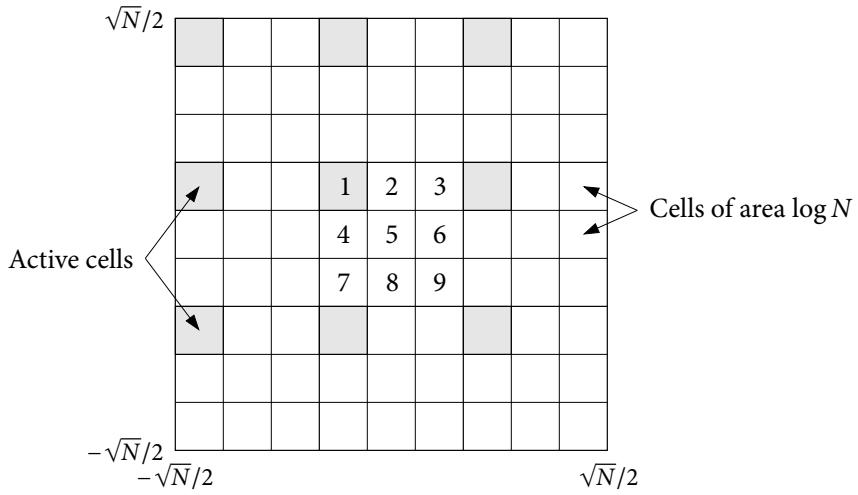


Figure 19.5. Cellular time-division scheme.

source node sends messages over several transmission blocks. Each transmission block is divided into nine *cell-blocks*. A cell is said to be *active* if its nodes are allowed to transmit. Each cell is active only during one out of the nine cell-blocks. Nodes in inactive cells act as receivers. As shown in Figure 19.6, each message is sent from its source node to the destination node using other nodes in cells along the straight line joining them (referred to as an *S-D line*) as relays.

Transmission from each node in an active cell to nodes in its four neighboring cells is performed using Gaussian random codes with power P and each receiver treats interference from other senders as noise. Let $S(N)$ be the maximum number of sources in a cell and $L(N)$ be the maximum number of S-D lines passing through a cell, over all cells.

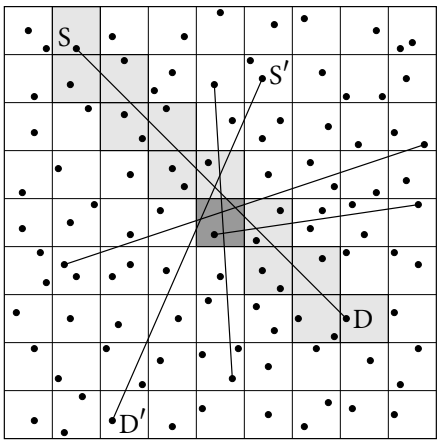


Figure 19.6. Messages transmitted via relays along S-D lines.

Each cell-block is divided into $S(N) + L(N)$ node-blocks for time-division transmission by nodes inside each active cell as illustrated in Figure 19.7. Each source node in an active cell broadcasts a *new* message during its node-block using a Gaussian random code with power P. One of the nodes in the active cell acts as a relay for the S-D pairs that communicate their messages through this cell. It relays the messages during the allotted $L(N)$ node-blocks using a Gaussian random code with power P.

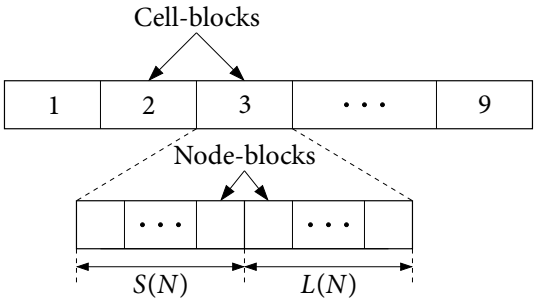


Figure 19.7. Time-division scheme.

Analysis of the probability of failure. The cellular time-division scheme fails if one or both of the following events occur:

$\mathcal{E}_1$ = {there is a cell with no nodes in it},

$\mathcal{E}_2$ = {transmission from a node in a cell to a node in a neighboring cell fails}.

Then the probability that the scheme fails is upper bounded as

$$\mathsf{P}(\mathcal{E}) \le \mathsf{P}(\mathcal{E}_1) + \mathsf{P}(\mathcal{E}_2 \cap \mathcal{E}_1^c).$$

It is straightforward to show that $\mathsf{P}(\mathcal{E}_1)$ tends to zero as $N \to \infty$. Consider the second term $\mathsf{P}(\mathcal{E}_2 \cap \mathcal{E}_1^c)$. From the cell geometry, the distance between each transmitting node in a cell and each receiving node in its neighboring cells is always less than or equal to $(5 \log N)^{1/2}$. Since each transmitting node uses power P, the received power at a node in a neighboring cell is always greater than or equal to $(5 \log N)^{-\nu/2} P$. Under worst-case placement of the sender, the receiver, and the interfering transmitters during a cell-block (see Figure 19.8), it can be shown that the total average interference power at a receiver from all other transmitting nodes is

$$I \le \sum_{j=1}^{\infty} \frac{2P}{\big((3j-2)^2 \log N\big)^{\nu/2}} + \sum_{j=1}^{\infty} \sum_{k=1}^{\infty} \frac{4P}{\big(((3j-2)^2 + (3k-1)^2) \log N\big)^{\nu/2}}. \tag{19.10}$$

Hence, if $\nu > 2$, $I \le a_3 (\log N)^{-\nu/2}$ for some constant $a_3 > 0$.

Since we are using Gaussian random codes, the probability of error tends to zero as the node-block length $n \to \infty$ if the transmission rate for each node block is less than

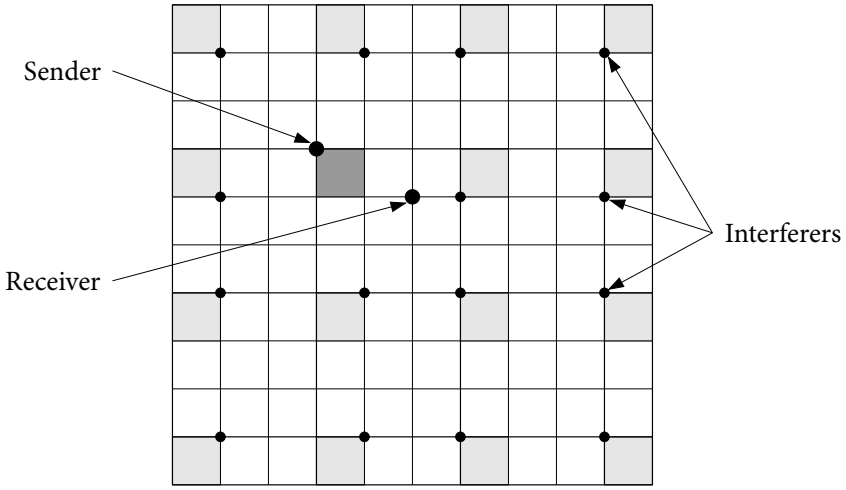


Figure 19.8. Placement of the active nodes assumed in the derivation of the bound on interference power.

$\mathsf{C}((5\log N)^{-\nu/2}P/(1+a_3(\log N)^{-\nu/2}))$. Thus, for a fixed network, $\mathsf{P}(\mathcal{E}_2 \cap \mathcal{E}_1^c)$ tends to zero as $n \to \infty$ if the symmetric rate

$$R(N) < \frac{1}{9(S(N)+L(N))}\,\mathsf{C}\left(\frac{(5\log N)^{-\nu/2}P}{1+a_3(\log N)^{-\nu/2}}\right). \tag{19.11}$$

In the following, we bound $S(N)+L(N)$ over a random network.

Lemma 19.1. $S(N)+L(N) = O\big((N\log N)^{1/2}\big)$ w.h.p.

The proof of this lemma is given in Appendix 19A. Combining Lemma 19.1 and the bound on $R(N)$ in (19.11), we have shown that $C(N) = \Omega(N^{-1/2}(\log N)^{-(\nu+1)/2})$ w.h.p., which completes the proof of the lower bound in Theorem 19.3.

Remark 19.5. The lower bound achieved by the cellular time-division scheme represents a vast improvement over time division with multihop, which, by comparison, achieves $C(N) = \Omega((\log N)^{-\nu/2}/N)$ w.h.p. This improvement is the result of spatial reuse of time (or frequency), which enables simultaneous transmission with relatively low interference due to the high path loss.

19.3.2 Proof of the Upper Bound

We prove the upper bound in Theorem 19.3, i.e., $C(N) = O(N^{-1/2+1/\nu}\log N)$ w.h.p. For a given random network, divide the square area of the network into two halves. Assume the case where there are at least $N/3$ sources on the left half and at least a third of them

transmit to destinations on the right half. Since the locations of sources and destinations are chosen independently, it can be easily shown that the probability of this event tends to one as $N \to \infty$. We relabel the nodes so that these sources are $1, \ldots, N'$ and the corresponding destinations are $N+1, \ldots, N+N'$.

By the cutset bound in Theorem 18.4, the symmetric capacity for these source nodes is upper bounded by

$$\max_{F(x^N)} \frac{1}{N'} I\big(X^{N'}; Y_{N+1}^{N+N'} \,\big|\, X_{N'+1}^{N}\big) \le \max_{F(x^{N'})} \frac{1}{N'} I\big(X^{N'}; \tilde{Y}_{N+1}^{N+N'}\big),$$

where $\tilde{Y}_k = \sum_{j=1}^{N'} g_{kj} X_j + Z_k$ for $k \in [N'+1 : 2N']$. Since the symmetric capacity of the original network is upper bounded by the symmetric capacity of these N' source–destination pairs, from this point on, we consider the subnetwork consisting only of these source–destination pairs and ignore the reception at the source nodes and the transmission at the destination nodes. To simplify the notation, we relabel N' as N and $\tilde{Y}_k$ as Y_k for $k \in [N+1 : 2N]$. Thus, each source node $j \in [1 : N]$ transmits X_j with the same average power constraint P and each destination node $k \in [N+1 : 2N]$ receives

$$Y_k = \sum_{j=1}^{N} g_{kj} X_j + Z_k.$$

We upper bound $(1/N) I(X^N; Y_{N+1}^{2N})$ for this $2N$-user interference channel.

Let node j (source or destination) be at random location (U_j, V_j). We create an *augmented network* by adding $2N$ mirror nodes as depicted in Figure 19.9. For every destination node Y_j, $j \in [N+1 : 2N]$, we add a sender node X_j at location $(-U_{N+j}, V_{N+j})$, and for every source node X_j, $j \in [1 : N]$, we add a receiver node Y_j at location $(-U_j, V_j)$.

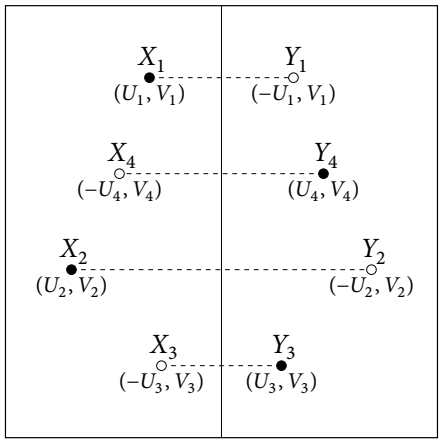


Figure 19.9. Augmented network.

The received vector of this augmented network is

$$Y^{2N} = GX^{2N} + Z^{2N},$$

where Z^{2N} is a vector of i.i.d. N(0, 1) noise components. The gain matrix G is symmetric and $G_{jj} = (2|U_j|)^{-\nu/2}$. Furthermore, it can be shown that $G \succeq 0$ (for $\nu > 0$).

Now consider

$$\begin{aligned}
NC(N) &\le \sup_{F(x^{2N}):\mathsf{E}|X_j^2|\le P, j\in[1:2N]} I(X^N; Y_{N+1}^{2N}) \\
&\le \sup_{F(x^{2N}):\mathsf{E}|X_j^2|\le P, j\in[1:2N]} I(X^{2N}; Y^{2N}) \\
&\le \max_{K_{\mathbf{X}}\succeq 0:\operatorname{tr}(K_{\mathbf{X}})\le 2NP} \frac{1}{2}\log|I + GK_{\mathbf{X}}G^T| \\
&= \max_{P_j:\sum_{j=1}^{2N} P_j \le 2NP} \frac{1}{2}\sum_{j=1}^{2N}\log(1 + P_j\lambda_j^2) \\
&\le \frac{1}{2}\sum_{j=1}^{2N}\log(1 + 2NP\lambda_j^2) \\
&\le \sum_{j=1}^{2N}\log(1 + (2NP)^{1/2}\lambda_j) \\
&= \log|I_{2N} + (2NP)^{1/2}G| \\
&\le \sum_{j=1}^{2N}\log(1 + (2NP)^{1/2}G_{jj}), \qquad (19.12)
\end{aligned}$$

where P_j and λ_j, $j \in [1 : 2N]$, are the eigenvalues of the positive semidefinite matrices $K_{\mathbf{X}}$ and G, respectively, and $G_{jj} = (2|U_j|)^{-\nu/2}$. Define

$$D(N) = \sum_{j=1}^{2N}\log\bigl(1 + (2|U_j|)^{-\nu/2}(2NP)^{1/2}\bigr).$$

Then we have the following.

Lemma 19.2. $D(N) = O\bigl(N^{1/2+1/\nu}\log N\bigr)$ w.h.p.

The proof of this lemma is given in Appendix 19B.

Combining the lemma with the bound in (19.12) completes the proof of Theorem 19.3.

Remark 19.6. If we assume the path loss to include *absorption*, i.e.,

$$g(r) = e^{-\gamma r/2}r^{-\nu/2}$$

for some $\gamma > 0$, the effect of interference in the network becomes more localized and the upper bound on $C(N)$ reduces to $O(N^{-1/2}(\log N)^2)$ w.h.p., which has roughly the same order as the lower bound.

SUMMARY

- Cutset bound for the Gaussian network
- Noisy network coding achieves within a constant gap of the cutset bound for Gaussian multimessage multicast networks
- Relaying plays a key role in combating high path loss and interference in large wireless networks
- Scaling laws for network capacity
- Random network model
- Cellular time-division scheme:
  - Outperforms time division with relaying via spatial reuse of time/frequency enabled by high path loss
  - Achieves close to the symmetric capacity order for most networks as the path loss exponent becomes large, and is order-optimal under the absorption model
- Use of network augmentation in the proof of the symmetric capacity upper bound
- **Open problems:**

  19.1. What is the capacity region of the Gaussian two-way relay channel with no direct links?

  19.2. What is the symmetric capacity scaling law for the random network model?

BIBLIOGRAPHIC NOTES

The noisy network coding inner bound on the capacity region of the Gaussian multimessage multicast network in (19.3) and the constant gap result in Theorem 19.2 were established by Lim, Kim, El Gamal, and Chung (2011). The Gaussian two-way relay channel with and without direct links was studied by Rankov and Wittneben (2006), Katti, Maric, Goldsmith, Katabi, and Médard (2007), Nam, Chung, and Lee (2010), and Lim, Kim, El Gamal, and Chung (2011, 2010). The layered noisy network coding scheme mentioned in Remark 19.2 was proposed by Lim, Kim, El Gamal, and Chung (2010), who showed that it can significantly improve the achievable rates over nonlayered noisy network coding.

The random network model was first introduced by Gupta and Kumar (2000). They analyzed the network under two *network theoretic* models for successful transmission, the signal-to-interference ratio (SIR) model and the *protocol* model. They roughly showed that the symmetric capacity under these models scales as $\Theta(N^{-1/2})$. Subsequent work under these network theoretic models include Grossglauser and Tse (2002) and El Gamal, Mammen, Prabhakar, and Shah (2006a,b).

The capacity scaling of a random network was first studied by Xie and Kumar (2004). Subsequent work includes Gastpar and Vetterli (2005) and Özgür, Lévêque, and Preissmann (2007). The lower bound in Theorem 19.3 is due to El Gamal, Mammen, Prabhakar, and Shah (2006a). This lower bound was improved to $C(N) = \Omega(N^{-1/2})$ w.h.p. by Franceschetti, Dousse, Tse, and Thiran (2007). The upper bound in Theorem 19.3 was established by Lévêque and Telatar (2005). Analysis of scaling laws based on physical limitations on electromagnetic wave propagation was studied in Franceschetti, Migliore, and Minero (2009) and Özgür, Lévêque, and Tse (2010).

PROBLEMS

19.1. Prove the cutset bound in Theorem 19.1.

19.2. Consider the Gaussian two-way relay channel in Section 19.1.2.

(a) Derive the cutset bound in (19.4), the decode–forward inner bound in (19.5), the amplify–forward inner bound in (19.6), and the noisy network coding inner bound in (19.7).

(b) Suppose that in the decode–forward coding scheme, node 3 uses network coding and broadcasts the modulo-2 sum of the binary sequence representations of M_1 and M_2, instead of (M_1, M_2), and nodes 1 and 2 find each other's message by first recovering the modulo-2 sum. Show that this modified coding scheme yields the lower bound

$$\begin{aligned} R_1 &< \min\{\mathsf{C}(S_{31}),\, \mathsf{C}(S_{13}),\, \mathsf{C}(S_{23})\}, \\ R_2 &< \min\{\mathsf{C}(S_{32}),\, \mathsf{C}(S_{13}),\, \mathsf{C}(S_{23})\}, \\ R_1 + R_2 &< \mathsf{C}(S_{31} + S_{32}). \end{aligned}$$

Note that this bound is worse than the decode–forward lower bound when node 3 broadcasts (M_1, M_2)! Explain this surprising result.

(c) Let $g_{31} = g_{32} = 1$ and $g_{13} = g_{23} = 2$. Show that the gap between the decode–forward inner bound and the cutset bound is unbounded.

(d) Let $g_{31} = g_{13} = g_{23} = 1$ and $g_{32} = \sqrt{P}$. Show that the gap between the amplify–forward inner bound and the cutset bound is unbounded.

19.3. Consider the cellular time-division scheme in Section 19.3.1.

(a) Show that $\mathsf{P}(\mathcal{E}_1)$ tends to zero as $n \to \infty$.

(b) Verify the upper bound on the total average interference power in (19.10).

19.4. *Capacity scaling of the N-user-pair Gaussian IC.* Consider the N-user-pair symmetric Gaussian interference channel

$$Y^N = GX^N + Z^N,$$

where the channel gain matrix is

$$G = \begin{bmatrix} 1 & a & \cdots & a \\ a & 1 & \cdots & a \\ \vdots & \vdots & \ddots & \vdots \\ a & a & \cdots & 1 \end{bmatrix}.$$

Assume average power constraint P on each sender. Denote the symmetric capacity by $C(N)$.

(a) Using time division with power control, show that the symmetric capacity is lower bounded as

$$C(N) \geq \frac{1}{N} \mathsf{C}(NP).$$

(b) Show that the symmetric capacity is upper bounded as $C(N) \leq \mathsf{C}(P)$. (Hint: Consider the case $a = 0$.)

(c) Tighten the bound in part (b) and show that

$$\begin{aligned} C(N) &\leq \frac{1}{2N} \log |I + GG^T P| \\ &= \frac{1}{2N} \log \big((1 + (a-1)^2 P)^{k-1} (1 + (a(N-1) + 1)^2 P)\big). \end{aligned}$$

(d) Show that when $a = 1$, the symmetric capacity is $C(N) = (1/N)\,\mathsf{C}(P)$.

APPENDIX 19A PROOF OF LEMMA 19.1

It is straightforward to show that the number of sources in each cell $S(N) = O(\log N)$ w.h.p. We now bound $L(N)$. Consider a *torus* with the same area and the same square cell division as the square area. For each S-D pair on the torus, send each packet along the four possible lines connecting them. Clearly for every configuration of nodes, each cell in the torus has at least as many S-D lines crossing it as in the original square. The reason we consider the torus is that the pmf of the number of lines in each cell becomes the same, which greatly simplifies the proof.

Let H_j be the total number of hops taken by packets traveling along one of the four lines between S-D pair j, $j \in [1 : N]$. It is not difficult to see that the expected length of each path is $\Theta(N^{1/2})$. Since the hops are along cells having side-length $(\log N)^{1/2}$,

$$\mathsf{E}(H_j) = \Theta\big((N/\log N)^{1/2}\big).$$

Fix a cell $c \in [1 : N/\log N]$ and define E_{jc} to be the indicator of the event that a line between S-D pair $j \in [1 : N]$ passes through cell $c \in [1 : N/\log N]$, i.e.,

$$E_{jc} = \begin{cases} 1 & \text{if a hop of S-D pair } j \text{ is in cell } c, \\ 0 & \text{otherwise.} \end{cases}$$

Summing up the total number of hops in the cells in two different ways, we obtain

$$\sum_{j=1}^{N} \sum_{c=1}^{N/\log N} E_{jc} = \sum_{j=1}^{N} H_j.$$

Taking expectations on both sides and noting that the probabilities $\mathsf{P}\{E_{jc} = 1\}$ are equal for all $j \in [1:N]$ because of the symmetry on the torus, we obtain

$$\frac{N^2}{\log N} \mathsf{P}\{E_{jc} = 1\} = N \mathsf{E}(H_j),$$

or equivalently,

$$\mathsf{P}\{E_{jc} = 1\} = \Theta\big((\log N/N)^{1/2}\big)$$

for $j \in [1:N]$ and $c \in [1:N/\log N]$. Now for a fixed cell c, the total number of lines passing through it is $L_c = \sum_{j=1}^{N} E_{jc}$. This is the sum of N i.i.d. Bernoulli random variables since the positions of the nodes are independent and E_{jc} depends only on the positions of the source and destination nodes of S-D pair j. Moreover

$$\mathsf{E}(L_c) = \sum_{j=1}^{N} \mathsf{P}\{E_{jc} = 1\} = \Theta\big((N \log N)^{1/2}\big)$$

for every cell c. Hence, by the Chernoff bound,

$$\mathsf{P}\{L_c > (1+\delta)\,\mathsf{E}(L_c)\} \le \exp(-\mathsf{E}(L_c)\delta^2/3).$$

Choosing $\delta = 2\sqrt{2\log N/\mathsf{E}(L_c)}$ yields

$$\mathsf{P}\{L_c > (1+\delta)\,\mathsf{E}(L_c)\} \le 1/N^2.$$

Since $\delta = o(1)$, $L_c = O(\mathsf{E}(L_c))$ with probability $\ge 1 - 1/N^2$. Finally using the union of events bound over $N/\log N$ cells shows that $L(N) = \max_{c\in[1:N/\log N]} L_c = O((N\log N)^{1/2})$ with probability $\ge 1 - 1/(N\log N)$ for sufficiently large N.

APPENDIX 19B PROOF OF LEMMA 19.2

Define

$$W(N) = \log\left(1 + (2U)^{-\nu/2}(2NP)^{1/2}\right),$$

where $U \sim \text{Unif}[0, N^{1/2}]$. Since $D(N)$ is the sum of i.i.d. random variables, we have

$$\mathsf{E}(D(N)) = N\,\mathsf{E}(W(N)),$$
$$\text{Var}(D(N)) = N\,\text{Var}(W(N)).$$

We find upper and lower bounds on $\mathsf{E}(W(N))$ and an upper bound on $\mathsf{E}(W^2(N))$. For

simplicity, we assume the natural logarithm here since we are only interested in order results. Let $a = e^{-\frac{\nu-1}{2}} P^{1/2}$, $\nu' = \nu/2$, $k = N^{1/2}$, and $u_0 = (ak)^{1/\nu'}$. Consider

$$\begin{aligned} k\,\mathsf{E}(W(N)) &= \int_0^k \log(1 + au^{-\nu'}k)\,du \\ &= \int_0^1 \log(1 + au^{-\nu'}k)\,du + \int_1^{u_0} \log(1 + au^{-\nu'}k)\,du \\ &\quad + \int_{u_0}^k \log(1 + au^{-\nu'}k)\,du \qquad (19.13) \\ &\le \int_0^1 \log((1 + ak)u^{-\nu'})\,du + \int_1^{u_0} \log(1 + ak)\,du + \int_{u_0}^k au^{-\nu'}k\,du \\ &= \log(1 + ak) + \nu' \int_0^1 \log(1/u)\,du + (u_0 - 1)\log(1 + ak) \\ &\quad + \frac{ak}{\nu' - 1}\left(u_0^{-(\nu'-1)} - k^{-(\nu'-1)}\right). \end{aligned}$$

Thus, there exists a constant $b_1 > 0$ such that for N sufficiently large,

$$\mathsf{E}(W(N)) \le b_1 N^{-1/2+1/\nu} \log N. \qquad (19.14)$$

Now we establish a lower bound on $\mathsf{E}(W(N))$. From (19.13), we have

$$k\,\mathsf{E}(W(N)) \ge \int_1^{u_0} \log(1 + au^{-\nu'}k)\,du \ge \int_1^{u_0} \log(1 + a)\,du = (u_0 - 1)\log(1 + a).$$

Thus there exists a constant $b_2 > 0$ such that for N sufficiently large,

$$\mathsf{E}(W(N)) \ge b_2 N^{-1/2+1/\nu}. \qquad (19.15)$$

Next we find an upper bound on $\mathsf{E}(W^2(N))$. Consider

$$\begin{aligned} k\,\mathsf{E}(W^2(N)) &= \int_0^1 \left(\log(1 + au^{-\nu'}k)\right)^2 du + \int_1^{u_0} \left(\log(1 + au^{-\nu'}k)\right)^2 du \\ &\quad + \int_{u_0}^k \left(\log(1 + au^{-\nu'}k)\right)^2 du \\ &\le \int_0^1 \left(\log((1 + ak)u^{-\nu'})\right)^2 du + \int_1^{u_0} \left(\log(1 + ak)\right)^2 du + \int_{u_0}^k a^2 u^{-2\nu'} k^2\,du \\ &\le \left(\log(1 + ak)\right)^2 + (\nu')^2 \int_0^1 (\log(1/u))^2\,du \\ &\quad + 2\nu' \log(1 + ak) \int_0^1 \log(1/u)\,du + (u_0 - 1)\left(\log(1 + ak)\right)^2 \\ &\quad + \frac{a^2k^2}{2\nu' - 1}\left(u_0^{-(2\nu'-1)} - k^{-(2\nu'-1)}\right). \end{aligned}$$

Thus there exists a constant $b_3 > 0$ such that for N sufficiently large,

$$\mathsf{E}(W^2(N)) \leq b_3 N^{-1/2+1/\nu} (\log N)^2. \tag{19.16}$$

Finally, using the Chebyshev lemma in Appendix B and substituting from (19.14), (19.15), and (19.16), then for N sufficiently large, we have

$$\begin{aligned}
\mathsf{P}\{D(N) \geq 2b_1 N^{1/2+1/\nu} \log N\} &\leq \mathsf{P}\{D(N) \geq 2\,\mathsf{E}(D(N))\} \\
&\leq \frac{\mathrm{Var}(D(N))}{(\mathsf{E}[D(N)])^2} \\
&\leq \frac{N\,\mathsf{E}(W^2(N))}{N^2(\mathsf{E}[W(N)])^2} \\
&\leq \frac{b_3 N^{-1/2+1/\nu} (\log N)^2}{b_2^2 N^{2/\nu}} \\
&= \left(\frac{b_3}{b_2^2}\right) N^{-1/2-1/\nu} (\log N)^2,
\end{aligned}$$

which tends to zero as $N \to \infty$. This completes the proof of the lemma.

CHAPTER 24

Networking and Information Theory

The source and network models we discussed so far capture many essential ingredients of real-world communication networks, including

- noise,
- multiple access,
- broadcast,
- interference,
- time variation and uncertainty about channel statistics,
- distributed compression and computing,
- joint source–channel coding,
- multihop relaying,
- node cooperation,
- interaction and feedback, and
- secure communication.

Although a general theory for information flow under these models remains elusive, we have seen that there are several coding techniques—some of which are optimal or close to optimal—that promise significant performance improvements over today's practice. Still, the models we discussed do not capture other key aspects of real-world networks.

- We assumed that data is always available at the communication nodes. In real-world networks, data is bursty and the nodes have finite buffer sizes.
- We assumed that the network has a known and fixed number of users. In real-world networks, users can enter and leave the network at will.
- We assumed that the network operation is centralized and communication over the network is synchronous. Many real-world networks are decentralized and communication is asynchronous.

- We analyzed performance assuming arbitrarily long delays. In many networking applications, delay is a primary concern.
- We ignored the overhead (protocol) needed to set up the communication as well as the cost of feedback and channel state information.

While these key aspects of real-world networks have been at the heart of the field of computer networks, they have not been satisfactorily addressed by network information theory, either because of their incompatibility with the basic asymptotic approach of information theory or because the resulting models are messy and intractable. There have been several success stories at the intersection of networking and network information theory, however. In this chapter we discuss three representative examples.

We first consider the channel coding problem for a DMC with random data arrival. We show that reliable communication is feasible provided that the data arrival rate is less than the channel capacity. Similar results can be established for multiuser channels and multiple data streams. A key new ingredient in this study is the notion of queue stability.

The second example we discuss is motivated by the random medium access control scheme for sharing a channel among multiple senders such as in the ALOHA network. We model a 2-sender 1-receiver random access system by a modulo-2 sum MAC with multiplicative binary state available partially at each sender and completely at the receiver. We apply various coding approaches introduced in Chapter 23 to this model and compare the corresponding performance metrics.

Finally, we investigate the effect of asynchrony on the capacity region of the DM-MAC. We extend the synchronous multiple access communication system setup in Chapter 4 to multiple transmission blocks in order to incorporate unknown transmission delays. When the delay is small relative to the transmission block length, the capacity region does not change. However, when we allow arbitrary delay, time sharing cannot be used and hence the capacity region can be smaller than for the synchronous case.

24.1 RANDOM DATA ARRIVALS

In the point-to-point communication system setup in Section 3.1 and subsequent extensions to multiuser channels, we assumed that data is always available at the encoder. In many networking applications, however, data is bursty and it may or may not be available at the senders when the channel is free. Moreover, the amount of data at a sender may exceed its finite buffer size, which results in data loss even before transmission takes place. It turns out that under fairly general data arrival models, if the data rate λ bits/transmission is below the capacity C of the channel, then the data can be reliably communicated to the receiver, while if $\lambda > C$, data cannot be reliably communicated either because the incoming data exceeds the sender's queue size or because transmission rate exceeds the channel capacity. We illustrate this general result using a simple random data arrival process.

Consider the point-to-point communication system with random data arrival at its input depicted in Figure 24.1. Suppose that data packets arrive at the encoder at the "end"

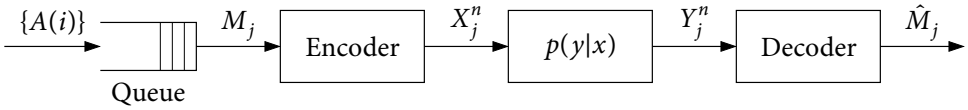


Figure 24.1. Communication system with random data arrival.

of transmission time $i = 1, 2, \ldots$ according to an i.i.d. process $\{A(i)\}$, where

$$A(i) = \begin{cases} k & \text{with probability } p, \\ 0 & \text{with probability } \bar{p}. \end{cases}$$

Thus, a packet randomly and uniformly chosen from the set of k-bit sequences arrives at the encoder with probability p and no packet arrives with probability $\bar{p}$. Assume that the packets arriving at different transmission times are independent of each other.

A $(2^{nR}, n)$ *augmented* block code for the DMC consists of

- an augmented message set $[1 : 2^{nR}] \cup \{0\}$,
- an encoder that assigns a codeword $x^n(m)$ to each $m \in [1 : 2^{nR}] \cup \{0\}$, and
- a decoder that assigns a message $\hat{m} \in [1 : 2^{nR}] \cup \{0\}$ or an error message e to each received sequence y^n.

The code is used in consecutive transmission blocks as follows. Let $Q(i)$ be the number of bits (backlog) in the sender's queue at the "beginning" of transmission time $i = 1, 2, \ldots$. At the beginning of time jn, $j = 1, 2, \ldots$, that is, at the beginning of transmission block j, nR bits are taken out of the queue if $Q(jn) \geq nR$. The bits are represented by a message $M_j \in [1 : 2^{nR}]$ and the codeword $x^n(m_j)$ is sent over the DMC. If $Q(jn) < nR$, no bits are taken out of the queue and the "0-message" codeword $x^n(0)$ is sent. Thus, the backlog $Q(i)$ is a time-varying Markov process with transition law

$$Q(i+1) = \begin{cases} Q(i) - nR + A(i) & \text{if } i = jn \text{ and } Q(i) \geq nR, \\ Q(i) + A(i) & \text{otherwise.} \end{cases} \tag{24.1}$$

The queue is said to be *stable* if $\sup_i \mathsf{E}(Q(i)) \leq B$ for some constant $B < \infty$. By the Markov inequality, queue stability implies that the probability of data loss can be made as small as desired with a finite buffer size. Define the *arrival rate* $\lambda = kp$ as the product of the packet arrival rate $p \in (0, 1]$ and packet size k bits. We have the following sufficient and necessary conditions on the stability of the queue in terms of the transmission rate R and the arrival rate λ.

Lemma 24.1. If $\lambda < R$, then the queue is stable. Conversely, if the queue is stable, then $\lambda \leq R$.

The proof of this lemma is given in Appendix 24.1.

Let $p_j = \mathsf{P}\{M_j = 0\}$ be the probability that the sender queue has less than nR bits at the beginning of transmission block j. By the definition of the arrival time process, $M_j \,|\, \{M_j \neq 0\} \sim \text{Unif}[1 : 2^{nR}]$. Define the probability of error in transmission block j as

$$P_{ej}^{(n)} = \mathsf{P}\{\hat{M}_j \neq M_j\} = p_j \,\mathsf{P}\{\hat{M}_j \neq 0 \,|\, M_j = 0\} + \frac{(1 - p_j)}{2^{nR}} \sum_{m=1}^{2^{nR}} \mathsf{P}\{\hat{M}_j \neq m \,|\, M_j = m\}.$$

The data arriving at the encoder according to the process $\{A(i)\}$ is said to be reliably communicated at rate R over the DMC if the queue is stable and there exists a sequence of $(2^{nR}, n)$ augmented codes such that $\lim_{n\to\infty} \sup_j P_{ej}^{(n)} = 0$. We wish to find the necessary and sufficient condition for reliable communication of the data over the DMC.

Theorem 24.1. The random data arrival process $\{A(i)\}$ with arrival rate λ can be reliably communicated at rate R over a DMC $p(y|x)$ with capacity C if $\lambda < R < C$. Conversely, if the process $\{A(i)\}$ can be reliably communicated at rate R over this DMC, then $\lambda \leq R \leq C$.

Proof. To prove achievability, let $\lambda < R < C$. Then the queue is stable by Lemma 24.1 and there exists a sequence of $(2^{nR} + 1, n)$ (regular) channel codes such that both the average probability of error $P_e^{(n)}$ and $\mathsf{P}\{\hat{M} \neq M \,|\, M = m'\}$ for some m' tend to zero as $n \to \infty$. By relabeling $m' = 0$, we have shown that there exists a sequence of $(2^{nR}, n)$ augmented codes such that $P_{ej}^{(n)}$ tends to zero as $n \to \infty$ for every j.

To prove the converse, note first that $\lambda \leq R$ from Lemma 24.1. Now, for each j, following similar steps to the converse proof of the channel coding theorem in Section 3.1.4, we obtain

$$\begin{aligned} nR &= H(M_j \,|\, M_j \neq 0) \\ &\leq I(M_j; Y^n \,|\, M_j \neq 0) + n\epsilon_n \\ &\leq \sum_{i=1}^{n} I(X_i; Y_i \,|\, M_j \neq 0) + n\epsilon_n \\ &\leq n(C + \epsilon_n). \end{aligned} \tag{24.2}$$

This completes the proof of Theorem 24.1.

Remark 24.1. Theorem 24.1 continues to hold for arrival processes for which Lemma 24.1 holds. It can be also extended to multiuser channels with random data arrivals at each sender. For example, consider the case of a DM-MAC with two independent i.i.d. arrival processes $\{A_1(i)\}$ and $\{A_2(i)\}$ of arrival rates λ_1 and λ_2, respectively. The *stability region* $\mathscr{S}$ for the two sender queues is the closure of the set of arrival rates (λ_1, λ_2) such that both queues are stable. We define the augmented code $(2^{nR_1}, 2^{nR_2}, n)$, the average probability of error, and achievability as for the point-to-point case. Let $\mathscr{C}$ be the capacity region of the DM-MAC. Then it can be readily shown that $\mathscr{S} = \mathscr{C}$. Note that the same result holds when the packet arrivals (but not the packet contents) are correlated.

Remark 24.2. The conclusion that randomly arriving data can be communicated reliably over a channel when the arrival rate is less than the capacity trivializes the effect of randomness in data arrival. In real-world applications, packet delay constraints are as important as queue stability. However, the above result, and the asymptotic approach of information theory in general, does not capture such constraints well.

24.2 RANDOM ACCESS CHANNEL

The previous section dealt with random data arrivals at the senders. In this section, we consider random data arrivals at the receivers. We discuss random access, which is a popular scheme for medium access control in local area networks. In these networks, the number of senders is not fixed a priori and hence using time division can be inefficient. The random access scheme improves upon time division by having each active sender transmit its packets in randomly selected transmission blocks. In practical random access control systems, however, the packets are encoded at a fixed rate and if more than one sender transmits in the same block, the packets are lost. It turns out that we can do better by using more sophisticated coding schemes.

We model a random access channel by a modulo-2 sum MAC with multiplicative binary state components as depicted in Figure 24.2. The output of the channel at time i is

$$Y_i = S_{1i} \cdot X_{1i} \oplus S_{2i} \cdot X_{2i},$$

where the states S_{1i} and S_{2i} are constant over each *access time interval* $[(l-1)k+1 : lk]$ of length k for $l = 1, 2, \ldots$, and the processes $\{\bar{S}_{1l}\}_{l=1}^{\infty} = \{S_{1,(l-1)k+1}\}_{l=1}^{\infty}$ and $\{\bar{S}_{2l}\}_{l=1}^{\infty} = \{S_{2,(l-1)k+1}\}_{l=1}^{\infty}$ are independent Bern(p) processes. Sender $j = 1, 2$ is active (has a packet to transmit) when $S_j = 1$ and is inactive when $S_j = 0$. We assume that the receiver knows which senders are active in each access time interval, but each sender knows only its own activity.

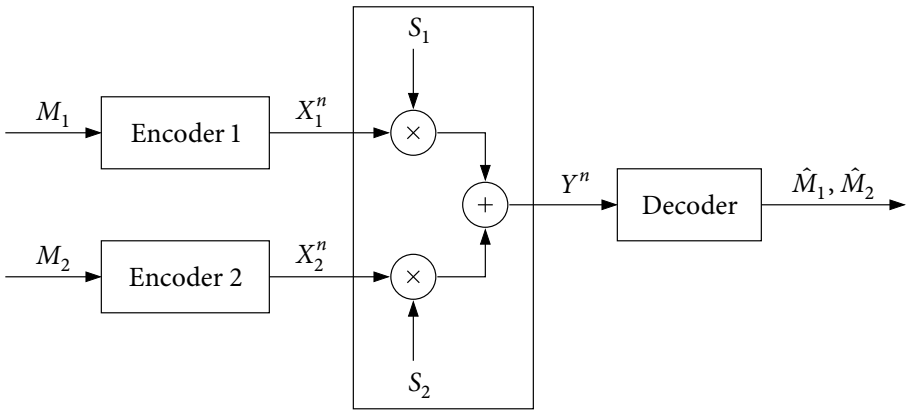


Figure 24.2. Random access channel.

Note that this model is analogous to the Gaussian fading MAC in Section 23.5, where the channel gains are available at the receiver but each sender knows only the gain of its own channel. Since each sender becomes active at random in each block, the communication model corresponds to the slow fading scenario. Using the analogy to the fading MAC, we consider different coding approaches and corresponding performance metrics for the random access channel. Unlike the fading MAC, however, no coordination is allowed between the senders in the random access channel.

Compound channel approach. In this approach, we code for the worst case in which no packets are to be transmitted (i.e., $S_{1i} = S_{2i} = 0$ for all $i \in [1 : n]$). Hence, the capacity region is $\{(0, 0)\}$.

ALOHA. In this approach, sender $j = 1, 2$ transmits at rate $R_j = 1$ when it is active and at rate $R_j = 0$ when it is not. When there is collision (that is, both senders are active), decoding simply fails. The *ALOHA sum-capacity* (that is, the average total throughput) is

$$C_{\text{ALOHA}} = p(1 - p) + p(1 - p) = 2p(1 - p).$$

Adaptive coding. By reducing the rates in the ALOHA approach to $\tilde{R}_j \le 1$ when sender $j = 1, 2$ is active (so that the messages can be recovered even under collision), we can increase the average throughput.

To analyze the achievable rates for this approach, consider the 2-sender 3-receiver channel depicted in Figure 24.3. It can be easily shown that the capacity region of this channel is the set of rate pairs $(\tilde{R}_1, \tilde{R}_2)$ such that $\tilde{R}_1 + \tilde{R}_2 \le 1$ and is achieved using simultaneous decoding without time sharing; see Problem 24.4. Hence, any rate pair $(\tilde{R}_1, \tilde{R}_2)$ in the capacity region of the 2-sender 3-receiver channel is achievable for the random access channel, even though each sender is aware only of its own activity. In particular, the *adaptive coding sum-capacity* is

$$C_{\text{A}} = \max_{(\tilde{R}_1, \tilde{R}_2): \tilde{R}_1 + \tilde{R}_2 \le 1} \big(\mathsf{P}\{S_1 = 1\}\tilde{R}_1 + \mathsf{P}\{S_2 = 1\}\tilde{R}_2\big) = p.$$

Broadcast channel approach. In the ALOHA approach, the messages cannot be recovered at all when there is a collision. In the adaptive coding approach, both messages must

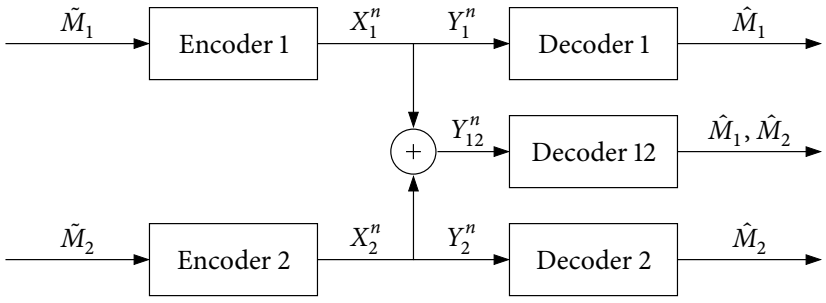


Figure 24.3. Adaptive coding for the random access channel.

be recovered even when there is a collision. The broadcast approach combines these two approaches by requiring only part of each message to be recovered when there is a collision and the rest of the message to be also recovered when there is no collision. This is achieved using superposition coding. To analyze the achievable rates for this strategy, consider the 2-sender 3-receiver channel depicted in Figure 24.4. Here the message pair $(\tilde{M}_{j0}, \tilde{M}_{jj})$ from the active sender j is to be recovered when there is no collision, while the message pair $(\tilde{M}_{10}, \tilde{M}_{20})$, one from each sender is to be recovered when there is collision. It can be shown (see Problem 24.5) that the capacity region of this 2-sender 3-receiver channel is the set of rate quadruples $(\tilde{R}_{10}, \tilde{R}_{11}, \tilde{R}_{20}, \tilde{R}_{22})$ such that

$$\begin{aligned} \tilde{R}_{10} + \tilde{R}_{20} + \tilde{R}_{11} &\le 1, \\ \tilde{R}_{10} + \tilde{R}_{20} + \tilde{R}_{22} &\le 1. \end{aligned} \tag{24.3}$$

As for the adaptive coding case, this region can be achieved using simultaneous decoding without time sharing. Note that taking $(\tilde{R}_{11}, \tilde{R}_{22}) = (0, 0)$ reduces to the adaptive coding case. The average throughput of sender $j \in \{1, 2\}$ is

$$R_j = p(1-p)(\tilde{R}_{j0} + \tilde{R}_{jj}) + p^2 \tilde{R}_{j0} = p\tilde{R}_{j0} + p(1-p)\tilde{R}_{jj}.$$

Thus, the *broadcast sum-capacity* is

$$C_{\text{BC}} = \max\big(p(\tilde{R}_{10} + \tilde{R}_{20}) + p(1-p)(\tilde{R}_{11} + \tilde{R}_{22})\big),$$

where the maximum is over all rate quadruples in the capacity region in (24.3). By symmetry, it can be readily checked that

$$C_{\text{BC}} = \max\{2p(1-p),\ p\}.$$

Note that this sum-capacity is achieved by setting $\tilde{R}_{11} = \tilde{R}_{22} = 1, \tilde{R}_{10} = \tilde{R}_{20} = 0$ for $p \le 1/2$, and $\tilde{R}_{10} = \tilde{R}_{20} = 1/2$, $\tilde{R}_{11} = \tilde{R}_{22} = 0$ for $p \ge 1/2$. Hence, ignoring collision (ALOHA) is throughput-optimal when $p \le 1/2$, while the broadcast channel approach reduces to adaptive coding when $p \ge 1/2$.

Figure 24.5 compares the sum-capacities C_{CC} (compound channel approach), C_{ALOHA} (ALOHA), C_{A} (adaptive coding), and C_{BC} (broadcast channel approach). Note that the broadcast channel approach performs better than adaptive coding when the senders are active less often ($p \le 1/2$).

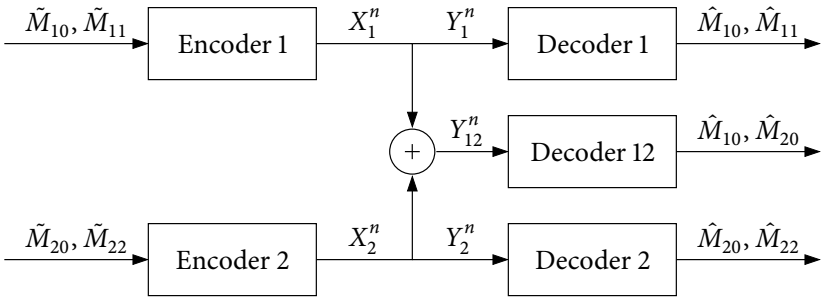


Figure 24.4. Broadcast coding for the random access channel.

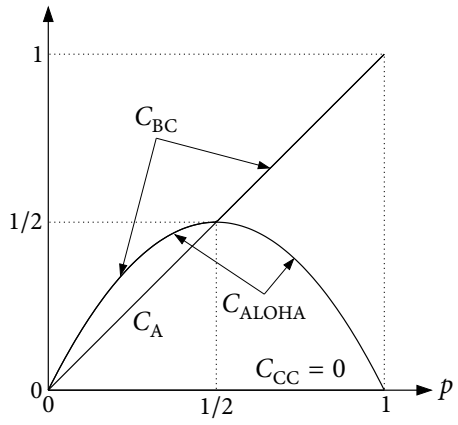


Figure 24.5. Comparison of the sum-capacities of the random access channel—C_{CC} for the compound approach, C_{ALOHA} for ALOHA, C_A for adaptive coding, and C_{BC} for the broadcast channel approach.

24.3 ASYNCHRONOUS MAC

In the single-hop channel models we discussed in Part II of the book, we assumed that the transmissions from the senders to the receivers are synchronized (at both the symbol and block levels). In practice, such complete synchronization is often not feasible. How does the lack of synchronization affect the capacity region of the channel? We answer this question for the asynchronous multiple access communication system depicted in Figure 24.6.

Suppose that sender $j = 1, 2$ wishes to communicate an i.i.d. message sequence $(M_{j1}, M_{j2}, \ldots)$. Assume that the same codebook is used in each transmission block. Further assume that symbols are synchronized, but that the blocks sent by the two encoders incur arbitrary delays $d_1, d_2 \in [0 : d]$, respectively, for some $d \le n - 1$. Assume that the encoders and the decoder do not know the delays a priori. The received sequence Y^n is distributed according to

$$p(y^n | x^n_{1,1-d_1}, x^n_{2,1-d_2}) = \prod_{i=1}^{n} p_{Y|X_1,X_2}(y_i | x_{1,i-d_1}, x_{2,i-d_2}),$$

where the symbols with negative indices are from the previous transmission block.

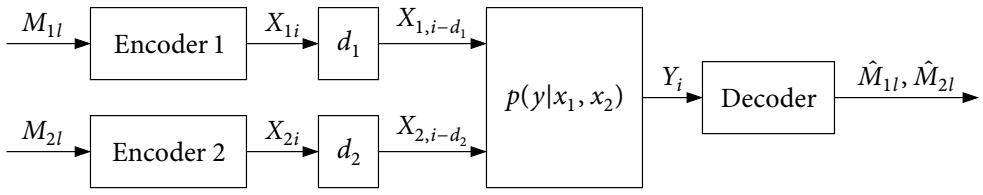


Figure 24.6. Asynchronous multiple access communication system.

A $(2^{nR_1}, 2^{nR_2}, n, d)$ code for the asynchronous DM-MAC consists of

- two message sets $[1 : 2^{nR_1}]$ and $[1 : 2^{nR_2}]$,
- two encoders, where encoder 1 assigns a sequence of codewords $x_1^n(m_{1l})$ to each message sequence $m_{1l} \in [1 : 2^{nR_1}]$, $l = 1, 2, \ldots$, and encoder 2 assigns a sequence of codewords $x_2^n(m_{2l})$ to each message sequence $m_{2l} \in [1 : 2^{nR_2}]$, $l = 1, 2, \ldots$, and
- a decoder that assigns a sequence of message pairs $(\hat{m}_{1l}, \hat{m}_{2l}) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$ or an error message e to each received sequence $y_{(l-1)n+1}^{ln+d}$ for each $l = 1, 2, \ldots$ (the received sequence $y_{(l-1)n+1}^{ln+d}$ can include parts of the previous and next blocks).

We assume that the message sequences $\{M_{1l}\}_{l=1}^{\infty}$ and $\{M_{2l}\}_{l=1}^{\infty}$ are independent and each message pair (M_{1l}, M_{2l}), $l = 1, 2, \ldots$, is uniformly distributed over $[1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$. The average probability of error is defined as

$$P_e^{(n)} = \max_{d_1, d_2 \in [0:d]} \sup_l P_{el}^{(n)}(d_1, d_2),$$

where $P_{el}^{(n)}(d_1, d_2) = \mathsf{P}\{(\hat{M}_{1l}, \hat{M}_{2l}) \neq (M_{1l}, M_{2l}) \,|\, d_1, d_2\}$. Note that by the memoryless property of the channel and the definition of the code, $\sup_l P_{el}^{(n)}(d_1, d_2) = P_{el}^{(n)}(d_1, d_2)$ for all l. Thus in the following, we drop the subscript l. Achievability and the capacity region are defined as for the synchronous DM-MAC.

We consider two degrees of asynchrony.

Mild asynchrony. Suppose that d/n tends to zero as $n \to \infty$. Then, it can be shown that the capacity region is the same as for the synchronous case.

Total asynchrony. Suppose that d_1 and d_2 can vary from 0 to $(n-1)$, i.e., $d = n - 1$. In this case, time sharing is no longer feasible and the capacity region reduces to the following.

Theorem 24.2. The capacity region of the totally asynchronous DM-MAC is the set of all rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\le I(X_1; Y \,|\, X_2), \\ R_2 &\le I(X_2; Y \,|\, X_1), \\ R_1 + R_2 &\le I(X_1, X_2; Y) \end{aligned}$$

for some pmf $p(x_1)p(x_2)$.

Note that this region is not convex in general, since time sharing is sometimes necessary; see Problem 4.2. Hence, unlike the synchronous case, the capacity region for networks with total asynchrony is not necessarily convex.

Remark 24.3. The sum-capacity of the totally asynchronous DM-MAC is the same as that of the synchronous DM-MAC and is given by

$$C_{\text{sum}} = \max_{p(x_1)p(x_2)} I(X_1, X_2; Y).$$

Remark 24.4. The capacity region of the Gaussian MAC does not change with asynchrony because time sharing is not required. However, under total asynchrony, simultaneous decoding is needed to achieve all the points in the capacity region.

Remark 24.5. Theorem 24.2 also shows that the capacity of a point-to-point channel does not change with asynchrony.

We prove Theorem 24.2 in the next two subsections.

24.3.1 Proof of Achievability

Divide each n-transmission block into $(b + 1)$ subblocks each consisting of k symbols as illustrated in Figure 24.7; thus $n = (b + 1)k$ and the delays range from 0 to $(b + 1)k - 1$. The first subblock labeled $j = 0$ is the *preamble* subblock. Also divide the message pair (M_1, M_2) into b independent submessage pairs $(M_{1j}, M_{2j}) \in [1 : 2^{kR_1}] \times [1 : 2^{kR_2}]$, $j \in [1 : b]$, and send them in the following b subblocks. Note that the resulting rate pair for this code, $(bR_1/(b + 1), bR_2/(b + 1))$, can be made arbitrarily close to (R_1, R_2) as $b \to \infty$.

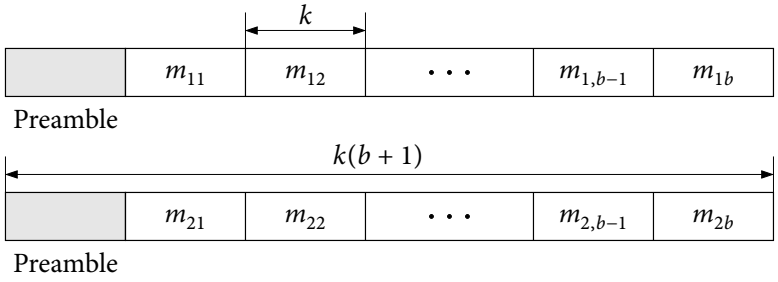


Figure 24.7. Transmission block divided into subblocks.

Codebook generation. Fix a product pmf $p(x_1)p(x_2)$. Randomly and independently generate a codebook for each subblock. Randomly generate a preamble codeword $x_1^k(0)$ according to $\prod_{i=1}^k p_{X_1}(x_{1i})$. For each $j \in [1 : b]$, randomly and independently generate 2^{kR_1} codewords $x_1^k(m_{1j})$, $m_{1j} \in [1 : 2^{kR_1}]$, each according to $\prod_{i=1}^k p_{X_1}(x_{i1})$. Similarly generate a preamble codeword $x_2^k(0)$ and codewords $x_2^k(m_{2j})$, $m_{2j} \in [1 : 2^{kR_2}]$, $j \in [1 : b]$, each according to $\prod_{i=1}^k p_{X_2}(x_{i2})$.

Encoding. To send the submessages m_1^b, encoder 1 first transmits its preamble codeword $x_1^k(0)$ followed by $x_1^k(m_{1j})$ for each $j \in [1 : b]$. Similarly, encoder 2 transmits its preamble codeword $x_2^k(0)$ followed by $x_2^k(m_{2j})$ for each $j \in [1 : b]$.

Decoding. The decoding procedure consists of two steps—preamble decoding and message decoding. The decoder declares $\hat{d}_1$ to be the estimate for d_1 if it is the unique number in $[0 : (b + 1)k - 1]$ such that $\big(x_1^k(0), y_{\hat{d}_1+1}^{\hat{d}_1+k}\big) \in \mathcal{T}_\epsilon^{(n)}$. Similarly, the decoder declares

$\hat{d}_2$ to be the estimate for d_2 if it is the unique number in $[0 : (b+1)k - 1]$ such that $(x_2^k(0), y_{\hat{d}_2+1}^{\hat{d}_2+k}) \in \mathcal{T}_\epsilon^{(n)}$.

Assume without loss of generality that $\hat{d}_1 \le \hat{d}_2$. Referring to Figure 24.8, define the sequences

$$\begin{aligned}
\mathbf{x}_1(m_1^b) &= (x_{1,\delta+1}^k(0), x_1^k(m_{11}), x_1^k(m_{12}), \ldots, x_1^k(m_{1b}), x_1^\delta(0)),\\
\mathbf{x}_2(\tilde{m}_2^{b+1}) &= (x_2^k(\tilde{m}_{21}), x_2^k(\tilde{m}_{22}), \ldots, x_2^k(\tilde{m}_{2,b+1})),\\
\mathbf{y} &= y_{\hat{d}_1+\delta+1}^{(b+1)k+\hat{d}_1+\delta},
\end{aligned}$$

where $\delta = \hat{d}_2 - \hat{d}_1 \pmod k$. The receiver declares that $\hat{m}_1^b$ is the sequence of submessages sent by sender 1 if it is the unique submessage sequence such that $(\mathbf{x}_1(\hat{m}_1^b), \mathbf{x}_2(\tilde{m}_2^{b+1}), \mathbf{y}) \in \mathcal{T}_\epsilon^{(n)}$ for some $\tilde{m}_2^{b+1}$.

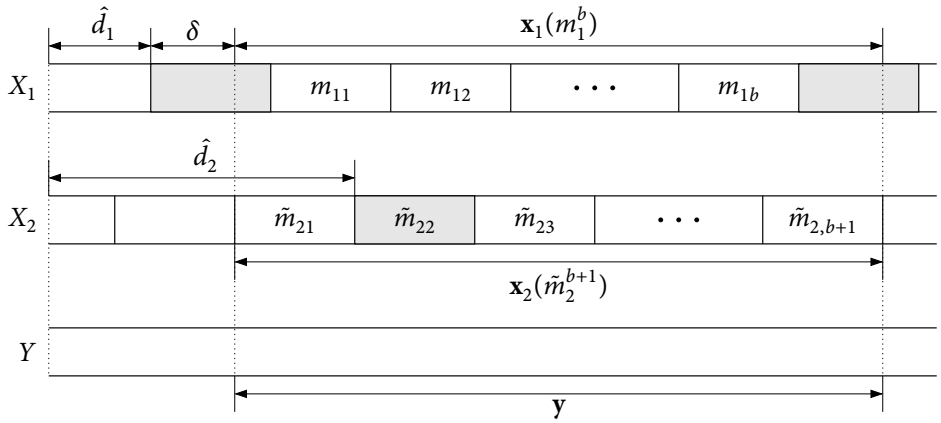


Figure 24.8. Asynchronous transmission and received sequence.

To recover the message sequence m_2^b, the same procedure is repeated beginning with the preamble of sender 2.

Analysis of the probability of error. We bound the probability of decoding error for the submessages M_1^b from sender 1 averaged over the codes. Assume without loss of generality that $M_1^b = \mathbf{1} = (1, \ldots, 1)$ and $d_1 \le d_2$. Let $\tilde{M}_2^{b+1}$, $\mathbf{X}_1(M_1^b)$, $\mathbf{X}_2(\tilde{M}_2^{b+1})$, and $\mathbf{Y}$ be defined as before (see Figure 24.8) with (d_1, d_2) in place of $(\hat{d}_1, \hat{d}_2)$. The decoder makes an error only if one or more of the following events occur:

$$\begin{aligned}
\mathcal{E}_0 &= \{(\hat{d}_1(Y^{2n-1}), \hat{d}_2(Y^{2n-1})) \ne (d_1, d_2)\},\\
\mathcal{E}_{11} &= \{(\mathbf{X}_1(\mathbf{1}), \mathbf{X}_2(\tilde{M}_2^{b+1}), \mathbf{Y}) \notin \mathcal{T}_\epsilon^{(n)}\},\\
\mathcal{E}_{12} &= \{(\mathbf{X}_1(m_1^b), \mathbf{X}_2(\bar{m}_2^{b+1}), \mathbf{Y}) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_1^b \ne \mathbf{1}, \bar{m}_2^{b+1} \ne \tilde{M}_2^{b+1}\}.
\end{aligned}$$

Thus, the probability of decoding error for M_1^b is upper bounded as

$$\mathsf{P}(\mathcal{E}_1) \le \mathsf{P}(\mathcal{E}_0) + \mathsf{P}(\mathcal{E}_{11} \cap \mathcal{E}_0^c) + \mathsf{P}(\mathcal{E}_{12} \cap \mathcal{E}_0^c). \tag{24.4}$$

To bound the first term, the probability of preamble decoding error, define the events

$$\mathcal{E}_{01} = \{(X_1^k(0), Y_{d_1+1}^{d_1+k}) \notin \mathcal{T}_\epsilon^{(n)}\},$$
$$\mathcal{E}_{02} = \{(X_2^k(0), Y_{d_2+1}^{d_2+k}) \notin \mathcal{T}_\epsilon^{(n)}\},$$
$$\mathcal{E}_{03} = \{(X_1^k(0), Y_{\tilde{d}_1+1}^{\tilde{d}_1+k}) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{d}_1 \neq d_1, \tilde{d}_1 \in [0 : (b+1)k-1]\},$$
$$\mathcal{E}_{04} = \{(X_2^k(0), Y_{\tilde{d}_2+1}^{\tilde{d}_2+k}) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{d}_2 \neq d_2, \tilde{d}_2 \in [0 : (b+1)k-1]\}.$$

Then

$$\mathsf{P}(\mathcal{E}_0) \le \mathsf{P}(\mathcal{E}_{01}) + \mathsf{P}(\mathcal{E}_{02}) + \mathsf{P}(\mathcal{E}_{03}) + \mathsf{P}(\mathcal{E}_{04}).$$

By the LLN, the first two terms tend to zero as $k \to \infty$. To bound the other two terms, we use the following.

Lemma 24.2. Let $(X, Y) \sim p(x, y) \neq p(x)p(y)$ and $(X^n, Y^n) \sim \prod_{i=1}^n p_{X,Y}(x_i, y_i)$. If $\epsilon > 0$ is sufficiently small, then there exists $\gamma(\epsilon) > 0$ that depends only on $p(x, y)$ such that

$$\mathsf{P}\{(X^k, Y_{d+1}^{d+k}) \in \mathcal{T}_\epsilon^{(k)}\} \le 2^{-k\gamma(\epsilon)}$$

for every $d \neq 0$.

The proof of this lemma is given in Appendix 24B.

Now using this lemma with $X^k \leftarrow X_1^k(0)$ and $Y_{d+1}^{d+k} \leftarrow Y_{\tilde{d}_1+1}^{\tilde{d}_1+k}$, we have

$$\mathsf{P}\{(X_1^k(0), Y_{\tilde{d}_1+1}^{\tilde{d}_1+k}) \in \mathcal{T}_\epsilon^{(k)}\} \le 2^{-k\gamma(\epsilon)}$$

for $\tilde{d}_1 < d_1$, and the same bound holds also for $\tilde{d}_1 > d_1$ by changing the role of X and Y in the lemma. Thus, by the union of events bound,

$$\mathsf{P}(\mathcal{E}_{03}) \le (b+1)k2^{-k\gamma(\epsilon)},$$

which tends to zero as $k \to \infty$. Similarly, $\mathsf{P}(\mathcal{E}_{04})$ tends to zero as $k \to \infty$.

We continue with bounding the last two terms in (24.4). By the LLN, $\mathsf{P}(\mathcal{E}_{11} \cap \mathcal{E}_0^c)$ tends to zero as $n \to \infty$. To upper bound $\mathsf{P}(\mathcal{E}_{12} \cap \mathcal{E}_0^c)$, define the events

$$\mathcal{E}(\mathcal{J}_1, \mathcal{J}_2) = \{(\mathbf{X}_1(m_1^b), \mathbf{X}_2(\bar{m}_2^{b+1}), \mathbf{Y}) \in \mathcal{T}_\epsilon^{(n)} \text{ for } m_{1j_1} = 1, j_1 \notin \mathcal{J}_1, \bar{m}_{2j_2} = \tilde{M}_{2j_2}, j_2 \notin \mathcal{J}_2$$
$$\text{and some } m_{1j_1} \neq 1, j_1 \in \mathcal{J}_1, \bar{m}_{2j_2} \neq \tilde{M}_{2j_2}, j_2 \in \mathcal{J}_2\}$$

for each $\mathcal{J}_1 \subseteq [1 : b]$ and $\mathcal{J}_2 \subseteq [1 : b+1]$. Then

$$\mathsf{P}(\mathcal{E}_{12} \cap \mathcal{E}_0^c) \le \sum_{\emptyset \neq \mathcal{J}_1 \subseteq [1:b],\, \mathcal{J}_2 \subseteq [1:b+1]} \mathsf{P}(\mathcal{E}(\mathcal{J}_1, \mathcal{J}_2)).$$

We bound each term. Consider the event $\mathcal{E}(\mathcal{J}_1, \mathcal{J}_2)$ illustrated in Figure 24.9 for $b = 5$, $\mathcal{J}_1 = \{1, 3\}$, $\mathcal{J}_2 = \{3, 4\}$. The $(b+1)k$ transmissions are divided into the following four groups:

- Transmissions where both m_{1j_1} and $\bar{m}_{2j_2}$ are correct: Each symbol in this group is generated according to $p(x_1)p(x_2)p(y|x_1, x_2)$. Assume that there are k_1 such symbols.
- Transmissions where m_{1j_1} is in error but $\bar{m}_{2j_2}$ is correct: Each symbol in this group is generated according to $p(x_1)p(x_2)p(y|x_2)$. Assume that there are k_2 such symbols.
- Transmissions where $\bar{m}_{2j_2}$ is in error but m_{1j_1} is correct: Each symbol in this group is generated according to $p(x_1)p(x_2)p(y|x_1)$. Assume that there are k_3 such symbols.
- Transmissions where both m_{1j_1} and $\bar{m}_{2j_2}$ are in error: Each symbol in this group is generated according to $p(x_1)p(x_2)p(y)$. Assume that there are k_4 such symbols.

Note that $k_1 + k_2 + k_3 + k_4 = (b + 1)k$, $k_2 + k_4 = k|\mathcal{J}_1|$, and $k_3 + k_4 = k|\mathcal{J}_2|$.

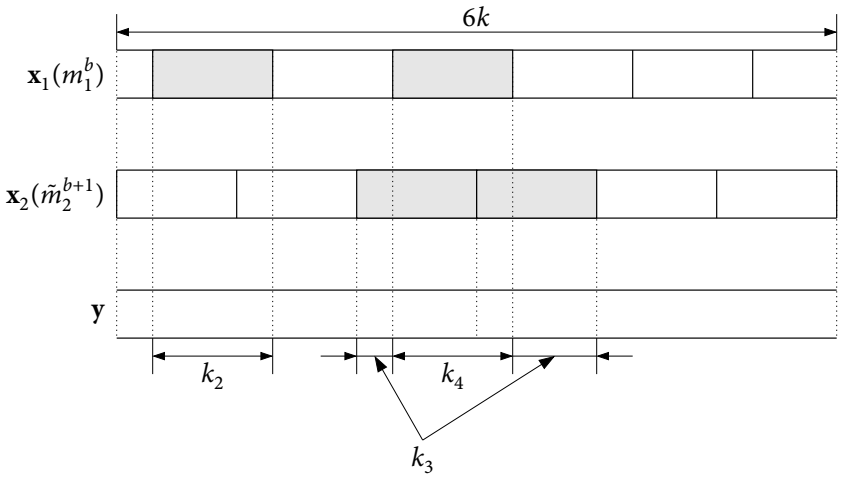


Figure 24.9. Illustration of error event $\mathcal{E}(\mathcal{J}_1, \mathcal{J}_2)$ partitioning into four groups. The shaded subblocks denote the messages in error.

Now, by the independence of the subblock codebooks and the joint typicality lemma,

$$\begin{aligned}&\mathsf{P}\{(\mathbf{X}_1(m_1^b), \mathbf{X}_2(\bar{m}_2^{b+1}), \mathbf{Y}) \in \mathcal{T}_\epsilon^{(n)}\}\\ &\qquad \le 2^{-k_2(I(X_1;Y|X_2)-\delta(\epsilon))} \cdot 2^{-k_3(I(X_2;Y|X_1)-\delta(\epsilon))} \cdot 2^{-k_4(I(X_1,X_2;Y)-\delta(\epsilon))} \end{aligned} \tag{24.5}$$

for each submessage sequence pair $(m_1^b, \bar{m}_2^{b+2})$ with the given error location. Furthermore, the total number of such submessage sequence pairs is upper bounded by $2^{k(|\mathcal{J}_1|R_1+|\mathcal{J}_2|R_2)}$. Thus, by the union of events bound and (24.5), we have

$$\begin{aligned}\mathsf{P}(\mathcal{E}(\mathcal{J}_1, \mathcal{J}_2)) &\le 2^{k(|\mathcal{J}_1|R_1+|\mathcal{J}_2|R_2)} \cdot 2^{-k_2(I(X_1;Y|X_2)-\delta(\epsilon))-k_3(I(X_2;Y|X_1)-\delta(\epsilon))-k_4(I(X_1,X_2;Y)-\delta(\epsilon))}\\ &= 2^{-k_2(I(X_1;Y|X_2)-R_1-\delta(\epsilon))} \cdot 2^{-k_3(I(X_2;Y|X_1)-R_2-\delta(\epsilon))} \cdot 2^{-k_4(I(X_1,X_2;Y)-R_1-R_2-\delta(\epsilon))},\end{aligned}$$

which tends to zero as $k \to \infty$ if $R_1 < I(X_1; Y|X_2) - \delta(\epsilon)$, $R_2 < I(X_2; Y|X_1) - \delta(\epsilon)$, and $R_1 + R_2 < I(X_1, X_2; Y) - \delta(\epsilon)$.

The probability of decoding error for M_2^b can be bounded similarly. This completes the achievability proof of Theorem 24.2.

24.3.2 Proof of the Converse

Given a sequence of $(2^{nR_1}, 2^{nR_2}, n, d = n-1)$ codes such that $\lim_{n\to\infty} P_e^{(n)} = 0$, we wish to show that the rate pair (R_1, R_2) must satisfy the inequalities in Theorem 24.2 for some product pmf $p(x_1)p(x_2)$. Recall that the codebook is used independently in consecutive blocks. Assume that $d_1 = 0$ and the receiver can synchronize the decoding with the transmitted sequence from sender 1. The probability of error in this case is

$$\max_{d_2\in[0:n-1]} \sup_l P_{el}^{(n)}(0, d_2) \le \max_{d_1,d_2\in[0:n-1]} \sup_l P_{el}^{(n)}(d_1, d_2) = P_e^{(n)}.$$

Further assume that $D_2 \sim \text{Unif}[0 : n-1]$. Then the expected probability of error is upper bounded as $\mathsf{E}_{D_2}(\sup_l P_{el}^{(n)}(0, D_2)) \le P_e^{(n)}$. We now prove the converse under these more relaxed assumptions.

To simplify the notation and ignore the edge effect, we assume that the communication started in the distant past, so (X_1^n, X_2^n, Y^n) has the same distribution as $(X_{1,n+1}^{2n}, X_{2,n+1}^{2n}, Y_{n+1}^{2n})$. Consider decoding the received sequence $Y^{(\kappa+1)n-1}$ to recover the sequence of κ message pairs $(M_{1l}, M_{2l}) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$, $l \in [1 : \kappa]$.

By Fano's inequality,

$$H(M_{1l}, M_{2l}|Y^{(\kappa+1)n}, D_2) \le H(M_{1l}, M_{2l}|Y^{(\kappa+1)n-1}) \le n\epsilon_n$$

for $l \in [1 : \kappa]$, where ϵ_n tends to zero as $n \to \infty$.

Following the converse proof for the synchronous DM-MAC in Section 4.5, it is easy to show that

$$\begin{aligned}
\kappa n R_1 &\le \sum_{i=1}^{(\kappa+1)n} I(X_{1i}; Y_i|X_{2,i-D_2}, D_2) + \kappa n\epsilon_n,\\
\kappa n R_2 &\le \sum_{i=1}^{(\kappa+1)n} I(X_{2,i-D_2}; Y_i|X_{1i}, D_2) + \kappa n\epsilon_n,\\
\kappa n(R_1 + R_2) &\le \sum_{i=1}^{(\kappa+1)n} I(X_{1i}, X_{2,i-D_2}; Y_i|D_2) + \kappa n\epsilon_n.
\end{aligned}$$

Now let $Q \sim \text{Unif}[1 : n]$ (not over $[1 : (\kappa+1)n-1]$) be the time-sharing random variable independent of $(X_1^{\kappa n}, X_2^{\kappa n}, Y^{(\kappa+1)n}, D_2)$. Then

$$\begin{aligned}
\kappa n R_1 &\le \sum_{l=1}^{\kappa+1} nI(X_{1,Q+(l-1)n}; Y_{Q+(l-1)n}|X_{2,Q+(l-1)n-D_2}, D_2, Q) + \kappa n\epsilon_n\\
&\overset{(a)}{=} (\kappa+1)nI(X_{1Q}; Y_Q|X_{2,Q-D_2}, Q, D_2) + \kappa n\epsilon_n\\
&= (\kappa+1)nI(X_1; Y|X_2, Q, D_2) + \kappa n\epsilon_n\\
&\overset{(b)}{\le} (\kappa+1)nI(X_1; Y|X_2) + \kappa n\epsilon_n,
\end{aligned}$$

where $X_1 = X_{1Q}$, $X_2 = X_{2,Q-D_2}$, $Y = Y_Q$, (a) follows since the same codebook is used over blocks, and (b) follows since $(Q, D_2) \to (X_1, X_2) \to Y$ form a Markov chain. Similarly

$$\kappa n R_2 \le (\kappa + 1) n I(X_2; Y | X_1) + \kappa n \epsilon_n,$$
$$\kappa n (R_1 + R_2) \le (\kappa + 1) n I(X_1, X_2; Y) + \kappa n \epsilon_n.$$

Note that since $D_2 \sim \text{Unif}[0 : n-1]$ is independent of Q, X_2 is independent of Q and thus of X_1. Combining the above inequalities, and letting $n \to \infty$ and then $\kappa \to \infty$ completes the proof of Theorem 24.2.

SUMMARY

- DMC with random arrival model:
  - Queue stability
  - Channel capacity is the limit on the arrival rate for reliable communication
  - Extensions to multiuser channels
- Random access channel as a MAC with state:
  - Compound channel approach
  - ALOHA
  - Adaptive coding
  - Broadcast channel approach
- Asynchronous MAC:
  - Capacity region does not change under mild asynchrony
  - Capacity region under total asynchrony reduces to the synchronous capacity region without time sharing
  - Subblock coding and synchronization via preamble decoding
  - Simultaneous decoding increases the rates under asynchrony
- **Open problem 24.1.** What is the capacity region of the asynchronous MAC when $d = \alpha n$ for $\alpha \in (0, 1)$?

BIBLIOGRAPHIC NOTES

The "unconsummated union" between information theory and networking was surveyed by Ephremides and Hajek (1998). This survey includes several topics at the intersection of the two fields, including multiple access protocols, timing channels, effective bandwidth

of bursty data sources, deterministic constraints on data streams, queuing theory, and switching networks. The result on the stability region of a DM-MAC mentioned in Remark 24.1 can be found, for example, in Kalyanarama Sesha Sayee and Mukherji (2006). The random access (collision) channel is motivated by the ALOHA System first described in Abramson (1970). A comparative study of information theoretic and collision resolution approaches to the random access channel is given by Gallager (1985). The adaptive coding approach in Section 24.2 is an example of the DM-MAC with distributed state information studied in Hwang, Malkin, El Gamal, and Cioffi (2007). The broadcast channel approach to the random access channel is due to Minero, Franceschetti, and Tse (2009). They analyzed the broadcast channel approach for the N-sender random access channel and demonstrated that simultaneous decoding can greatly improve the average throughput over simple collision resolution approaches as sketched in Figure 24.10.

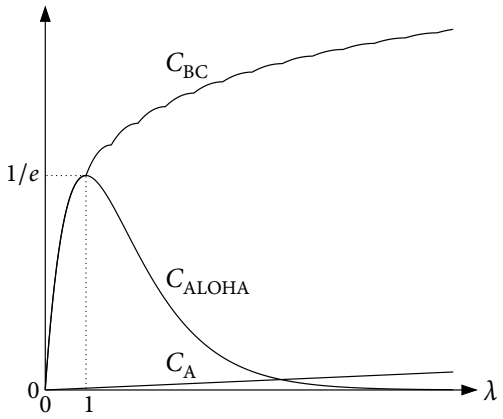


Figure 24.10. Comparison of the sum-capacities (average throughputs) of ALOHA (C_{ALOHA}), adaptive coding (C_{A}), and broadcast channel approach (C_{BC}) versus the load (average number of active senders) λ.

Cover, McEliece, and Posner (1981) showed that mild asynchrony does not affect the capacity region of the DM-MAC. Massey and Mathys (1985) studied total asynchrony in the collision channel without feedback and showed that time sharing cannot be used. The capacity region of the totally asynchronous DM-MAC in Theorem 24.2 is due to Poltyrev (1983) and Hui and Humblet (1985). Verdú (1989) extended this result to multiple access channels with memory and showed that unlike the memoryless case, asynchrony can in general reduce the sum-capacity.

PROBLEMS

24.1. Provide the details of the converse proof of Theorem 24.1 by justifying the second inequality in (24.2).

24.2. Consider the DM-MAC $p(y_1, y_2|x)$ with two i.i.d. arrival processes $\{A_1(i)\}$ and $\{A_2(i)\}$ of arrival rates λ_1 and λ_2, respectively. Show that the stability region $\mathscr{S}$ is equal to the capacity region $\mathscr{C}$.

24.3. *Nonslotted DMC with random data arrivals.* Consider the DMC with random data arrival process $\{A(i)\}$ as defined in Section 24.1. Suppose that the sender transmits a codeword if there are more than nR bits in the queue and transmits a fixed symbol, otherwise. Find the necessary and sufficient conditions for reliable communication (that is, the queue is stable and the message is recovered).

24.4. *Two-sender three-receiver channel with 2 messages.* Consider a DM 2-sender 3-receiver channel $p(y_1|x_1)p(y_2|x_2)p(y_{12}|x_1, x_2)$, where the message demands are specified as in Figure 24.3.

(a) Show that the capacity region of this channel is the set of rate pairs $(\tilde{R}_1, \tilde{R}_2)$ such that

$$\begin{aligned} \tilde{R}_1 &\le I(X_1; Y_1|Q), \\ \tilde{R}_1 &\le I(X_1; Y_{12}|X_2, Q), \\ \tilde{R}_2 &\le I(X_2; Y_2|Q), \\ \tilde{R}_2 &\le I(X_2; Y_{12}|X_1, Q), \\ \tilde{R}_1 + \tilde{R}_2 &\le I(X_1, X_2; Y_{12}|Q) \end{aligned}$$

for some $p(q)p(x_1|q)p(x_2|q)$.

(b) Consider the special case in Figure 24.4, where X_1 and X_2 are binary, and $Y_1 = X_1$, $Y_2 = X_2$, and $Y_{12} = X_1 \oplus X_2$. Show that the capacity region reduces to the set of rate pairs $(\tilde{R}_1, \tilde{R}_2)$ such that $\tilde{R}_1 + \tilde{R}_2 \le 1$ and can be achieved without time sharing.

24.5. *Two-sender three-receiver channel with 4 messages.* Consider a DM 2-sender 3-receiver channel $p(y_1|x_1)p(y_2|x_2)p(y_{12}|x_1, x_2)$, where the message demands are specified as in Figure 24.4.

(a) Show that a rate quadruple $(\tilde{R}_{10}, \tilde{R}_{11}, \tilde{R}_{20}, \tilde{R}_{22})$ is achievable if

$$\begin{aligned} \tilde{R}_{11} &\le I(X_1; Y_1|U_1, Q), \\ \tilde{R}_{10} + \tilde{R}_{11} &\le I(X_1; Y_1|Q), \\ \tilde{R}_{22} &\le I(X_2; Y_2|U_2, Q), \\ \tilde{R}_{20} + \tilde{R}_{22} &\le I(X_2; Y_2|Q), \\ \tilde{R}_{10} + \tilde{R}_{20} &\le I(U_1, U_2; Y_{12}, Q), \\ \tilde{R}_{10} &\le I(U_1; Y_{12}|U_2, Q), \\ \tilde{R}_{20} &\le I(U_2; Y_{12}|U_1, Q) \end{aligned}$$

for some pmf $p(q)p(u_1, x_1|q)p(u_2, x_2|q)$.

(b) Consider the special case in Figure 24.4, where X_1 and X_2 are binary, and $Y_1 = X_1$, $Y_2 = X_2$, and $Y_{12} = X_1 \oplus X_2$. Show that the above inner bound simplifies to (24.3). (Hint: Show that both regions have the same five extreme points $(1, 0, 0, 0)$, $(0, 1, 0, 0)$, $(0, 0, 1, 0)$, $(0, 0, 0, 1)$, and $(0, 1, 0, 1)$.)

(c) Prove the converse for the capacity region in (24.3).

24.6. *MAC and BC with known delays.* Consider the DM-MAC and the DM-BC with constant delays d_1 and d_2 known at the senders and the receivers. Show that the capacity regions for these channels coincide with those without any delays.

24.7. *Mild asynchrony.* Consider the DM-MAC with delays $d_1, d_2 \in [0 : d]$ such that d/n tends to zero as $n \to \infty$. Show that the capacity region is equal to that without any delays. (Hint: Consider all contiguous codewords of length $n - d$ and perform joint typicality decoding using y_{d+1}^n for each delay pair.)

APPENDIX 24A PROOF OF LEMMA 24.1

We first prove the converse, that is, the necessity of $\lambda \le R$. By the transition law for $Q(i)$ in (24.1),

$$Q(i+1) \ge \begin{cases} Q(i) - nR + A(i) & \text{if } i = jn, \\ Q(i) + A(i) & \text{otherwise.} \end{cases}$$

Hence, by summing over i and telescoping, we have $Q(jn+1) \ge \sum_{i=1}^{jn} A(i) - jnR$. By taking expectation on both sides and using the stability condition, we have $\infty > B \ge \mathsf{E}(Q(jn+1)) \ge jn(\lambda - R)$ for $j = 1, 2, \ldots$. This implies that $R \ge \lambda$.

Next we prove the sufficiency of $\lambda < R$ using an elementary form of Foster–Lyapunov techniques (Meyn and Tweedie 2009). Let $\tilde{Q}_j = Q((j-1)n+1)$ for $j = 1, 2, \ldots$ and $\tilde{A}_j = \sum_{i=(j-1)n+1}^{jn} A(i)$. Then, by the queue transition law,

$$\begin{aligned} \tilde{Q}_{j+1} &= \begin{cases} \tilde{Q}_j - nR + \tilde{A}_j & \text{if } \tilde{Q}_j \ge nR, \\ \tilde{Q}_j + \tilde{A}_j & \text{otherwise} \end{cases} \\ &\le \max\{\tilde{Q}_j - nR,\ nR\} + \tilde{A}_j \\ &= \max\{\tilde{Q}_j - 2nR,\ 0\} + \tilde{A}_j + nR. \end{aligned}$$

Since $(\max\{\tilde{Q}_j - 2nR,\ 0\})^2 \le (\tilde{Q}_j - 2nR)^2$,

$$\tilde{Q}_{j+1}^2 \le \tilde{Q}_j^2 + (2nR)^2 + (\tilde{A}_j + nR)^2 - 2\tilde{Q}_j(nR - \tilde{A}_j).$$

By taking expectation on both sides and using the independence of $\tilde{Q}_j$ and $\tilde{A}_j$ and the fact that $\mathsf{E}(\tilde{A}_j) = n\lambda$ and $\mathsf{E}((\tilde{A}_j + nR)^2) \le n^2(k+R)^2$, we obtain

$$\mathsf{E}(\tilde{Q}_{j+1}^2) \le \mathsf{E}(\tilde{Q}_j^2) + n^2((k+R)^2 + 4R^2)) - 2n(R-\lambda)\,\mathsf{E}(\tilde{Q}_j),$$

or equivalently,

$$\mathsf{E}(\tilde{Q}_j) \le \frac{n((k+R)^2+4R^2)}{2(R-\lambda)} + \frac{\mathsf{E}(\tilde{Q}_j^2) - \mathsf{E}(\tilde{Q}_{j+1}^2)}{2n(R-\lambda)}.$$

Since $\tilde{Q}_1 = 0$, summing over j and telescoping, we have

$$\frac{1}{b}\sum_{j=1}^{b} \mathsf{E}(\tilde{Q}_j) \le \frac{n((k+R)^2+4R^2)}{2(R-\lambda)} + \frac{\mathsf{E}(\tilde{Q}_1^2) - \mathsf{E}(\tilde{Q}_{b+1}^2)}{2nb(R-\lambda)} \le \frac{n((k+R)^2+4R^2)}{2(R-\lambda)}.$$

Recall the definition of $\tilde{Q}_j = Q((j-1)n+1)$ and note that $Q(i) \le Q((j-1)n+1) + kn$ for $i \in [(j-1)n+1 : jn]$. Therefore, we have *stability in the mean*, that is,

$$\sup_l \frac{1}{l}\sum_{i=1}^{l} \mathsf{E}(Q(i)) \le B < \infty. \tag{24.6}$$

To prove stability, i.e., $\sup_i \mathsf{E}(Q(i)) < \infty$, which is a stronger notion than stability in the mean in (24.6), we note that the Markov chain $\{\tilde{Q}_j\}$ is positively recurrent; otherwise, the stability in the mean would not hold. Furthermore, it can be readily checked that the Markov chain is aperiodic. Hence, the chain has a unique limiting distribution and $\mathsf{E}(\tilde{Q}_j)$ converges to a limit (Meyn and Tweedie 2009). But by the Cesàro mean lemma (Hardy 1992, Theorem 46), $(1/b)\sum_{j=1}^{b} \mathsf{E}(\tilde{Q}_j) < \infty$ for all b implies that $\lim_j \mathsf{E}(\tilde{Q}_j) < \infty$. Thus, $\sup_j \mathsf{E}(\tilde{Q}_j) < \infty$ (since $\mathsf{E}(\tilde{Q}_j) < \infty$ for all j). Finally, using the same argument as before, we can conclude that $\sup_i \mathsf{E}(Q(i)) < \infty$, which completes the proof of stability.

APPENDIX 24B PROOF OF LEMMA 24.2

First consider the case $d \ge k$ (indices for the underlying k-sequences do not overlap). Then $(X_1, Y_{d+1}), (X_2, Y_{d+2}), \ldots$ are i.i.d. with $(X_i, Y_{d+i}) \sim p_X(x_i)p_Y(y_{d+i})$. Hence, by the joint typicality lemma,

$$\mathsf{P}\{(X^k, Y_{d+1}^{d+k}) \in \mathcal{T}_\epsilon^{(n)}(X,Y)\} \le 2^{-k(I(X;Y)-\delta(\epsilon))}.$$

Next consider the case $d \in [1 : k-1]$. Then X^k and Y_{d+1}^{d+k} have overlapping indices and are no longer independent of each other. Suppose that $\epsilon > 0$ is sufficiently small that $(1-\epsilon)p_{X,Y}(x^*, y^*) \ge (1+\epsilon)p_X(x^*)p_Y(y^*)$ for some (x^*, y^*). Let $p = p_X(x^*)p_Y(y^*)$ and $q = p_{X,Y}(x^*, y^*)$. For $i \in [1 : k]$, define $\tilde{Y}_i = Y_{d+i}$ and

$$E_i = \begin{cases} 1 & \text{if } (X_i, \tilde{Y}_i) = (x^*, y^*), \\ 0 & \text{otherwise.} \end{cases}$$

Now consider

$$\pi(x, y | X^k, \tilde{Y}^k) = \frac{|\{i : (X_i, \tilde{Y}_i) = (x^*, y^*)\}|}{k} = \frac{1}{k}\sum_{i=1}^{k} E_i.$$

Since $\{(X_i, \tilde{Y}_i)\}$ is stationary ergodic with $p_{X_i,\tilde{Y}_i}(x^*, y^*) = p$ for all $i \in [1:k]$,

$$\begin{aligned}\mathsf{P}\{(X^k, Y_{d+1}^{d+k}) \in \mathcal{T}_\epsilon^{(n)}(X, Y)\} &\le \mathsf{P}\{\pi(x^*, y^* | X^k, \tilde{Y}^k) \ge (1-\epsilon)q\} \\ &\le \mathsf{P}\{\pi(x^*, y^* | X^k, \tilde{Y}^k) \ge (1+\epsilon)p\},\end{aligned}$$

which, by Birkhoff's ergodic theorem (Petersen 1983, Section 2.2), tends to zero as $n \to \infty$. To show the exponential tail, however, we should bound $\mathsf{P}\{\pi(x^*, y^*|X^k, \tilde{Y}_{d+1}^{d+k}) \ge (1+\epsilon)p\}$ more carefully.

Assuming that k is even, consider the following two cases. First suppose that d is odd. Let $U^{k/2} = ((X_{2i-1}, \tilde{Y}_{d+2i-1}) \colon i \in [1:k/2])$ be the subsequence of odd indices. Then $U^{k/2}$ is i.i.d. with $p_{U_i}(x^*, y^*) = p$ and by the Chernoff bound in Appendix B,

$$\mathsf{P}\{\pi(x^*, y^* | U^{k/2}) \ge (1+\epsilon)p\} \le e^{-kp\epsilon^2/6}.$$

Similarly, let $V^{k/2} = \{(X_{2i}, \tilde{Y}_{2i})\}_{i=1}^{k/2}$ be the subsequence of even indices. Then

$$\mathsf{P}\{\pi(x^*, y^* | V^{k/2}) \ge (1+\epsilon)p\} \le e^{-kp\epsilon^2/6}.$$

Thus, by the union of events bound,

$$\begin{aligned}&\mathsf{P}\{\pi(x^*, y^* | X^k, \tilde{Y}^k) \ge (1+\epsilon)p\} \\ &\quad = \mathsf{P}\{\pi(x^*, y^* | U^{k/2}, V^{k/2}) \ge (1+\epsilon)p\} \\ &\quad \le \mathsf{P}\{\pi(x^*, y^* | U^{k/2}) \ge (1+\epsilon)p \text{ or } \pi(x^*, y^* | V^{k/2}) \ge (1+\epsilon)p\} \\ &\quad \le 2e^{-kp\epsilon^2/6}.\end{aligned}$$

Next suppose that d is even. We can construct two i.i.d. subsequences by alternating even and odd indices for every d indices, we have

$$U^{k/2} = \big((X_i, \tilde{Y}_i) \colon i \text{ odd } \in [(2l-1)d + 1 : 2ld],\ i \text{ even } \in [2ld + 1 : 2(l+1)d]\big).$$

For example, if $d = 2$, then $U^{k/2} = ((X_i, Y_{d+i}) \colon i = 1, 4, 5, 8, 9, 12, \ldots)$. The rest of the analysis is the same as before. This completes the proof of the lemma.